PrepDSpace4Mobility

Towards a common European mobility data space

Perspectives, recommendations and building blocks

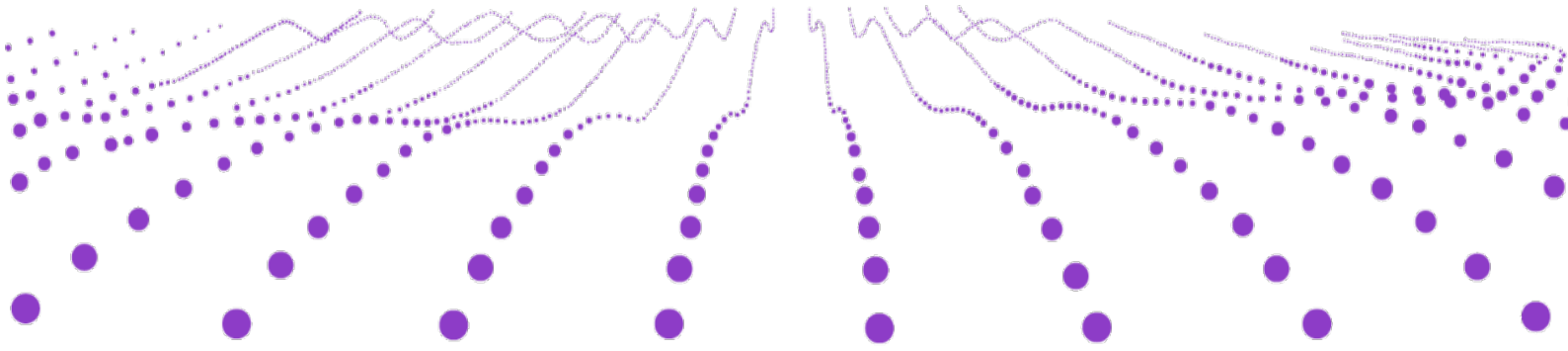
Deliverable D3.1

Version N°2

Authors (alphabetic order): Bakri, Taoufik (TNO), Bastiaansen, Harrie (TNO), Benmayor, Aliki (KU Leuven), Blaya, Mariano (IDSA), Böge, Gernot (FIWARE), Cases, Jean-Francois (Amadeus), Eisenrauch, Andreas (Amadeus), Engh, Emil (iSHARE) Epardeau, Dominique (ADP), Federl, Stefanie (acatech), Fernandes, Elora (KU Leuven), van der Hoeven, Gerard (iSHARE), King, Leona (KU Leuven), Kirstein, Lucie (acatech), Kraft, Volker (Fraunhofer IML), Lenz, Gadi (USI), Lilja, Juha (VTT), Morgan, Josefine (acatech), Nagel, Ingrid (Fraunhofer IVI), Öörni, Risto (VTT), Pretzsch, Sebastian (Fraunhofer IVI), Scholliers, Johan (VTT), Schulz, Holger (Fraunhofer IML), Spijkers, Nico (TNO).

We would like to thank all reviewers for dedicating their time and effort to offer valuable advice and comments on the report. Special thanks are extended to the reviews undertaken by the Data Space Support Centre community, the Green Deal data space community, the Energy data space community, the Smart and Sustainable Cities and Communities data space community, and members of the Alliance for Industrial Data, Edge and Cloud.

We extend our thanks to Nasim Kroegel (acatech) for extensive editorial support. We would also like to thank Theodore Best for contributing to the editing process.



Document summary information

Grant Agreement No	101083655	**Acronym**	PrepDSpace4Mobility
Full Title	Preparatory Actions for the Data Space for Mobility		
Start Date	01.10.2022	**Duration**	12 months
Project URL	https://www.mobilitydataspace-csa.eu		
Deliverable number	D3.1		
Work Package	WP3		
Submission date	29.09.2023		
Type of deliverable	Report	**Dissemination Level**	PU- Public
Lead Beneficiary	TNO		

Document history

Version	Date	Comment
V1	29.09.2023	First submission
V2	27.10.2023	Final deliverable

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the Directorate-General for Communications Networks, Content and Technology (DG CONNECT). Neither the European Union nor the granting authority can be held responsible for them.

Executive summary

This report provides a comprehensive analysis of the current challenges and possible future directions of the European Commission's European mobility data space (EMDS) initiative. Grounded in stakeholder engagement, surveys, and consultations, it presents recommendations on the foundational principles, technical developments, and business and governance models essential for the success of the EMDS. The report provides guidance for various stakeholders on the creation of an interoperable and value-driven mobility data sharing environment in Europe, while building upon the principles of data sovereignty and trust.

The findings from this project highlight key challenges and opportunities within the mobility and logistics data ecosystems in Europe. The findings emphasise the need for increased efforts in addressing interoperability challenges, as well as the development of common technical capabilities for data sovereignty and trust and data discoverability. With the insights and recommendations provided herein, Europe is better positioned to develop a more cohesive and efficient mobility data sharing framework.

The development and direction of the European Commission's initiative for a common European mobility data space (EMDS) will be informed by a multi-faceted approach. PrepDSpace4Mobility supports the initiative with two deliverables: 1) an inventory of data ecosystems in mobility and logistics and 2) this particular analysis report presenting perspectives, recommendations and important building blocks for the EMDS.

Methodology

To **analyse the requirements for the mobility sector**, two surveys were conducted using distinct questionnaires designed to identify data gaps overlaps, existing data sharing initiatives, and the technical and governance requirements of data-sharing ecosystems. In total, the project gathered responses from 63 organisations, spanning 18 diverse application domains within mobility and logistics. The consultation process involved 21 leading data-sharing initiatives across Europe. To ensure a broad scope and integration with other sectors, the project closely coordinated with four sectoral data space CSAs, specifically those working on tourism, smart cities, the green deal, and energy. To engage stakeholders and experts, the project hosted four workshops that collectively involved over 500 individuals. Additionally, the project organised two Public Stakeholder Forums, inviting authorities, agencies, technology providers, users in mobility and logistics, as well as data and service providers.

The **analysis of the building blocks and reference architecture for the EMDS** is grounded in the leading EU reference architectures for federated data sharing, specifically drawing from the work of the International Data Spaces Association (IDSA), Gaia-X, iSHARE, the Data Spaces Business Alliance (DSBA) and the preliminary version of the DSSC blueprint. PrepDSpace4Mobility built upon this prior work to develop a proposed set of building blocks and a reference architecture for the EMDS.

Context

The active engagement of stakeholders in Europe enabled the identification of several overarching challenges. These include a lack of knowledge concerning the conceptual and technical foundations of data spaces and the EMDS. In addition, the value proposition of the EMDS, and that of data spaces in general, requires further refinement and alignment with stakeholders' views, preferences and needs. Further, stakeholders viewed the project's surveys and consultations as challenging, indicating low adoption readiness and the need for enhanced awareness and education around the concept of the EMDS. Furthermore, general uncertainty persists among stakeholders regarding the future technical landscape with respect to the development of data spaces in general, especially regarding outcomes of the DSSC and SIMPL initiatives. In addition to the technical decisions underway at European level,

the future governance landscape of the EMDS is still evolving, which includes the strategy towards its operationalisation and its interplay with broader ecosystems and other sectoral data spaces.

With respect to the operationalisation of the EMDS and its governance, it has become apparent that several possible scenarios can be anticipated that range from a strong role of the EMDS in operating a data space to a more limited role in providing guidelines for interoperability. These scenarios include possibilities for the creation of:

1. A European Commission (EC)-driven initiative or organisation with an operational data space authority.
2. A Member State-driven European Digital Infrastructure Consortium (EDIC) serving as the foundational backbone of the EMDS.
3. A European association dedicated to data spaces in mobility, possibly steered by technical architects of Europe's major mobility and logistics data spaces.
4. A governance, regulatory or certification framework at European level.
5. An expert working group, responsible for defining and disseminating guidelines for interoperability between different mobility and logistics data ecosystems.

When evaluating these scenarios for the EMDS, it is key to consider both the long-term sustainability of EMDS operations model and its adequate thematic and geographic representativeness, with stakeholders highlighting planning stability and support for interoperability use cases as key priorities.

Overview of recommendations

The main recommendations derived from the analysis of the requirements of the mobility sector and the analysis of the building blocks and reference architecture for the EMDS are formulated along the lines of the DSSC taxonomy of data space building blocks. The recommendations cover a wide range of aspects, including requirements for mobility and logistics data sources, organisational, legal and financial aspects, as well as the technical building blocks and architecture proposed for the EMDS.

Key takeaways and recommendations from the analysis of **data source gaps and overlaps** include:

- Address the requirements of various types of data sharing including persistent data, streaming data, algorithms for local processing, and event-driven smart contracting. The DSSC technical grounding work will develop a common implementation approach for sharing persistent and streaming data. However, more emphasis should be put on algorithm sharing and event-driven smart contracting since their relevance for the EMDS is expected to increase rapidly;
- Bridge existing data accessibility gaps to increase discoverability and availability while reducing data acquisition barriers;
- Provide guidance to ensure a uniform approach of data quality across platforms;
- Support harmonisation and standardisation of data sets and data models;
- Streamline knowledge exchange to minimise redundancies in data sharing initiatives;
- Leverage synergies with the various types of data sharing initiatives in mobility and logistics and adjacent sectoral data spaces.

The analysis of the EMDS **business and funding models** provides insights into the added value that a common EMDS brings to multiple stakeholders in the ecosystem. The analysis highlighted multiple concerns from stakeholders about participation including the challenge in creating a sustainable and resilient business and funding model that caters to the diverse needs of the mobility and logistics sector. The value proposition centres around data sovereignty and trust in data sharing, backed by an adequate technical infrastructure and apt governance mechanisms. To ensure success and sustainability of the EMDS, it is recommended to:

- Prioritise discoverability, data sovereignty and trust;
- Establish a neutral governance entity;

- Integrate modern technical infrastructure aligned with the generic technical grounding of the EU data space approach;
- Simplify onboarding processes, with a special focus on SMEs and start-ups;
- Implement stringent standards for data and application quality;
- Accelerate use case development;
- Support the adoption and sustainability of the data space through public funding.

The EMDS **governance framework** serves as the foundation upon which the entire data space operates, encompassing the rules and practices that govern how data is managed, shared and utilised. These rules and practices should be compliant with legislation, ethical standards and interoperability between data spaces. To ensure transparent and effective data sharing, the EMDS governance framework should:

- Align EMDS development with the strategies at EU level, notably the DSSC, SIMPL and EDIB;
- Adopt a multi-level governance model, incorporating subsidiarity principles whilst adhering to the EU strategy for common European data spaces;
- Address thoroughly in the governance framework the complexities of data sharing collaboration in mobility and logistics, specifically the imbalances between stakeholder interests;
- Govern key capabilities of data sovereignty, trust, and discoverability at the European level to ensure interoperability;
- Streamline cross-sectoral collaborations and integrate best practices from existing data-sharing ecosystems and their use cases;
- Build upon existing governance frameworks maintained by an active community of users.

Legal considerations are central to the organisation and governance of data spaces, recognising regulatory compliance and contractual frameworks as legal basis, including both cross-sectoral “horizontal” EU legislation on data sharing and mobility specific “vertical” legislation. The complexity of the applicable legal framework points to a need for legal guidance under the EMDS. Key takeaways and recommendations include:

- Supporting privacy and data protection norms;
- Support stakeholders in respecting intellectual property rights and safeguard trade secrets;
- Support members regarding competition law and possible implications for data sharing;
- Investing in robust cyber resilience measures;
- Continuously monitoring legislative developments in the mobility sector;
- Delineating and clarifying roles and responsibilities for all participants, particularly regarding the Data Governance Act, ensuring awareness on obligations and rights;
- Examining the potential of data intermediation service providers;
- Bridging the legal-technical gap by forming cross-disciplinary teams that can effectively transpose legal requirements into technical capabilities;
- Promoting dialogue between other preparatory actions and initiatives to inform the EMDS.

The **technical grounding** for common building blocks is an integral part of the DSSC blueprint and provides the common technical basis for developing a federation of interoperable data spaces. The blueprint is expected to build upon the evolving work on reference architectures for federated data sharing that have evolved over the last years, including initiatives such as IDSA, Gaia-X, iSHARE, and the DSBA. In this context, it is important to reach consensus on protocols and specifications for implementing the key capabilities on data sovereignty, trust and discoverability are important in this context. Key takeaways and recommendations include:

- Ensuring alignment with overarching European data space architectures currently under development;

- Prioritising the development of Minimal Interoperability Mechanisms (MIMs), considering data sovereignty, trust, and discoverability as cornerstones of interoperable data spaces;
- Facilitating the adoption process for EMDS guidelines or frameworks through interconnection tools and scenarios.

Data interoperability entails the use of common data models, data formats and data exchange APIs to ensure semantic interoperability among data space participants. It also includes capabilities for both data provenance and traceability and for handling semantic differences in data model implementations.

The analysis shows that European mobility and logistics sectors face numerous hurdles in achieving data interoperability due to the heterogeneity of data models, formats, and standards. Influenced by different stakeholders, purposes, and regions, this diversity poses significant barriers to data harmonisation across Europe. For instance, while standards like NeTEx or DATEX II are utilised, their implementation can differ substantially by region. There is a pressing need for an overarching system to ensure effective data integration and utilisation. Key takeaway and recommendations include:

- Focusing on harmonising sector-specific data models;
- Implementing linked data concepts for a unified approach;
- Offering methods for data model registration and mappings and for run-time data conversion;
- Instituting unified metadata and information models;
- Ensuring full compatibility with existing mobility specific protocols;
- Employing data quality frameworks.

Data sovereignty and trust play an important role in fostering a conducive environment for data sharing within specific mobility data spaces and in a federation of interoperable mobility and other sectoral data spaces. They allow individuals and organisations to retain authority over their data and have confidence in the controlled usage of the data they share. Currently, many trust mechanisms and frameworks are in development, necessitating a harmonised and aligned approach. Moreover, given the unique nature of data in the mobility sector, it is necessary to consider specific requirements that might not be prevalent in other sectors, while adhering to broader requirements defined at EU level. Key takeaways and recommendations include:

- Aligning EMDS operations with the emerging EU technical framework for data spaces;
- Supporting decentralised trust mechanisms;
- Supporting delegation of authorisation rights to third parties;
- Implementing robust consent management systems to allow entitled parties, not just data holders, to provide consent for data sharing, thereby reinforcing data sovereignty;
- Supporting multiple approaches for agreements on authorisation policies, including the mechanism proposed by the EU CEF FEDeRATED initiative;
- Ensuring the confidentiality aspects of information security through data sovereignty and trust capabilities, as well as the data integrity and availability aspects of information security, as part of the governance framework;
- Designing robust conflict and incident management measures, especially relevant for cross-border mobility data sharing settings;
- Ensuring operations are mobile-friendly with information available offline and facilitate integration with prevalent digital wallets.

Data value creation capabilities allow participants in the EMDS to create value by making IT resources available to its participants. This requires a common means for describing the data space's IT resources, along with their associated terms, conditions and contracts, as well as their publication, discovery and accessibility. This may apply to both data services, to data apps and algorithms and to data models and mappings. These capabilities not only streamline IT resource registration, exposure, and discovery but also support the creation of multi-sided markets. Key takeaways and recommendations include:

- Developing a metadata broker that supports the four types of data sharing identified for the mobility and logistics data space;
- Harmonising the federation of metadata/context brokers to ensure discoverability across data spaces;
- Supporting semantic translation via tools like vocabulary hubs and semantic transformation engines to address semantic disparities in data models;
- Endorsing local execution of data apps, ensuring data protection and scalability;
- Integrating Mobility-as-a-Service requirements and considering the proposal of harmonised tools for varied ticket categories, pricing, and user demands;
- Exploring and supporting use cases and application areas that bridge various sectors, for which the EMDS can promote development and adoption, such as across energy, tourism, and smart city implementations.

To conclude, the ability to share data beyond mandated data sharing is crucial for mobility and logistics, as highlighted by the increasing number of data sharing initiatives in these sectors. This underscores the clear role for the EMDS in aligning, connecting, and building upon these initiatives. Given the cross-border nature of mobility and logistics, mobility data spaces need to be interoperable with other sectoral data space initiatives to ensure that data can be easily shared and understood across various sectors. There is a parallel need to strengthen alignment with various EU edge and cloud initiatives, notably through the active involvement of DSSC and SIMPL. Interoperability of data spaces and data sharing initiatives both within the mobility and logistics sector and across multiple sectors will significantly improve data accessibility, paving the way for new services across Europe.

Contents

List of Figures

List of Tables

List of Boxes

Glossary

Where applicable, the glossary builds and extends upon the Data Spaces Support Centre (DSSC) glossary[1].

Table 1: Glossary

Term	Definition
Data space concepts	
Data sharing	The act of providing data access for use by others, subject to applicable technical, financial, legal or organisational use requirements. The term refers to a full spectrum of practices related to sharing any kind of data, including open data and the many forms of sharing non-open data.
Data space	An infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space. A data space should be generic enough to support the implementation of multiple use cases.
Intra data space interoperability	Individual data spaces have a high degree of autonomy in developing and deploying their own internal agreements and architecture. Intra data space interoperability focusses on the alignment of the various capabilities (building blocks) within an individual data space.
Inter data space interoperability	Interoperability between multiple data spaces is key for the federation of data spaces as expressed in the ambition of the EU Data Strategy. Inter data space interoperability addresses the required alignment and guidelines for data spaces to ensure interoperability between them.
Federation of data spaces	The organisation of two or more data spaces that have agreed upon standards for harmonised operation,, under a common governance framework to realise mutual synergies to realise mutual synergies. Although operating autonomously and with possible different internal architectures, the goal is to jointly operate as a single and harmonised ecosystem towards participants.
Full harmonisation of data spaces	An approach for federation of data spaces in which the data spaces adhere to a set of agreed upon and harmonised principles for federating the (intermediary) data space building blocks, especially those for data sovereignty, trust and discoverability
Partial harmonisation of data spaces	An approach for federation of data spaces in which harmonisation is done by means of a “data space proxy” which absorbs the complexity of harmonisation and allows data consumers and data providers and consumers within a data space to simply connect to other data spaces via their proxy.
Data space role	A data space role corresponds to a primary activity in the overarching processes of data sharing within data spaces, which may be performed by an independent organisation.
Data space building block	A basic unit or component that can be implemented and combined with other building blocks to achieve the functionality of a data space, being either technical components or organisational concepts.
Data space initiative	A collaborative project of a consortium or network of committed partners to deploy and maintain a data space.
Data transaction	The act of data sharing between two or more data space participants.

[1] Data Spaces Support Centre (2023), “DSSC Glossary”, https://dssc.eu/wp-content/uploads/2023/03/DSSC-Data-Spaces-Glossary-v1.0.pdf.

Governance	The creation, development, maintenance and enforcement of a governance framework (for the EMDS).
Governance framework	The set of principles, standards, policies (rules/regulations) and practices that apply to the governance, management and operations within a particular scope (e.g. a data space, a data space initiative, or a data spaces blueprint) as well as to the enforcement thereof, and the resolution of any conflicts.
Data space roles	
Data space participant	A legal or natural person or organisation engaged in a data space.
Governance authority	The party accountable for the governance of the (EMDS) framework.
Data entitled party	A transaction participant that has the legal right to use, grant access to or share certain data.
Data provider	A transaction participant that, in the context of a specific data transaction, technically provides data to the data consumers.
Data app entitled party	A transaction participant that has the legal right to use, grant access to or share certain data apps.
Data app provider	A transaction participant that technically provides the data apps to consumers.
Data consumer	A transaction participant to whom data is technically supplied by a data provider in the context of a specific data transaction.
Data app consumer	A transaction participant to whom a data app is technically supplied by a data app provider in the context of a specific data transaction.
Data and process orchestrator	A data space participant that orchestrates the execution of a specific data sharing and data processing transaction, and ensures the intended results for the data and/or data app consumer. The data and process orchestrator properly manages the policies for the processes it orchestrates.
Data user	A transaction participant that has been granted (lawful) access and the right to use data as the result of a specific data transaction. Also known as a data rights receiver.
Data space intermediary	A data space enabler that (technically and legally) connects one or more data space members to the data space, thereby enabling them to establish relationships and execute data transactions with other members in the data space.
Operator/execution environment	A data space participant that provides a trustworthy process execution environment in which the workloads defined and orchestrated by the data and process orchestrator can be deployed.
Broker services provider	A data space participant that provides capabilities to register, manage and expose information about IT resources available in a data space, e.g. data services, data apps and computing resources.
Data usage accounting provider	A data space participant that manages and provides the basis for accounting access to and/or usage of resources (e.g. data, data apps) by various participants.
App store provider	A data space participant that provides data apps which contain applications (e.g. algorithms) that may be deployed within the secure processing environments of the data space, e.g. in a participants or a (cloud) execution environment. The data apps facilitate data processing workflows.
Semantic services provider	A data space participant that provides services to manage semantics within the data space, including a registry of vocabularies, and semantic mappings that can be used to transform data sets. Moreover, the transformation of data sets can be provided as a separate service.

Data space authority	A data space participant that is responsible for the (legal and operational) agreements within a data space for certification of participants and components used within the data space and for the operations of the data space.
Data space identity provider	A data space participant that offers a service to create, manage, maintain, monitor, and validate identity information of participants and/or components in a data space.
Provider data space	A data space where participants share data services and apps with those in other data spaces.
Consumer data space	A data space that has participants that request data services or data apps from participants in another data space, i.e. a provider data space.
Data space interconnectivity broker service provider	A participant in a federation of data spaces that manages information (metadata) about individual data spaces, e.g. on the roles they support and data services and data app providers and consumers they contain. Its focus on making the data spaces and their services findable and available.
Data space interconnectivity authority	A participant in a federation of data spaces that is responsible for the (legal and operational) agreements between individual data spaces for certification of participating data space and for the operations of the federation of data spaces.
Data space interconnectivity membership identity provider	A participant in a federation of data spaces that offers a service to create, maintain, manage, monitor, and validate identity information on participating data spaces.
Data space building blocks	
Vocabulary hub	A registry for publishing, editing, browsing and maintaining vocabularies and related documentation, including ontologies, reference data models, schema specifications and data model mappings.
Semantic transformation engine	A semantic transformation service between data formats. It uses vocabularies and mapping specifications as provided by the vocabulary hub.
Data space connector semantics configurator	A service to enable data space participants to use vocabularies to configure the semantic interoperability of implementations. Additionally, it can assist in creating mapping specifications that can be used in the semantic transformation engine.
Data space connector	A main component in a data space that provides the interconnection between an organisation or system and the data sharing and intermediary capabilities of the data space.
Policy enforcement framework	A capability to enforce the applicable policy conditions, e.g. specific access and usage policies.
Policy registry	A registry for applicable policies in a data space, i.e. the specific access and usage rights for data space participants as attributed by entitled parties to data services or data apps, including delegation of the rights to other data space participants.
Workload deployment orchestrator	A capability to deploy and execute data apps in a secure and controlled manner. This may be either in the security environment of the data provider or data consumer or in a secure (cloud) environment provided by a third party.
Data space membership certificate authority system	A capability to provide certificates to participants and/or software components as being member of the data space.
Dynamic attribute provisioning service	A registry for the dynamic attributes of software modules implemented by means of a data space connector, including the security profiles, certification status, etc.

Participant information system	A registry for the attributes of the participants, specifically for natural persons or organisations as legal entities, including the name and address details, chamber of commerce number, etc.
Data space catalogues	A registry to publish and manage the IT resources available within a data space, e.g. data services, data apps and computing resources.
App store	A registry to publish and manage data apps. These can be deployed within a data space connector.
Contract manager	A capability to support the offering of data resources and services under defined terms and conditions which clearly describe the rights and obligations for data and service usage.
Clearing house	A capability to handle all required pre-conditions before (sensitive and/or valuable) data can be shared. Moreover, the clearing house may also register and monitor data sharing transactions, e.g. as input for conflict resolution.
Billing engine	A capability for the billing process associated to data sharing transactions, e.g. generate invoices and manage the payment process.
Data space interconnectivity membership certificate authority	A capability to provide certificates for data spaces participating in the federation of (mobility) data spaces for verifying data space membership in a federation of data spaces.
Dynamic data space attribute provisioning service	A registry to publish and manage the dynamic attributes of the participating data spaces in a federation of data spaces, including the certification status, data space interconnectivity membership status and applicable agreements.
Data space interconnectivity metadata broker	A registry to publish and manage the participating data spaces in a federation of data spaces.
Federated building blocks	The enabling building blocks within a data space that can be federated with the corresponding building blocks in other data spaces based on a full harmonisation mode.
Non-federated building blocks	The enabling building blocks within a data space providing partial harmonisation capabilities to interact with corresponding building blocks in other data spaces.
Data space proxy	The capability to translate between specifications and requirements from a data space to and from the harmonised equivalents for partial harmonisation between data spaces.
Harmonisation profile	The harmonised (technical) protocols used within the harmonisation domain, i.e. to communicate between data space proxies.

Abbreviations

Table 2: Abbreviations

Abbreviation	
AI	Artificial Intelligence
AISBL	Association Internationale Sans But Lucratif
API	Application Programming Interface
BISL	Business Information Services Library
CCAM	Connected, Cooperative and Automated Mobility
CEF	Connecting Europe Facility
C-ITS	Cooperative Intelligent Transport Systems
CSA	Coordination and Support Action
DA	Data Act
DID	Decentralised IDentifier
DIGITAL	Digital Europe Programme
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
DSBA	Data Spaces Business Alliance
DSSC	Data Spaces Support Centre
DTLF	Digital Transport and Logistics Forum
EC	European Commission
EDC	Eclipse Dataspace Components
EDIB	European Data Innovation Board
EDIC	European Digital Infrastructure Consortium
EEIG	European Economic Interest Grouping
eFTI	Electronic Freight Transport Information
eIDAS	electronic identification Authentication and Trust Services
EIF	European Interoperability Framework
EMDS	European Mobility Data Space
eSEAL	Electronic Seal
EU	European Union
EV	Electric Vehicle
GDPR	General Data Protection Regulation
IAA	Identification and Authentication and Authorisation
IDSA	International Data Spaces Association
IoT	Internet-of-Things

ITS	Intelligent Transport System
ICT	Information Communications Technology
IT	Information Technology
KPI	Key Performance Indicator
MaaS	Mobility-as-a-Service
MDMS	Multimodal Digital Mobility Services
MIM	Minimal Interoperable Mechanism
MMTIS	Multimodal Travel Information Services
NAP	National Access Point
NAPCORE	National Access Point Coordination Organisation for Europe
NIS	Security of Network and Information Systems
OASC	Open & Agile Smart Cities
OCI	Open Container Initiative
OEM	Original Equipment Manufacturer
OTM	Open Trip Model
PDS	Personal Data Space
PEPPOL	Pan-European Public Procurement On-Line
PEF	Policy Enforcement Framework
PET	Privacy Enhancing Technologies
PKI	Public Key Infrastructure
RIS (COMEX)	River Information Services (enabled COrridor Management EXecution)
RTTI	Real-Time Traffic Information
SLA	Service Level Agreement
SME	Small and medium-sized Enterprise
SSI	Self Sovereign Identity
SUMI	Sustainable Urban Mobility Indicators
TFEU	Treaty on the Functioning of the EU
TOMP	Transport Operator to Mobility Provider
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-everything
VC	Verifiable Credential
WDO	Workload Deployment Orchestration

I. Introduction

The introduction provides the background and scope of the European Mobility Data Space (EMDS), outlining its ambitious goals and benefits. Additionally, it describes the background, objectives, scope and methodology used in the Digital Europe project PrepDSpace4Mobility. Lastly, it provides an overview of the report's structure to guide readers through the ensuing chapters which include various perspectives, recommendations and building blocks related to the EMDS.

1. Introduction: Background, scope and methodology

1.1. Background

Federated data sharing and data spaces have emerged as key priorities for the European Commission (EC). This is evident through recent initiatives such as the **European Data Strategy**[2], which encompasses pillars like the Data Act (DA)[3] and the Data Governance Act (DGA)[4], alongside complementary efforts such as the Digital Services Act (DSA)[5], the Digital Markets Act (DMA)[6] and the Artificial Intelligence Act[7]. Additionally, the EC is strongly committed to supporting the development of **reference architectures and the deployment and operationalisation of data spaces** in the context of its policy and regulatory initiatives.

The European Union's (EU) Data Strategy sets forth an ambitious vision for federated data sharing, referred to as "**common European data spaces**". Alternatively, it can be conceptualised as a "federation of interoperable data spaces".

Through the establishment of unified and interoperable data spaces across 12 key sectors, the EC aims to address existing legal and technical obstacles to data sharing to unlock the potential for data driven innovation in Europe. These data spaces aim to enable secure and reliable sharing of data throughout the EU, giving businesses, public entities and individuals control over their generated data while ensuring its trustworthy and innovative utilisation. In addition, these initiatives aim to increase data availability and accessibility. Consequently, the creation of these shared European data spaces is expected to fuel the growth of novel data-driven offerings and solutions that is fundamental for the ambition of an EU-wide single market for data.

The **common European Mobility Data Space (EMDS)** is foreseen as one of the sectoral data spaces to be developed in alignment with the broader European ambition. The preparatory action for the data space for mobility (PrepDSpace4Mobility) and its follow-up deployment initiative, both funded under the Digital Europe Programme (DIGITAL), pave the way towards the realisation of the EMDS.

Benefits of the data space concept

A data space is a decentralised infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space. Such an ecosystem allows participants to freely exchange data by adhering to a clear set of rules that protect data sovereignty and guarantee transparency and fairness. A data space does not act as another platform pooling data. Instead, it allows data to remain with the provider, while only metadata or algorithms are shared.

A data space can improve the conditions for **sharing of both open and protected or sensitive data**. For types of data which require protection, data spaces offer the technical means to exchange it in a secure way while enforcing certain usage policies to ensure compliance with whatever restrictions are

[2] European Commission (2020), "A European strategy for data", https://digital-strategy.ec.europa.eu/en/policies/strategy-data.
[3] European Commission (2022), "Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)", COM(2022) 68 final, Brussels.
[4] European Commission (2022), "European Data Governance Act", https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.
[5] European Commission (2022), "European Digital Services Act", https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.
[6] European Commission (2022), "European Digital Markets Act", https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.
[7] European Union (2021), "European Artificial Intelligence Act", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

applicable to them. For data which can be widely shared, e.g. open data, the data space can help to standardise formats and quality, and make the data more accessible and more visible to a wider range of users, while also pooling metadata from different sources.

Data spaces, envisioned as a one-stop shop for data, form a **level playing field in Europe's data strategy**. They facilitate interoperability within a federated network of data ecosystems and services, reducing transaction costs for their participants by centralising metadata visibility (e.g. via a catalogue) and ensuring the interoperability of data formats and interfaces used to exchange data. This level playing field is critical for **fostering new use cases and innovations** in addressing cross-border mobility and logistics challenges. For example, at the intersection of traffic management and private logistics, enhanced data sharing between the public and private sectors across borders, promises significant efficiency gains. Additionally, prioritising interoperability is vital for use cases in the smart city domain that require data sharing from diverse sources spanning various sectors, to enhance urban planning. Whether it pertains to emissions, infrastructure, sensors, or mobile network data, interoperability holds the key to improved urban planning.

Ultimately, **increased interoperability**, **data sovereignty and trust**, as well as the enhanced **discoverability and accessibility** of data contribute to the development of a data economy across borders. Data spaces are conceived as thriving ecosystems that support joint data value creation and hence enable new services, products, businesses, and innovation.

Objectives of the EMDS

Six main objectives for the EMDS have been defined by the EC[8]:

1. "Facilitate the discovery of available data sources, by providing tools for the user to understand the data quality and related access conditions.
2. Identify essential data and increase their availability to support services considered crucial across the EU's territory covering themes from sustainability to multimodality.
3. Facilitate data access and re-use through the modal and cross-modal harmonisation of sharing conditions in a fair, transparent, proportionate and non-discriminatory manner.
4. Enable technical, organisational and legal interoperability for data access, re-use and data sharing. This should be enabled between various public and private actors, data intermediaries and data sources, through the deployment of use cases. These use cases should be based on voluntary common recommendations and frameworks addressing data semantics, technical protocols, business processes and governance structure, in coherence with the new and emerging EU data-related legislation and in compliance with data protection rules.
5. Optimise data collection and reduce administrative burden, through identifying gaps and overlaps in existing data collection arrangements and making recommendations for respective adjustments in sectoral legislation.
6. Facilitate interoperability with other common European data spaces and allow data sharing and re-use among those in line with new and emerging EU data-related legislation."

1.2. Project objectives

PrepDSpace4Mobility supports the EC's initiative on a common EMDS as part of the overarching ambition to create common European data spaces as expressed in the European Data Strategy[2]. This collaborative initiative encompasses various aspects of mobility, including (1) **personal mobility**, (2) **logistics** and (3) **Cooperative, Connected and Automated Mobility** (CCAM).

[8] European Commission (2022), "Transport data - creating a common European mobility data space (Communication)", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Transport-data-creating-a-common-European-mobility-data-space-communication-_en.

General and specific project objectives

The PrepDSpace4Mobility project has two general objectives[9]:

1. To **contribute to the further development** of the common European mobility data space announced in the Data Strategy and in the Sustainable and Smart Mobility Strategy, built and operated in full compliance with existing EU legislation in the mobility and transport sectors.
2. To **support the creation of a technical infrastructure** combined with governance mechanisms that will facilitate easy, cross-border access to key data resources in this area. This will be achieved on the basis of and in full alignment with existing and upcoming mobility and transport initiatives (some of which are regulated) that organise the sharing of data for passengers and freight and form an integral part of the emerging European data and cloud services infrastructure.

To address these two general objectives, the PrepDSpace4Mobility action has three specific objectives:

1. To **support the ongoing Commission initiative** launched on the common European mobility data space, in particular:
   - Making an inventory of existing data platforms and marketplaces ("data ecosystems") and providing a catalogue of transport data eco-systems;
   - Identifying gaps and overlaps of data currently covered (or not covered) by existing initiatives;
   - Identifying common building blocks which could contribute to the long-term convergence of existing and new data-related initiatives in transport and explore possible options for suitable frameworks for sharing and managing data exchange across existing and emerging data initiatives in the mobility sector;
   - Identifying opportunities for integrating the EMDS and/or data ecosystems in the emerging European data and cloud services infrastructure.
2. To **work in liaison with the Data Spaces Support Centre** and the Alliance for Industrial Data, Cloud and Edge, and to ensure alignment with the European Data Spaces Technical Framework and with the rest of the ecosystem, notably concerning common tools such as:
   - A data space reference architecture, building blocks, common toolboxes and common standards for cloud services;
   - Data governance models, business models and strategies for running data spaces, with the aim to recommend possible common tools, building on existing data ecosystems.
3. To **exploit, disseminate and communicate** the preliminary and final project results.

Target audience and transfer of results

Various (mobility) data space development and deployment initiatives contribute to the overarching ambition of the common European data spaces, as expressed in the EU Data Strategy[2]. These initiatives constitute the primary target for this deliverable.

At the EU level, several actions are in place to support the establishment and development of common data spaces (Figure 1).

[9] EC Directorate-General for Communications, Networks, Content and Technology (DG CNECT) (2022), "Project 101083655 - Grant Agreement".

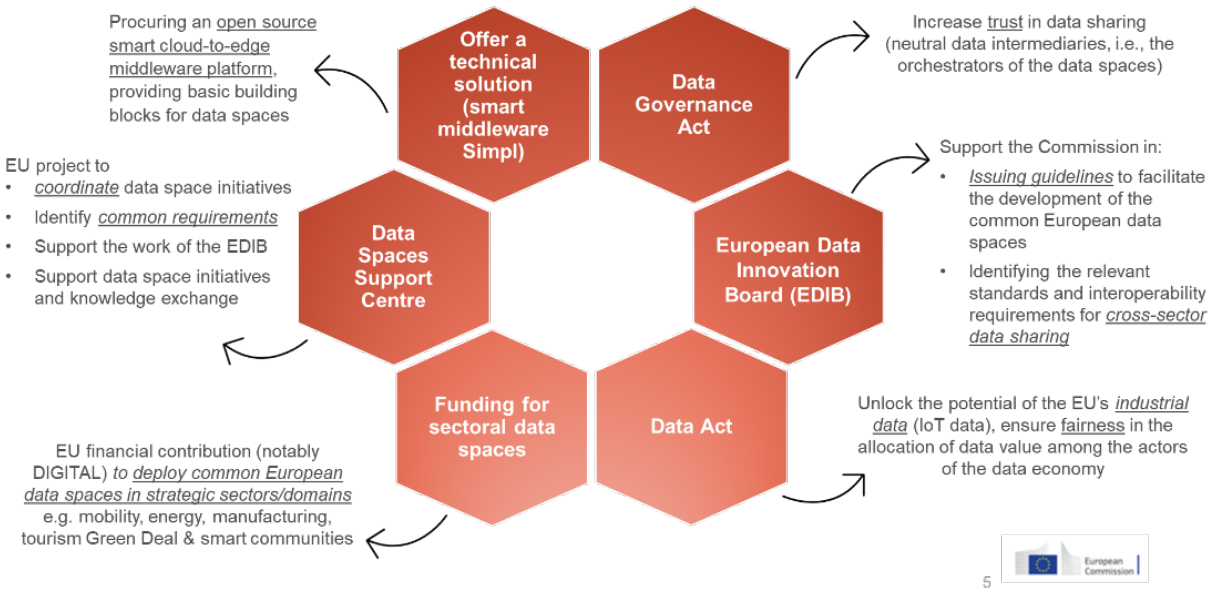


Figure 1: EC's actions supporting European common data spaces.[10]

The project results will primarily be directed towards the EU initiatives supporting the deployment of common European data spaces that focus on the technical aspects as illustrated in Figure 1, i.e.:

- Actions in the context of the EMDS encompassing the preparatory action (PrepDSpace4Mobility), an EC funded Technical Support Action, and a follow-up deployment project under DIGITAL, expected to start in November 2023.
- The **Data Spaces Support Centre (DSSC)**[11]: Funded under Digital Europe, the DSSC aims to facilitate the creation of common data spaces that collectively establish an interoperable data sharing environment in Europe. The project is scheduled to run from October 2022 until March 2026.
- The **EU SIMPL procurement initiative**[12] : This initiative procures the open source development of the Smart Middleware building blocks. These building blocks are intended to enable cloud-to-edge federations and provide support for all major data initiatives funded by the EC, such as the common European data spaces.
- The **European Data Innovation Board (EDIB)**[13]: The EDIB will advise the EC on issuing guidelines to facilitate the development of common European data spaces and the identification of the relevant standards and interoperability requirements for cross-sector data sharing. The EDIB's scope includes data intermediation, data altruism and the use of public data that cannot be made available as open data, while prioritising cross-sectoral interoperability standards. The EDIB will be supported by the DSSC. The EC will remain the ultimate decision-making authority.
- **European Digital Infrastructure Consortium (EDIC)** initiatives[14]: A new legal framework for multi-country projects.

[10] EU PrepDSpace4Mobility CSA (2023), "First Public Stakeholder Forum", https://mobilitydataspace-csa.eu/wp-content/uploads/2023/03/psf-28february.pdf.
[11] Data Spaces Support Centre (2023), "Data Spaces Support Centre (DSSC)", https://dssc.eu.
[12] EU Digital Europe Program, (2023) "SIMPL: cloud-to-edge federations and data spaces made simple", https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple.
[13] European Commission (2023), "Data Governance Act explained", https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.
[14] European Commission (2023), "Policy Programme: Path to the Digital Decade – Questions and Answers", https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_4631.

- **National, regional or local data space initiatives:** Such initiatives in mobility and logistics that are in the process of setting up or scaling.

1.3. DSSC taxonomy of building blocks

The results of PrepDSpace4Mobility are embedded in a wider context of EU initiatives promoting data sharing interoperability. The concept and approach for federated data sharing, data spaces and the common European data spaces are currently under development. Several reference architecture initiatives (e.g. International Data Spaces Association [IDSA], Gaia-X[15], iSHARE[16], and the Data Spaces Business Alliance [DSBA][17]), building block initiatives (e.g. FIWARE[18], Connecting Europe Facility [CEF] Digital[19], and EU Directorate-General for Informatics building blocks[20]), and further EU flagship initiatives (e.g. DSSC, SIMPL[21], and the EDIB[22]) are evolving. As a result, reference guidelines and interoperability standards for individual data space instances (i.e., **intra data space interoperability**) and for connectivity between multiple data space instances (i.e., **inter data space interoperability**) are still being agreed upon and standardised.

It is important to acknowledge that technically specifying the individual building blocks and setting the standards exceeds the feasibility and scope of the PrepDSpace4Mobility action. In fact, attempting to do so solely from the perspective of EMDS would significantly hinder the efforts of current and upcoming EU initiatives which play a crucial role in defining the blueprint, establishing agreements and setting standards for federated data sharing across a variety of sectoral data spaces. These initiatives are also responsible for addressing the identification, specification and development of associated building blocks and ensuring their interoperability and federation.

It is, therefore, vital that data spaces are developed from a common and "federation/ interoperability" perspective. This is also acknowledged by the DSSC in their forthcoming report on **data space synergies** which elaborates on the pivotal role these synergies play in the vision and development of European data spaces and data markets:

"Synergies represent the interaction and cooperation among data spaces, resulting in a collective impact greater than the sum of individual parts. Data spaces can be nested and overlapping, enabling multiple layers of data sharing and facilitating the implementation of diverse use cases. Synergies are essential for enabling and facilitating the development and coexistence of multiple data spaces, ultimately realising the envisioned benefits for individuals, society, and businesses". From the synergies perspective, the implementation of a data space should "use common building blocks whenever possible. Aligning the technical planning and development with DSSC blueprint building blocks would be recommended, as would sourcing available open source implementations […] as one of the main drivers for trustworthiness and a way to avoid lock-in effects."[23]

---

[15] EU Gaia-X Initiative (n.d.), "Gaia-X: A Federated and Secure Data Infrastructure", https://www.gaia-x.eu.
[16] iSHARE Foundation (n.d.), "iSHARE – Trust Framework for Data Spaces", https://ishare.eu.
[17] Data Spaces Business Alliance (n.d.), "The Data Spaces Business Alliance. Unleashing the European Data Economy", https://data-spaces-business-alliance.eu/.
[18] FIWARE Foundation (n.d.), "FIWARE Catalogue", https://www.fiware.org/catalogue.
[19] European Commission (n.d.), "Connecting Europe Facility - CEF Digital", https://digital-strategy.ec.europa.eu/en/activities/cef-digital.
20 European Commission (n.d.), "Directorate-General for Informatics - DIGIT", https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics_en.
[21] European Commission (2023), "SIMPL: cloud-to-edge federations and data spaces made simple", https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple.
[22]European Commission (2023), "Data Governance Act explained", https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.
[23] Data Spaces Support Centre (2023), "Data Spaces' Synergies", forthcoming.

The EU-funded DSSC currently functions as an umbrella, harmonising the work of various sectoral common European data space initiatives. Hence, where applicable, the **DSSC glossary**[24] and **taxonomy of building blocks**[25] (Figure 2) are used throughout this report. The DSSC glossary and taxonomy build and extend upon the Open DEI[26] soft infrastructure, which consists of 12 building blocks[27].

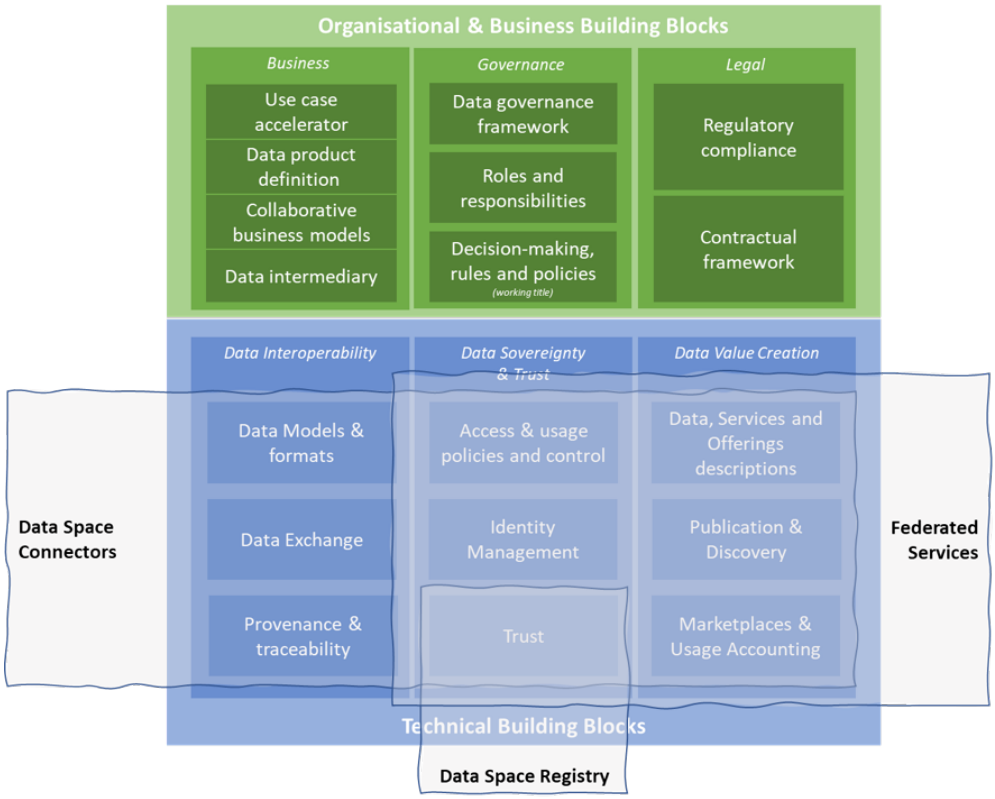


Figure 2: The DSSC taxonomy of building blocks.

The DSSC glossary mainly refers to a data space building block as an asset, defining it as a "basic unit or component that can be implemented and combined with other building blocks to achieve the functionality of a data space".

The DSSC taxonomy distinguishes between two categories of building blocks:

- **Organisational and business building blocks**: These relate to business models of data spaces, the governance of data spaces and the legal frameworks for data spaces.
- **Technical building blocks**: These relate to the technical aspects and technical agreements that individual data space participants and trusted intermediaries need to adhere to.

The EC's Digital Europe Programme refers to technical building blocks as "open and reusable digital solution[s]. [They] can take the shape of a framework, a standard, a software, or a software as a service (…), or any combination thereof."[28]

[24] Data Spaces Support Centre (2023), "DSSC Glossary", https://dssc.eu/wp-content/uploads/2023/03/DSSC-Data-Spaces-Glossary-v1.0.pdf.
[25] Data Spaces Support Centre (2023), "DSSC Blueprint for Data Spaces. Taxonomy of Building Blocks"". Paper in preparation.
[26] EU Open DEI project (n.d.), "Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry", https://www.opendei.eu.
[27] EU Open DEI project (2021), "Design Principles for Data Spaces. Position Paper", https://design-principles-for-data-spaces.org.
[28] See European Commission (2023), "Digital Europe: eIDAS enablers. Give your digital project a boost", https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Homepage.

In addition, the technical building blocks will require "**Technical Grounding**", which involves their implementation in software or services intended for use in a data space and the federation of data spaces. The technical services (as framed by the DSBA[29]) encompass three main categories:

- **Data space connectors** serving as secure gateways, enabling systems and organisations to access a data space securely;
- **Federated services** offering various functionalities, such as validation or cataloguing of services;
- **Data space registries** registering the participants of a data space.

Technical grounding is further addressed in Chapter 6.

The upcoming DSSC synergies report[23] further introduces the terminology of "non-operational common building blocks", such as design frameworks and blueprints, open standards, open source software, legal and business templates, contractual templates, business planning tools (e.g. the use case accelerator), and other technology assets.

This report adopts the definition of a building block from the DSSC taxonomy allowing it to include both technical assets and organisational, business and non-operational capabilities. Moreover, the term "building block" is used for any capability or activity that contributes to the development, deployment, and evolution of the mobility and logistics sector towards the EMDS, in alignment with the overarching ambition of the common European data spaces.

1.4. Methodology

The methodology of this report combines various approaches to effectively gather and analyse relevant data and insights from different stakeholder groups active in the mobility and logistics domain. The following list provides an overview of the actions conducted, alongside their objectives:

- **Inventory:** An extensive inventory of existing data sources and data sharing initiatives was conducted first to understand the current landscape of mobility and logistics data. This inventory included internet links, contacts, geographical coverage, and distinctions in data availability between private and public entities.
- **Survey:** Questionnaires were distributed to data ecosystems and other stakeholders to collect information on data gaps, overlaps, existing data sharing initiatives, usage and need of building blocks, and expectations or requirements related to the EMDS.
- **Expert workshops using interactive live questionnaires and discussions:** Innovative tools such as Menti, Padlet and Google Jamboard were used during and after expert workshops. They facilitated interactive live surveys and discussions to validate assumptions and findings.
- **Interviews:** Selected stakeholders, initiatives and other Coordination and Support Actions (CSA) relevant to the EMDS were interviewed to gain deeper insights into data sharing challenges and perspectives.
- **Calls for inputs:** These were circulated via LinkedIn and email to data ecosystems included in the inventory, thereby providing stakeholders with opportunities to share further information and express requirements during individual calls.
- **Working group meetings:** These focused on the organisational and technical building blocks of the EMDS as defined in the DSSC taxonomy (Figure 2).
- **Expert opinions:** Inputs from project partners, external experts, advisory boards and external reviewers contributed to the analysis, leveraging their wide range of knowledge and experience in data sharing initiatives.

[29] Data Space Business Alliance (2023), "Technical Convergence. Discussion Document", Version 2.0, https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.

- **Alignment and Review:** Alignment sessions were conducted in collaboration with the Data Spaces Support Centre and the Alliance for Industrial Data, Cloud, and Edge. Additionally, this report was reviewed by several experts and initiatives (see Acknowledgements), ensuring alignment with best practices in the field.

Consultation activities

Various consultation activities were planned throughout the project´s duration to ensure meaningful data collection to assist in the analysis. A combination of quantitative and qualitative data collection activities, including questionnaires, interviews and workshop, was used. This section provides an overview of the different primary data collection activities.

Survey

In the first few months, the project team designed and developed questionnaires as part of a survey involving a broad set of stakeholder groups active in various mobility and logistics application domains. The questionnaires addressed 1) data sources provided and required, as well as 2) characteristics and needs of data sharing initiatives to aid in the identification of organisational, business, and technical building blocks. The questionnaire was launched in March 2023 and concluded in July 2023[30]. A total of 63 different organisations submitted responses. The questionnaire on data sources provided and required yielded 51 responses, and the questionnaire on data sharing initiatives 38 responses, respectively.

The mobility sector was categorised into 18 individual thematic categories representing use case clusters. Specific functional building blocks and possible gaps are easier to identify at this level. Table 3 shows these thematic clusters and describes the meaning of data sharing and interoperability in these areas:

Table 3: Identified thematic categories of the mobility sector.

Thematic category	Description
Public transport	Building blocks for interoperability in public transport enable better planning, management and optimisation of services, as well as improved passenger information and multimodal integration. Data sources include ticketing systems, vehicle location systems, sensors and user feedback.
Individual transport	Data provision in individual transport allows for more personalised and efficient mobility solutions, such as navigation, parking, insurance, maintenance as well as connected and automated driving. Data sources include vehicle, smartphone and road infrastructure data.
Shared mobility	In shared mobility, data availability facilitates the provision and use of mobility services that are shared among multiple users, such as carsharing, bike-sharing, ridesharing and ride-hailing. Data sources include service providers, users and platforms.
Electric vehicles and charging	Sharing data concerning electric vehicles and charging enables the development and deployment of electric mobility solutions that are integrated with other modes of transport and energy systems. Data sources include vehicle batteries, charging stations, grid operators and energy markets.
Multimodal Mobility in smart cities incl. smart parking	The provision of data for mobility in smart cities supports the creation and implementation of smart mobility policies and initiatives that aim to improve urban mobility performance, sustainability and liveability. Data sources include

[30] To attract additional responses, the survey was relaunched during the summer. The first period ran from March 2023 to June 2023. The second set was disseminated during the months of June and July 2023.

Thematic category	Description
	urban sensors, cameras, traffic lights, public transport systems and citizen participation platforms.
On-demand mobility	The availability of data in on-demand mobility allows for the provision and use of mobility services that are customised to meet the specific needs and preferences of users. These services include taxi services, ride-hailing services and microtransit services. Data sources for these services include service providers, users, platforms and regulators.
Mobility-as-a-Service (MaaS)	MaaS data availability allows for the provision and use of mobility services that offer a single digital platform for multiple modes of transport. Data sources include MaaS operators, transport providers, users and authorities.
Vehicle data	Vehicle data availability enables the collection and analysis of data generated by vehicles or related to vehicles, such as location, speed, fuel consumption or diagnostic data. Data sources include vehicle sensors, telematics devices, onboard computers or smartphones.
Cooperative, connected and automated mobility (CCAM)	CCAM focused on enhanced road and vehicle safety by exchanging information between vehicles and the road infrastructure. Although most use cases relate to direct message exchange via broadcast, there are some use cases that involve information exchange via backend systems and cloud services that might be relevant for mobility data spaces as well. E.g.: • Vehicle-infrastructure real-time safety and traffic data, • Cloud service for vehicle-infrastructure real-time safety and traffic data, • Cloud services for vehicle-to-X real-time sensor data, • Cloud services for navigation and traffic data (semi)static, • Cloud services for live traffic and safety data • Cloud services for road operator traffic and safety information • Urban Data Access Platform real-time traffic light data
Road transport	Data about road transport enables the collection and dissemination of information related to road conditions, traffic flows, incidents or events that affect road mobility. Data sources include road sensors, cameras, traffic management centres or road users.
Road operator information: static and dynamic	Data about road operator information enables the collection and dissemination of information related to road infrastructure characteristics or operations that affect road mobility. Static information includes road network geometry, topology or attributes. Dynamic information includes road works, tolling schemes or speed limits. Data sources include road operators, authorities or service providers.
Rail transport	Rail transport information enables the collection and dissemination of information related to rail infrastructure, services or operations that affect rail mobility. Data sources include rail operators, authorities or service providers.
Air transport	Data availability in air transport enables the collection and dissemination of information related to air infrastructure, services or operations that affect air mobility. Data sources include air operators, authorities or service providers.
Inland waterway freight transport	Data availability in inland waterway freight transport enables the collection and analysis of data related to the movement of goods by inland waterways, such as rivers, canals or lakes. Data sources include vessels, terminals, locks or cargo owners.
Maritime freight transport	Data in maritime freight transport is used to collect and analyse data related to the movement of goods by sea. Data sources include ships, containers, ports or cargo owners.

Thematic category	Description
Logistics	Logistics data is used to collect and analyse data related to planning, execution, and control of the flow of goods and services from origin to destination. Data sources include supply chain actors, transport modes, warehouses or customers.
Sustainable Urban Mobility Indicators (SUMI)	SUMI data is used to collect and analyse data related to the performance and impact of urban mobility systems on various dimensions, such as accessibility, safety, environment or social inclusion. Data sources include authorities, operators, users or surveys. The SUMI are currently under revision.
Geospatial data	Geospatial data is used to collect and analyse data related to the location and attributes of geographic features or phenomena that affect mobility, such as roads, buildings, landmarks or weather. Data sources include satellites, drones, maps or sensors.

Interviews

To complement the questionnaire, interviews were conducted with stakeholders from 21 key data sharing initiatives in the field of mobility and logistics as listed in Table 4, as well as with four other CSAs as listed Table 5 below.

Table 4: Interviewed initiatives and stakeholders in alphabetical order.

Organisation/initiative
Digital Container Shipping Association
Digital Infrastructure for Logistics
Digital Transport and Logistics Forum (DTLF); FEDeRATED
E015 Digital Ecosystem Lombardy
ENTUR
European Federated Network of Information eXchange in LogistiX (FENIX)
electronic Freight Transport Information (eFTI)
ITxPT
FinTraffic
Global Data Service Organisation for Tyres and Automotive Components
MobiData BW
MobiData Lab
Mobility Data Space (MDS)
MinervaS
National Access Point Coordination Organisation for Europe (NAPCORE), Working Group 1
Nationaal Dataportaal Wegverkeer
NordicWay
Norwegian Public Roads Administration vegvesen
Rail Net Europe
TÜV Rheinland
ZF Friedrichshafen AG

Table 5: Consulted CSAs preparing sectoral European data spaces, in alphabetical order.

Name of CSAs
Data Space for Tourism
Data Space for Smart and Sustainable Cities and Communities
Green Deal Data Space (GREAT)
Int:net project, Energy Data Cluster

Expert workshops

To actively engage with the mobility and logistics community, four expert workshops were organised within the framework of the PrepDS4Mobility project. These workshops aimed to collect insights from a diverse group of stakeholders involved in the mobility and logistics domain, often focusing on specific application domains.

- The **first expert workshop** was hosted by FIWARE on January 31, 2023, with a total of 149 attendees.
  In this first workshop, the main objective was to share the proposed methodology for analysing a common EMDS approach. The workshop primarily targeted stakeholders within the EU's mobility and logistics sector, welcoming a broader audience interested in EMDS developments. Insights and queries were used to refine the methodological approach and gather input on ongoing data sharing initiatives.
- The **second expert workshop** was hosted by ERTICO on May 10th, 2023 with a total of 195 attendees.
  The main objective of this workshop was to gather necessary input from stakeholders, with a particular focus on the communities in sustainable and clean mobility, CCAM, urban mobility, and logistics. Topics were categorised in four areas: data needs, technical needs, operational necessities, and governance needs. The aim was to acquire insights from current experiences crucial for a common EMDS.
- The **third expert workshop** was hosted by FIWARE on May 30th, 2023, with a total of 98 attendees.
  The workshop's main objective was to collect evidence from stakeholders involved in the wider mobility and logistics domain, with a particular focus on those with an expertise or experience in data provisioning, usage, or sharing. Apart from gathering input on data needs and use cases, this workshop provided an opportunity to gather insights on crucial organisational, business, and technical characteristics vital for the functioning of an EMDS.
- **The fourth expert workshop** was hosted by ERTICO on July 14th, 2023, with a total of 111 attendees.

In this final workshop, evidence was predominantly collected from stakeholders associated with map update exchange, road safety, MaaS, and traffic management. These topics were further divided into business models, governance and legal aspects, and technical building blocks. Similar to the first workshop, experiences from the mentioned application domains, insights into their current experiences related to the topics, and thoughts concerning a common EMDS were gathered to provide input.

Limitations

It is important to recognise potential limitations in participation representation across EU countries and within the mobility sectors during the consultation activities. Despite these disparities, efforts were made to ensure that insights derived from the study could still be generalised to benefit the analysis. Careful note was taken of the challenges posed by the substantial numbers of unanswered questions in the questionnaires.

Opportunities for improvement were identified in data collection methods, including suggestions to enhance the number of respondents and increase coverage in EU countries. Alternative formats, such as expert interviews, were explored to gather more in-depth information, which required significant time and effort to ensure a wide variety of interviewees.

Several limitations with regard to the analysis should be noted:

- The representation of Western European countries was predominant compared to other EU regions. Despite this disparity, insights derived from this analysis remain relevant and applicable within the scope of identifying data needs and common strategies to overcome data gaps. The prevalence of initiatives from Western European countries in the analysis is largely due to the presence of specific advanced projects and widespread adoption of data sharing practices in these regions. Selected lighthouse projects exemplify sturdy frameworks and firmly established collaborations. It is expected that the insights gathered from these advanced contexts will provide a strong foundation for the evolving landscape in other regions, guiding them as they embark on similar initiatives. Additionally, initiatives such as NAPCORE that are inherently international and encompass interests from across Europe have also been included in the analysis.
- There was a noticeable skewed distribution in terms of organisational roles and the proportion of public versus private entities that participated in the questionnaires and workshops. Specifically, the organisational roles of data sharing initiative and the public sector[31] were overrepresented, while data providers[32] were slightly underrepresented. Additionally, a disparity in the mobility sector should be taken into account. Respondents active in the personal mobility domains and their related data sources that are provided (such as public transport, multimodal mobility, etc.) are slightly overrepresented compared to CCAM, logistics or other domains[33]. This could introduce biases in the findings, as certain perspectives and data from underrepresented sectors might not have been adequately captured.
- In the initial phase, the project received a total of 22 questionnaire responses regarding data source needs that fed into the analysis of data sources gaps and overlaps. In order to amend and clarify the requirement and insights derived from this questionnaire, two supplementary activities were launched: First, additional attention was paid to further stakeholder consultation activities, such as interviews and expert workshops. Simultaneously, a second shortened questionnaire was issued resulting in 29 usable responses that relate to the data sources gaps and overlaps. The two questionnaires (1A and 1B in the first and 1 in the second phase) shared 7 comparable questions as well as unique ones (five in the first questionnaire and four in the second). Upon analysis, it was observed that similar results were obtained from identical questions in both questionnaires. Consequently, statements and recommendations are presented across both questionnaires based on these identical results. In cases where unique insights emerged, they are discussed separately and are always accompanied by a note indicating the number of responses underlying the analysis.

[31] In the first questionnaire (N=22), public organisations represented 48%, private organisations 19%, non-profit organisations 19%, and 14% identified as other. In the second questionnaire (N=29), public organisations accounted for 59%, private organisations 21% and non-profit organisations for 17%, while 3% accounted for other (i.e. organisation for academic research).

[32] In the first questionnaire (n=22), 19% identified as data source providers, 67% are active in a data sharing initiative as enablers, software providers or platform providers; and 14% identified as other. In the second questionnaire (n=20), 22% identified as data source providers; 58% identified as enablers, software provider or platform providers, 15% as data consumer and 5% as other (i.e. academic research partner, living lab operator).

[33] In the second questionnaire related to application area (n=20), logistics represented 30%, CCAM 30%, personal mobility 20%, and another 20% as other.

To ensure a comprehensive understanding of the mobility data landscape across all sectors, it is essential to be mindful of these limitations when interpreting the results.

1.5. Structure of the report

This report summarises the project's work on:

- Identifying gaps and overlaps of data currently covered (or not covered) by existing initiatives;
- Identifying common building blocks for a future common EMDS;
- Identifying opportunities for integrating the EMDS and/or data ecosystems in the emerging European data and cloud services infrastructure.

The report is structured into four main parts:

- **Mobility and logistics data requirements**
  This part covers the results of the data source analysis, including data gaps and overlaps, as a prerequisite for making a variety of data sources available and supporting multiple types of data sharing.
- **Organisational and business building blocks**
  This part addresses the three pillars of the DSSC organisational and business building blocks: business, governance and legal. Additionally, it includes funding models as part of the business building blocks.
- **Technical building blocks**
  This part addresses the three pillars of the DSSC technical building block: data interoperability, data sovereignty and trust, along with data value creation. The part begins with a chapter on "Technical Grounding", presenting the common architecture and building blocks for the common European data spaces within the DSSC blueprint and SIMPL procurement initiatives.
- **Reference architectures, alignment and conclusions**
  The concluding part of the report provides reference architectures for (a) individual mobility data spaces (intra data space interoperability) and (b) for interconnecting multiple mobility and logistics data spaces (inter data space interoperability). It identifies aspects for further alignment with leading EU initiatives on data spaces, and with edge and cloud developments. The section concludes by providing an overarching summary, along with considerations for the operationalisation of the EMDS.

II. Mobility and logistics data requirements

This part examines existing practices in mobility data sharing and pinpoints gaps and overlaps in data availability. It further identifies the common practices and needs of the mobility sector, which may serve as a basis for determining requirements for the development of the EMDS.

2. Gaps and overlaps in mobility data sharing

2.1. Introduction

This chapter illustrates current data availability and addresses gaps and overlaps regarding data sources and data sharing in mobility and logistics. While the inventory encompasses existing data sharing initiatives[34], this chapter addresses the current gaps and overlaps in three areas: a) identifying the data sharing types and data sets that should be prioritised, b) assessing challenges related to data availability and data reliability, and c) exploring the hurdles preventing stakeholders to engage in data sharing.

There are several aspects related to mobility-related data gaps that can be observed. These aspects include:

- **Availability** of data, which relates to coverage per application domain and the degree of granularity;
- **Reliability**, which links to the quality and consistency of the data made available;
- **Accessibility,** which relates to how data can be accessed and used collectively (e.g. not following a standardised format makes data less accessible).

Overlaps in mobility-related data can represent either duplications or opportunities to enhance synergies. It is important to acknowledge that, due to evolving data needs in mobility, and it is difficult to firmly determine the gaps and overlaps.

Despite recent progress in data set provision and the support of various EU initiatives promoting data sharing (e.g. NAPCORE and the Digital Transport and Logistics Forum), there remains a pressing need for additional advancements in the availability, reliability, and accessibility of mobility-related data. Against this context, this chapter provides specific recommendations, thereby contributing to the ongoing dialogue on data sharing and the design of foundational elements for a common EMDS.

The chapter does not provide an exhaustive overview of data on a per-country or per-sector basis (e.g. logistics, personal mobility, CCAM, maritime, etc.). Instead, its purpose is to highlight general trends and patterns. The EMDS should not solely focus on addressing specific data gaps, as there are already numerous initiatives, associations, and entities actively involved in data collection, harmonisation, sharing, and analysis covering specific sub-domains of mobility. Rather, the primary objective of the EMDS should be to establish a mutual collaborative framework that is widely embraced and build on existing standardisation efforts in the different sub-sectors of transport.

Section 2.2 presents the insights on data sharing and data set availability resulting from engagements with public and private stakeholders. Section 2.3 addresses the key challenges for data availability and reliability, based on the gaps in data needs and overlaps within the mobility and logistics domain that have been identified. Finally, Section 2.4 provides recommendations on data availability.

2.2. Identifying priority data sharing types and data sets

This section presents insights gathered from public and private stakeholders regarding data sharing and data set availability. The analysis identifies key themes concerning the availability, accessibility, and usability of mobility- and logistics-related data sources across various application domains. It further distinguishes between identifying common gaps that require consideration and resolution in these fields, along overlaps that point to opportunities for convergence within a common EMDS.

[34] EU PrepDSpace4Mobility CSA (2023), “Data Ecosystems Inventory”, https://mobilitydataspace-csa.eu/inventory.

Data sources provided

Responses to the project's survey reveal variation in data provisioning across application domains, with some domains more strongly represented than others (Figure 3). The analysis indicates that data sets related **to movement of persons, goods, and vehicles** are of high importance for respondents' activities. However, respondents tended to be less active in providing transport-related data sources, such as those related to inland waterway freight transport, air transport and operation services (. Operational data related to e.g. freight navigation- and travel management services, fleet management and goods). As well as data related to relative newer mobility concept such as on-demand mobility and shared mobility. Data related to sustainable urban mobility indicators are also limited in terms of provisioning. While those data sets are valuable for certain applications within the mobility sector to calculate specific impacts (e.g. environmental impact assessments, affordability and accessibility of public transport), the immediate and direct relevance of movement-related data makes it a primary focus for many stakeholders. Certain data sources (e.g. geospatial data) have the potential to become more accessible for the mobility domain with the linkage of different sectoral data spaces at EU level, notably with the Green Deal data initiatives.

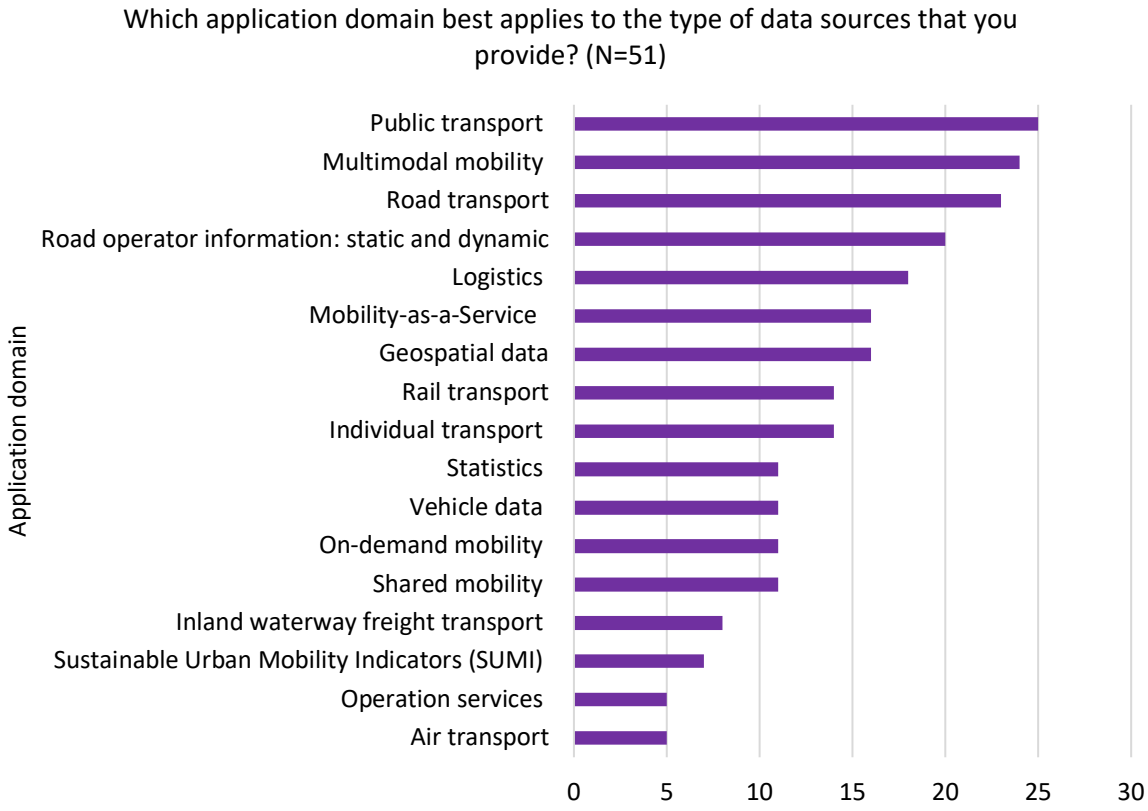


Figure 3: Types of data sources provided by respondents.

Data gaps identified

Evidence was collected from inventoried data ecosystems and other stakeholders to identify data needs and assess their prioritisation based on feedback from the questionnaires and several workshops. This process aimed to understand the significance of different data types for various business cases, highlighting areas where data availability was lacking yet considered essential for creating value. Primary data needs were determined by the frequency of mentions by stakeholders and their associated application domains. An overview of the variety of required data sources is presented in Table 6. Additionally, findings from questionnaire responses and stakeholder consultations reveal instances of use cases that require data sources which are currently inaccessible.

Table 6: Overview of identified use cases and their required data sources.

Examples of use cases mentioned	Additional data source types indicated as not attainable	Specificities, if any
Monitoring sustainable urban mobility	Emissions data	Emissions on vehicle level
Improving city authorities' operational picture of the usage of their urban environment	Shared mobility data	Real-time location and availability of car sharing data
Last mile delivery of consumer products in an urban environment	Last mile delivery data	
Urban traffic and perturbation in real time	Real-time transit data	
Improved count of diversity of traffic on cross-roads	Vehicle type, pedestrian and cyclist flows	• Real-time vehicle detection and count • Speed estimations
Identifying optimal locations for Electric Vehicle (EV) charging points	E-mobility infrastructure data	• Location of charging points for EV • Charging event of charging points
Improved multimodal offerings	Payments and ticketing information data	Ticketing information
Multimodal/Intermodal routing	Real-time data of public transport; information on interlinking between modes of transport (people, freight); harmonised (data pool for) public transport timetable data	Combined trip information of modalities
Smart traffic management systems	Real-time use of the road network	• Traffic volume • Traffic speed • Travel times
Determining attributes of vulnerable road users for improved object recognition	Vulnerable road users counts and accompanying infrastructure conditions.	• Improved quality and coherence of speed limit ranges, areas, junctions, carriageways, and lighting conditions. • Improved coherence in characteristics of types of vulnerable road users (e.g. non-motorised, motorcyclists, persons with disabilities or with reduced mobility and orientation)
Improved safety of road design	In-vehicle data, traffic safety related data	• Self-driving or driver assistance capabilities of vehicle • Mixed traffic situations.

Examples of use cases mentioned	Additional data source types indicated as not attainable	Specificities, if any
Cross-border transport planning and operations	Cargo data	• Travel times • Cross border delays • Cost-effective routes • Transported goods
Calibration of traffic models	Historical and real-time data	• Different types of modes (pedestrian, cycling, micro-mobility) • Disruptions • Information from journey planners (planned, booked and executed trips)
Digital train operations in cross-border traffic	Real-time data on movement of trains for national and cross-border traffic	Operational real-time data on movement of trains for both passenger and freight transport

Indeed, there is a wide array of data needs, given that various stakeholders **necessitate specific data types** to tackle their unique challenges and optimise their operations. Data unavailability manifests in various scenarios, for instance:

- Lack of road sensor data for situational awareness of vehicles and communication among different connected vehicles;
- Lack of multimodal trip data inhibiting understanding of interconnected transport modes both for passengers and for freight, complicated by the separate organisation of transport modes;
- Lack of road infrastructure conditions such as safe cycling paths and their conditions;
- Restricted access to the number of public transportation users due to data sensitivity and privacy concerns.

These needs vary greatly depending on the objectives within a specific application domain (see Box 1 for an example on the Sustainable Urban Mobility Indicators [SUMI]). This heterogeneity underscores the diverse needs among mobility actors and necessitates careful design in EMDS building blocks.

The Sustainable Urban Mobility Indicators (SUMI) were developed as part of an EU project spanning from 2017 to 2020, coordinated by Rupprecht Consult. The initiative involved a testing phase conducted across several cities. During this testing phase, it became evident that some of the indicators imposed a significant burden on cities, requiring extensive raw data for accurate calculation. Notably, smaller cities faced considerable challenges in calculating these indicators due to data availability issues. To mitigate this, proxy data or adapted existing data could be used for the SUMI indicator calculations if the necessary data was lacking or insufficient. Overall, there exists a notable gap between the data needed for SUMI calculations in cities and the available data sets at the city level.

There is an ongoing revision of SUMI as part of a follow-up project. This endeavour aligns with the activities stipulated in Article 40 of the proposed Trans-European Transport Network Regulation (COM(2021) 812 final of 14.12.2021). The Commission aims to adopt an implementing act defining the methodology for collecting indicator data. This methodology will encompass critical areas such as greenhouse gas emissions, congestion, accidents and injuries, modal share, and access to mobility services, as well as data on air and noise pollution.

The EMDS deployment initiative funded under DIGITAL starting in November 2023 includes activities for enabling the sharing, availability, and reuse of data for SUMI. This approach integrates the experience and recommendations gleaned from PrepDSpace4Mobility. Additionally, the project

offers valuable opportunities for the integration of more urban or regional data ecosystems, representing a crucial step towards enhancing data visibility and accessibility throughout Europe[35].

Box 1: Example: Sustainable Urban Mobility Indicators (SUMI).

Data sharing types

The array of stakeholders providing supporting evidence within this project include public transportation companies, logistics service providers, government agencies, urban planners, service providers, academia, research institutes, technology providers, and several more. During the project's first expert workshop, these experts were presented with the question, "Which of the following paradigms of data sharing should be supported in data spaces?". Participants were afforded the opportunity to select multiple responses:

- Bilateral sharing of messages (e.g. notifications, request/replies);
- Algorithm sharing for local processing of (sensitive) data (e.g. to support Privacy enhancing Technologies);
- Bilateral sharing of persistent (semi-static) data (e.g. transactional data);
- Multilateral sharing of (real-time) streaming data (e.g. for Internet-of-Things).

In total, 29 votes favoured the inclusion of multilateral sharing of (real-time) streaming data, closely followed by bilateral sharing of persistent (semi-static) data with 27 votes and algorithm sharing for local processing of (sensitive) data with 22 votes. The answer option "Bilateral sharing of messages" received the fewest votes (Figure 4).

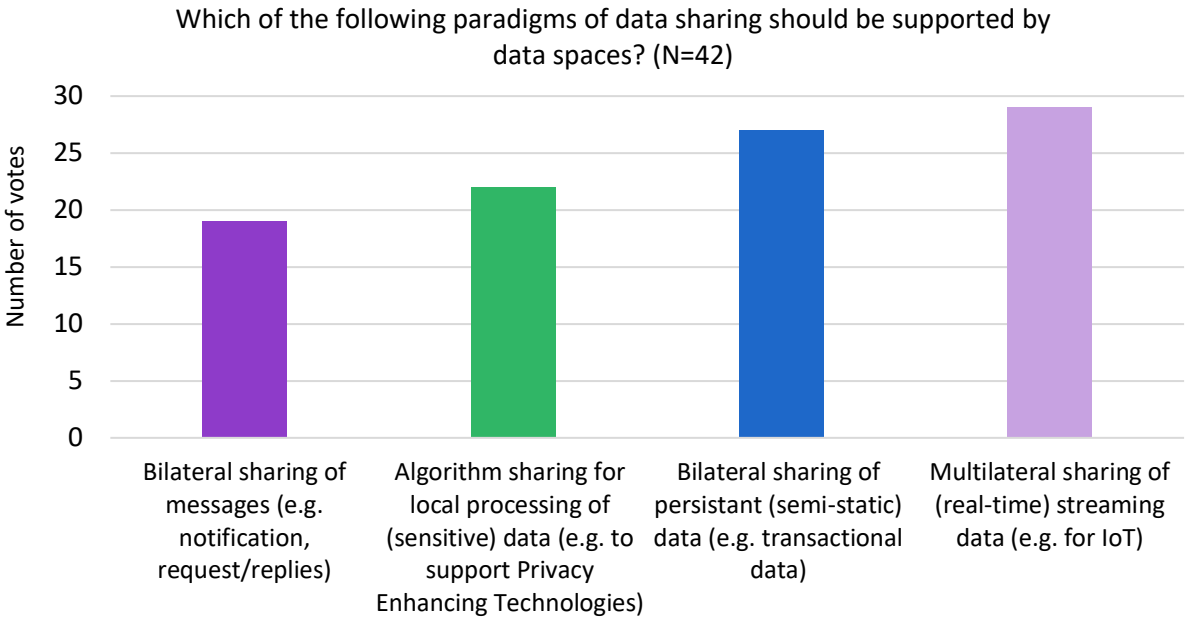


Figure 4: Responses on which paradigms of data sharing should be supported by data spaces.

During this first workshop, experts provided specific comments and remarks regarding data needs, quality, and availability. Concerning data needs, participants stressed the importance of a uniform standard of data sets, connectors, and structure. They also highlighted the need for a **comprehensive overview of state-of-the-art standards**, their harmonisation, and a wider geographical coverage. An EU regulation for data management was proposed which should include aspects for a transparent

[35] Senior Consultant at RUPPRECHT CONSULT – Forschung & Beratung GmbH (2023), personal communication, September 14. 2023.

maintenance procedure as well as guidelines for data management, aiming to address challenges posed by different data formats, which lead to increased costs and errors.

Trust was identified as a fundamental factor; without it, maintaining quality standards is difficult. Participants highlighted the necessity of a high quality and trusted environment for data sharing. They advocated for an automatic quality check that assesses not only data quality but also integrity and sovereignty. Furthermore, trustworthy data should be marked (or rated) as such: for example, specific data from highly trusted sources as well as highly trusted real-time mobility data sets (for example from the public sector).

Regarding data availability, participants highlighted the importance of **collaboration between public and private entities** to obtain data from a single source. In addition, a future EMDS should not only offer data provided by vendors, but also allow data to be searched. Further remarks and feedback from the participants included adaptability regarding new needs and constant innovation.

The diverse types of data sharing and the corresponding data needs can be illustrated by three examples of varying application domains in mobility:

- **CCAM**[36]: Higher levels of automation require static and dynamic streaming data, often referred to as Vehicle-to-everything (V2X)[37], to support use cases such as improving traffic safety or reducing traffic congestion at a very high frequency with low latency. Information on location, speed, and acceleration of the vehicle combined, for example, with (dynamic) traffic signs, traffic light information, and real-time traffic updates requires high levels of trust, security, and robustness in the data exchange.
- **Logistics:** In the field of logistics, higher levels of efficiency are required to optimise supply chains. Especially in multi-modal goods transport, exchanging, sharing, and exploiting real-time data is important for improving numerous operational processes. Due to the presence of different proprietary data formats and schemes, the cost associated with implementing standards and the lack of trust among partners creates uncertainties when it comes to supporting a seamless exchange. This complexity increases when taking into account the cross-border nature of the business processes[38]. In this context, the need for seamless data exchange is particularly pressing.
- **Urban mobility**: The concept of Mobility-as-a-Service (MaaS) requires stakeholders to actively share data to integrate various mobility services, including ride-hailing, public transport, and micro-mobility. Relevant players must provide access to the necessary data and exchange information among different stakeholders. This sharing is crucial to streamline the search and availability of vehicles, routing details, and booking and payment processes. It also ensures real-time updates on vehicle availability and estimated arrival times. Service providers must actively share this information in a trustworthy and standardised manner to deliver seamless and convenient mobility experiences to end-users. Achieving this necessitates establishing an open, collaborative, and cooperative framework that ensures technical and operational interoperability. Additionally, public authorities aim for better oversight of urban traffic flows. By integrating multiple data sources for analysis, traffic management can be optimised. Currently, this data is shared in both persistent (semi-static) and streaming formats, such as Internet-of-Things (IoT) devices, but it remains fragmented and organised in silos.

[36] Several initiatives are actively working to enhance knowledge and collaboration regarding data sharing within the CCAM community in EU. Notable examples include the CCAM partnership (https://www.ccam.eu/), C-Roads (https://www.c-roads.eu/platform.html) and the NordicWay initiative (https://www.nordicway.net/).

[37] Data sharing among vehicles and between vehicles and infrastructure is collectively referred to as V2X.

[38] See FEDeRATED - EU project for digital co-operation in logistics (2023), "FEDeRATED. Network of Platforms", http://www.federatedplatforms.eu and FENIX Network (2023), "A European Federated Network of Information eXchange in LogistiX", https://fenix-network.eu/.

Identifying data sharing types reveals diverse perceptions, needs, and experiences among mobility and logistics stakeholders. It is important to note that not all data sharing usage patterns and applications are predictable. Moreover, the right data sharing infrastructure can lead to new applications and business models. This section introduces a four-type data sharing typology for the EMDS, derived from input on experiences in mobility and logistics data sharing initiatives.[39]

1. **Sharing of persistent (static or semi-static) data**
   This may include a fixed set of data or data on operations, for which sharing across organisations enables a competitive or collaborative strategy, result in efficiency gains, provides new business opportunities, or aligns with public goals. In the context of public transit, static data is also known and referred to as schedule data.

2. **Sharing of (real-time) streaming data**
   Sensors, systems and (distributed) devices increasingly provide real-time streaming data as part of the emerging IoT. The data streams may need to be shared in a controlled manner among multiple receivers or consumers, with timeliness being an important aspect.

3. **Algorithm sharing for local processing of (sensitive) data**
   This type of data sharing allows processing algorithms to locally access (sensitive) data, i.e., within the domain of a data provider. It is also referred to as "Compute-to-Data". Various types of usage scenarios for the mobility sector could be envisaged, e.g.:

   - **Supporting Privacy Enhancing Technologies**[40] (PETs): PETs such as Federated Learning and secure Multi-Party Computation use distributed algorithms to locally access sensitive or private data. PETs can mitigate the need to share (sensitive) data altogether.

     In the mobility sector, sharing and correlating data from different actors within the ecosystem, both public and private can enhance internal processes within the organisations and enable the provision of more intelligent and sustainable mobility services at a global level. However, guaranteeing data privacy is key for stimulating data sharing, especially when considering valuable business data or user data protected by the General Data Protection Regulation (GDPR). For example, a public transport operator might aim to cross-reference their public transport usage data with data provisioned by a private telecommunication operator to perform advanced data analytics for a better understanding of mobility patterns around their city. This would require data about the usage of public transport as well as highly sensitive and protected personal data collected by the telecom operator. The data originating from both sources needs to be forwarded to a third party data analytics service provider to perform the analysis and return actionable insights to the public transport operator.

     Examples in the logistics domain showcasing these types of distributed data processing algorithms are being explored and developed to secure privacy sensitive information.

[39] TKI Dinalog Data Logistics for Logistics Data (DL4LD) project e.a. (2020), "The Logistics Data Sharing Infrastructure - White Paper", https://www.researchgate.net/publication/344068649_The_Logistics_Data_Sharing_Infrastructure.
[40] Organisation for Economic Cooperation and Development (OECD), "Emerging Privacy Enhancing Technologies - Current Regulatory & Policy Approaches", https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm.

These include Talking Trucks[41] and Smart Truck Parking[42], both involving privacy-sensitive driver data.

- **Local data pre-processing**: Data pre-processing may be done locally by means of shared applications, prior to sharing the processed data with other data space participants. This may for instance apply to applications or data apps for semantic data model management and transformation and for managing data quality.
- **Enhanced data access and protection on digital twin platforms**: Digital twin platforms may require improved data access and protection by means of the integration of PET mechanisms as part of an effective defence-in-depth strategy[43].

4. **Event-driven smart contracting for data flow control**
   This allows for data to be shared between organisations by means of a controlled data flow. In logistics, for example, event-driven real-time data flow control allows improved visibility along the supply chain and tracking of goods and trucks, and transportation conditions (e.g. for perishable or dangerous goods). Further, it enables the (automated) sharing of transport documents for business reporting or legal compliance. This type of data sharing specifically refers to data sharing concepts and architectures that have been developed by the EU CEF FEDeRATED project[44]. In the FEDeRATED architecture[45], a key element is the concept of "events", which are defined in the ontology. Data providers implement a publish-subscribe mechanism for events, while data consumers have the option to subscribe to specific events. Published events incorporate a link to the resource where additional data about the event can be accessed, provided that the data consumer is authorised to do so. This architecture forms the foundation for developing the Basic Data Infrastructure aimed at establishing a logistics data space for Europe[46].

A snapshot (Figure 5) of the supported data sharing typologies reveals that sharing of persistent (static or semi-static) data and sharing of (real-time) streaming data are currently experienced as common practice by stakeholders. As AI methods become integrated, the requirements for data sovereignty, blockchain approaches, algorithms for local data processing, and smart contracts gain importance. However, these types of data sharing are currently underrepresented.

[41] G.L.J. Pingen, C.R. van Ommeren, C.J. van Leeuwen, R.W. Fransen, T. Elfrink, Y.C. de Vries, J. Karunakaran, E. Demirović, N. Yorke-Smith (2022), "Talking Trucks - Decentralized Collaborative Multi-Agent Order Scheduling for Self-Organizing Logistics", Proceedings of the 32nd International Conference on Automated Planning and Scheduling, ICAPS, https://pure.tudelft.nl/ws/portalfiles/portal/140322747/19834_Article_Text_23847_1_2_20220613.pdf.

[42] J.P.S. Piest, S. Slavova and W. J. A. van Heeswijk, (2023), "A Reference Use Case, Data Space Architecture, and Prototype for Smart Truck Parking", in: Proceedings of the 22nd CIAO! Doctoral Consortium, and Enterprise Engineering Working Conference Forum 2022 co-located with 12th EEWC 2022, (CEUR Workshop Proceedings; Vol. 3388), https://ceur-ws.org/Vol-3388/paper1.pdf, p. 1-15.

[43] G. Ahmadi-Assalemi, H. Al-Khateeb and A. Aggoun (2022), "Privacy-enhancing technologies in the design of digital twins for smart cities", https://doi.org/10.12968/S1353-4858%2822%2970046-3.

[44] EU FEDeRATED project, "EU-project for digital cooperation", http://www.federatedplatforms.eu.

[45] EU FEDeRATED project (2022), "FEDeRATED Reference Data Sharing Architecture", draft, http://www.federatedplatforms.eu/index.php/library/item/draft-federated-reference-architecture-document-june-2022.

[46] BDI, "Basic Data Infrastructure - BDI", https://bdinetwork.org.

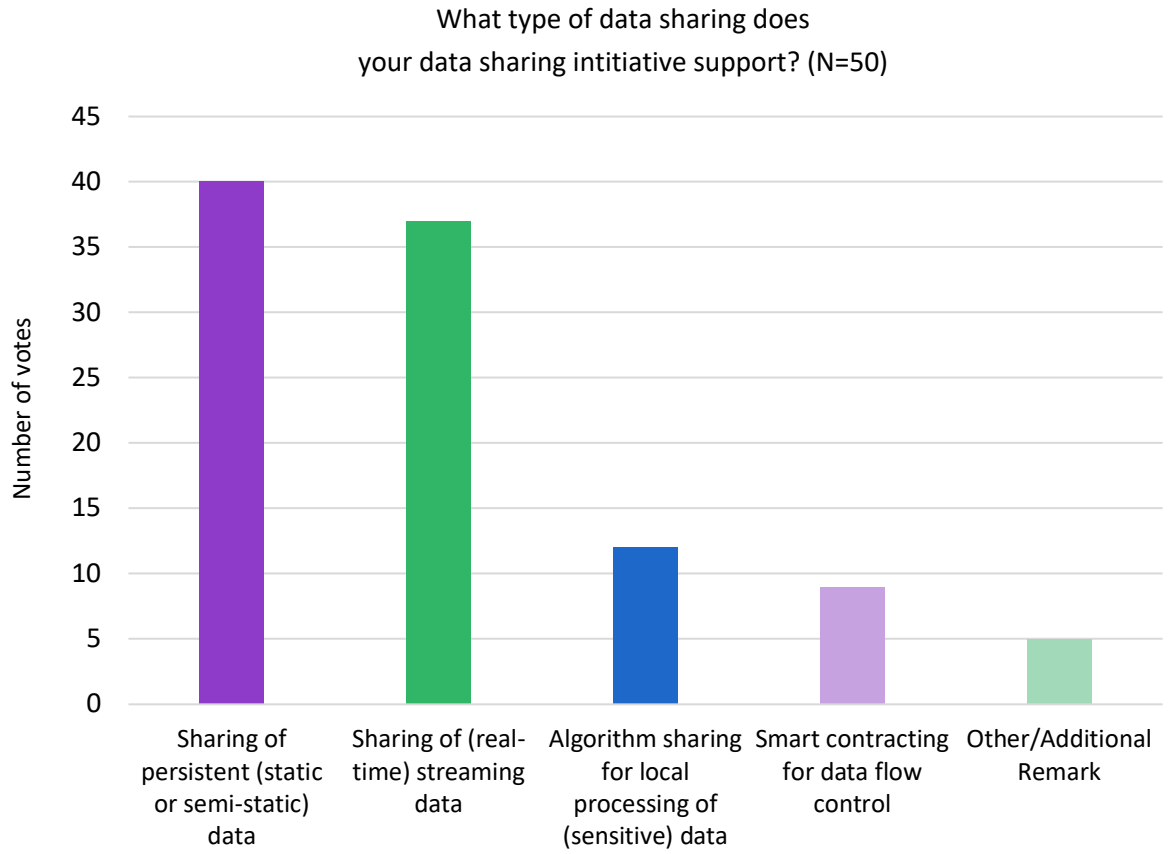


Figure 5: Responses on different types of data sharing.

Although about two-thirds of respondents indicated they offer options for querying specific data elements based on the two questionnaires, this can still be described as a gap. This is because there is a wide array of possibilities in querying languages and Application Programming Interfaces (APIs), highlighting a lack of consistency in this aspect. Access policies and conditions, as well as usage policies and conditions, are identified as an open issue for approximately half of the participants, based on their questionnaire responses. These findings are largely congruent with the findings of the FIWARE expert workshop where different types of data sharing were discussed.

Overlaps in data availability and usage

There are several overlaps in data availability and usage. For example, organisations or sectors might be collecting similar data related to weather patterns, customer demographics, or transportation trends from one specific region or area. Such duplications can lead to unnecessary resource expenditure and fragmented insights. Moreover, **coherence becomes a concern** when multiple data sets purport to measure the same phenomenon but exhibit significant discrepancies. For instance, as highlighted in an interview with an expert from the maritime sector, vessel schedules lack standardisation in the context of container movement. Consequently, there are various timestamps associated with one vessel's arrival at a port. This lack of harmonisation hampers efficiency and, consequently, in this case, contributes to increased CO_2 emissions. Additionally, overlaps in data utilisation occur when different entities analyse or use similar data sets independently. Instead of collaborating and sharing insights, they might **duplicate efforts**, resulting in missed opportunities for more comprehensive analyses and informed decision-making.

An analysis of travel information data and its current landscape reveals that multiple major corporations collect and offer similar services and data. This setup can result in several negative impacts, including:

- **Consumer confusion**: Overlapping travel information can be problematic for consumers. Various services may provide different data, resulting in different route recommendations. This divergence can lead to confusion for individuals attempting to plan their journeys, ultimately eroding confidence in the accuracy of the provided information.
- **Inefficient use of resources**: Companies collecting similar data often build overlapping infrastructure and resources. This includes implementing and maintaining sensors, data collection systems, and data analytics infrastructure. These overlapping efforts result in resource wastage and may contribute to higher costs for companies.

To mitigate the adverse effects of data overlap, companies and government agencies can collaborate to share data, set standards for data exchange, and ensure coordination between different mobility information providers. This approach can help prevent duplication, improve data quality and increase efficiency in the sector.

On the other hand, data overlaps can also yield beneficial effects in the mobility and logistics sector, particularly when this overlap is well managed and exploited. Some potential positive outcomes comprise:

- **Increased data accuracy**: When multiple sources collect and share similar data, it can lead to increased data accuracy. Errors and inaccuracies in data can be identified and corrected through comparison with other data sources, ultimately providing users with more reliable information. A specific example is in the road traffic domain, where static information collected via inductive-loop traffic detectors can be complemented by more dynamic floating car data sources to increase coverage of flows across a road network.
- **Redundancy and resilience**: In case of failure or breakdown of one data source, overlapping data sources can act as backups when appropriately designated for this purpose. This increases the resilience of mobility systems and ensures that users continue to have access to critical information even if problems arise at a single data source. This can be particularly relevant for CCAM applications.
- **Data fusion and improved decision-making**: By combining and analysing overlapping data sources, companies, and governments can acquire a deeper understanding of mobility and logistics patterns and behaviours. In turn, this can lead to improved decision-making in urban planning, traffic management and mobility policy.

This type of overlaps relates to **synergies** that, when harnessed through more coordinated efforts, can produce positive outcomes for both businesses and society. Multiple stakeholders generate and collect similar types of data. For example, original equipment manufacturers (OEMs), location-based service providers, public transportation companies, road authorities, municipalities, and national statistical agencies have overlapping data on traffic conditions. Furthermore, several platforms provide the same data in different formats (e.g. RDF, XML, Atom, Odata, csv, JSON, JSON-LD, SHP). Some of these platforms have a broad distribution, especially in specific domains like public transport, individual transport, both mainly road-based, and transport infrastructure management companies, while others maintain a narrower focus. In addition, data service providers who often act as intermediaries frequently utilise similar types of data sources, which are subsequently offered to users. While different stakeholders hold similar types of data, **data interoperability and data quality issues** still make it challenging to integrate data sources. Thus, while the overlapping availability in data sources may initially be perceived as redundant, opportunities for synergies emerge when details per data source vary and can be combined or fused. An EMDS should serve as an opportunity to harmonise

standards and target interoperability between application domains in use, without limiting the potential inclusion of new ones that are mature and supported by relevant communities.

2.3. Key challenges for data availability and reliability

Several gaps in data requirements and overlaps within the mobility and logistics domain were identified. These gaps highlighted various challenges, concerns, and needs related to data availability, accessibility, and the nature of business practices within and between different application domains.

The list describing required data sources (outlined in Table 6) draws on a broad range of current use cases in the mobility and logistics domain. However, attempting to rank these data sources by importance or demand is not particularly advantageous, as the significance of the data sources can vary across different contexts or use cases. While the list highlights diverse data sources, determining a hierarchy per application domain is challenging. Moreover, significant data challenges extend beyond domain-specific concerns, they encompass broader issues such as data acquisition strategies, licensing, ownership, quality, standardisation, organisational hurdles and stakeholder management.

Strategies to obtain data and data licensing: Various practices exist for acquiring data within the mobility and logistics domain. Based on questionnaire responses, stakeholders acquire data from a combination of sources, with the majority relying on open data provisioning (Figure 6). The second most common method is via intermediaries, metadata brokers, or trusted third parties. Data marketplaces are the third most popular option, slightly less prevalent than intermediaries.

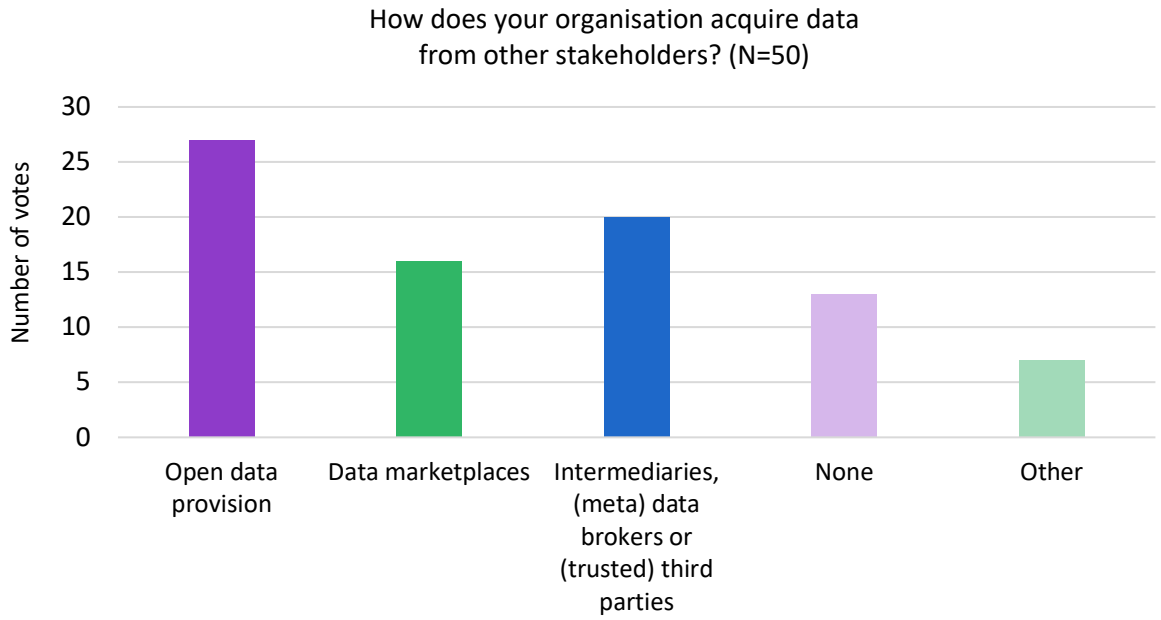


Figure 6: Strategies for obtaining data.

Despite the existence of these strategies, data accessibility poses significant challenges. The mobility and logistics sector experiences extensive data generation and collection by numerous stakeholders, including transportation companies, logistics service providers, government agencies, and technology service providers such as real-time transportation visibility platform providers. This data is highly fragmented and **dispersed across different systems**, organisations, and platforms. Mobility data serves as a foundation for a diverse range of services, from real-time tracking of logistics vehicles to efficient ticketing provision. The specific data needs also vary depending on the actor: car manufacturers collect in-vehicle data on vehicle performance, public transportation agencies need data on passenger flow and schedules, and government agencies gather data on road infrastructure. However, this fragmentation hampers overall data accessibility, making it challenging to find and access data from different sources to meet specific data needs or gain a comprehensive view across

application domains. While the use of open data is popular, caution is needed as some data may originate from various sources and be employed multiple times with minor variations. There is also variation in the number of data providers that provide data at data marketplaces, intermediaries, (meta) data brokers, or (trusted) third parties. This variability indicates a strong need for trustworthy, validated data sources that guarantee data sovereignty for those providing data under the EMDS.

Alongside inquiries about of strategies to obtain data, the question arises of how data use should be licensed. Based on the desired types of data licenses (Figure 7), it is evident that more than two-thirds of the responders request a registration as a necessary prerequisite for accessing data. 28% advocate for a stronger legal binding through a concrete license agreement, and almost a quarter are open to allow free access. Overall, the perspectives are varied. Therefore, a solution must take a holistic view on usage control, access control, data security, and other considerations. Nevertheless, data that is freely available and of fundamental importance for potential users should remain easily accessible within the framework of an EMDS. While recognising that some data should be freely available to a certain extent, it is essential to determine how data covered by licensing should be priced and structured. Section 3.4 further reflects on these questions and addresses various fee options.

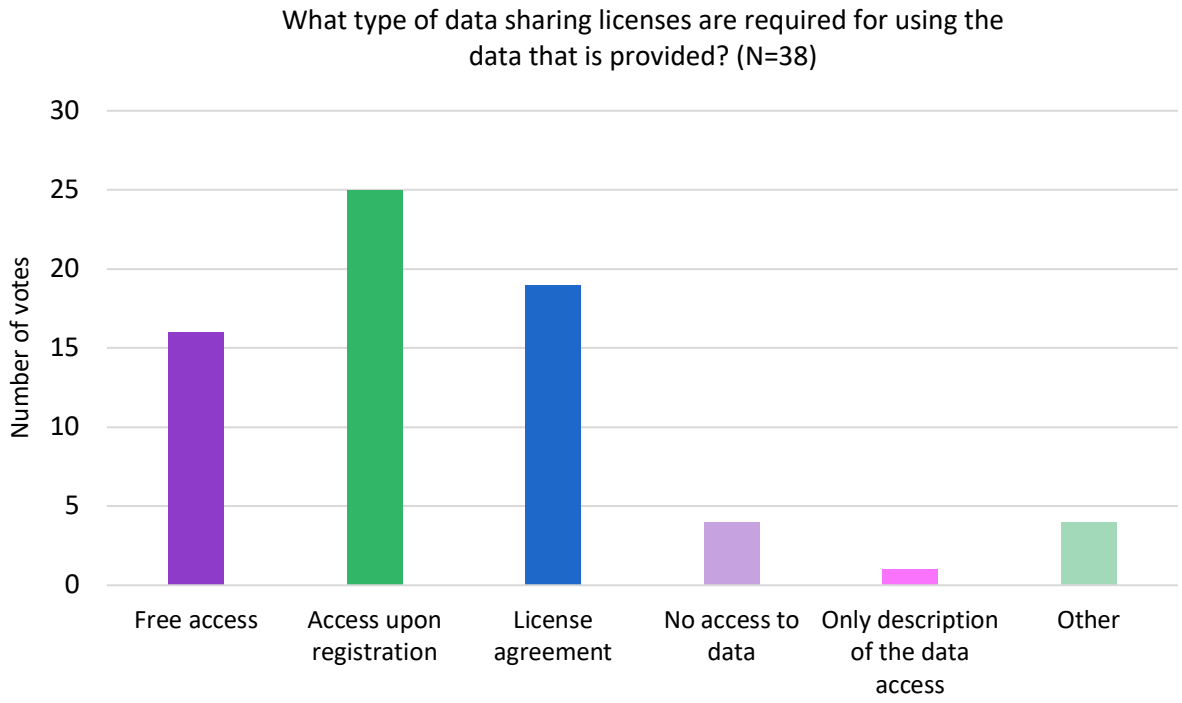


Figure 7: Categories of data licenses required when accessing data.

Data ownership issues

Understanding the barriers to acquiring and exchanging data is crucial in the development of the EMDS. The assessment of hurdles, as revealed by stakeholders (Figure 8), highlights **complex and interlinked challenges**. Privacy concerns, data sovereignty constraints, data quality concerns, and commercial sensitivity are concerns identified for over half of the respondents. These barriers primarily centre around identifying the right data holder and navigating the process to access the data.

However, simply having the option to query available data, as mentioned by more than two-thirds of the respondents, is insufficient in addressing the various challenges and obstacles associated with data acquisition and data exchange. Similarly, the reported presence of usage (over 80%) and access policies (over 75% of the respondents) falls short in terms of establishing a convincing sense of trust and security. Addressing these concerns and constraints is a prerequisite for the success of the EMDS.

As shown in the previous section, stakeholders are generally aware of relevant data sources for their value creation but face challenges in identifying and accessing the appropriate data. Data silos are present due to different types of data ownership structures. Each stakeholder may have created their own data silo and restrict conditions of sharing their data due to concerns about competitive advantage, data privacy, or the costs and complexity of data sharing. Identifying the right data owner is therefore fundamental in establishing a suitable data sharing mechanism.

Data quality and standardisation

As previously mentioned, stakeholders in mobility and logistics employ a diverse array of data formats, structures, and naming conventions to represent similar types of data. According to the findings from the questionnaires, nearly one-third of these stakeholders utilise proprietary interfaces, while a quarter employ a combination of standardised and proprietary interfaces. These **differences in interfaces** creates inconsistencies that pose considerable challenges in terms of data integration and analysis. Furthermore, issues persist with the maintenance and regular updates of data sets, primarily stemming from incomplete or inadequate metadata and inaccuracies within the data sets provided by various data platforms. Seemingly trivial discrepancies, such as variations in station names (e.g. "*München Hbf*" versus "*München*") or disparities in data granularity, further compound the challenges encountered when trying to integrate and compare data. For instance, one organisation may collect highly detailed data pertaining to individual vehicle movements, while another entity may possess solely aggregated data pertaining to vehicle usage within a specific road network. While some application domains have standards for harmonised data exchange, their adoption varies, impeding widespread data accessibility[47].

Moreover, the degree of data validation is important. For end-users, the availability of relevant information depends significantly upon the data quality and data validation. If end-users aim to access consistently accurate information irrespective of the application or data service used, data validation must be **uniform and synchronised** across the entire spectrum of data providers. This necessitates adherence to established reference frameworks, thereby ensuring the flow of high-quality data. A good example of this principle is within the public sector domain, where the concept of "profiles" has been adopted. Rather than advocating for data delivery solely based on mandatory elements, a defined set of elements drawn from a reference standard has been established, tailored to address the specific requirements of various use cases. This pragmatic approach streamlines the implementation of, at times, intricate standards, often relying on simplified standards or pre-existing versions that have already undergone successful implementation. Nevertheless, challenges persist. In Germany, the standards of the Association of German Transport Companies (Verband Deutscher Verkehrsunternehmen) for the exchange of public transport traffic data (VDV 453[48]/454[49]) are still widespread, despite the existence of a corresponding superordinate EU standard (SIRI[50]). Consequently, there is a challenge to mobilise stakeholders to transition to a standard, especially if they do not perceive a direct benefit for themselves (i.e. a positive externality).

[47] In the most recent report on NAP data availability by the NAPCORE project, a survey was conducted to monitor progress on NAP implementations across Europe. Although different types of standards exist (e.g. NeTEx, SIRI, DATEX II) which support data availability for various types of data sources, adoption, and usage of those standards greatly differ per country in the EU. In addition, interpretation of what data quality constitutes is interpreted differently by the NAP operators as this could mean a lack of information on the quality of data sets or no clear consensus on implemented data quality criteria/requirements, see NAPCORE Working Group 3 (2023), "Second Report on NAP Data Availability", https://drive.google.com/file/d/1XUbN3MnDGm9R6agbUNxw-_0MaBc8wvIm/view.

[48] Verband Deutscher Verkehrsunternehmen (2020), "VDV-Schrift 453. Ist-Daten-Schnittstelle", Version 3.0, https://www.vdv.de/downloads/4337/453v3.0%20SDS/force.

[49] Verband Deutscher Verkehrsunternehmen (2020), "VDV Schrift 454. Ist-Daten-Schnittstelle – Fahrplanauskunft", Version 3.0, https://www.vdv.de/i-d-s-downloads.aspx.

[50] SIRI (2023), "Standard Interface for Real-time Information", https://www.siri-cen.eu.

Addressing this requires collaborative efforts among stakeholders to establish common frameworks to improve the ability to effectively leverage each other's data. There are examples of application domains where standardisation promotes data interoperability, either through a common data model or format, or through development of mechanism for secured and controlled access to data, showcasing an effort to close these gaps. These include DATEX II[51], NeTEx[52], and, within the logistics initiatives, OpenTripModel[53], which is used to exchange logistic trip data between or shippers, carriers, software vendors, OEMs, and truck manufacturers. Cooperation and coordination are key drivers for improved data interoperability, facilitating adequate standardisation of data and its adoption across all relevant stakeholders. It is worth highlighting NAPCORE, which enhances data harmonisation across the National Access Points (NAPs) and the DTLF, supporting and contributing to the development of implementations that Member States need to adopt, such as the new eFTI regulation.

Organisational hurdles and stakeholder management

To establish a thriving data sharing ecosystem that caters to diverse data needs, engaging a sufficient number of data providers and stakeholders is vital. Several key challenges need to be addressed which are related to organisational hurdles or stakeholder (mis)management. Firstly, some stakeholders may not feel compelled to share data **without legal mandates**. Secondly, establishing trust among data providers is essential for successful data sharing. Additionally, providing incentives for data sharing can **encourage broader participation**. Lastly, some organisations may struggle to offer data initially or participate in data sharing at all due to a **lack of data literacy or expertise**. Addressing these challenges is vital to establish a robust and comprehensive data space.

In certain scenarios, stakeholders might not feel obligated to share data unless mandated by legislation. This is particularly evident in Business-to-Government settings. In one instance, a public data platform for mobility data, as reported in interviews, expressed difficulties in acquiring the required data for the designated area. Public entities of this nature often face challenges in acquiring desired data due to the lack of a regulatory framework compelling commercial companies to share data to the desired extent. Consequently, they often advise cities to incorporate contract clauses mandating private mobility companies to share relevant mobility data. Ideally, a comprehensive regulatory framework would eliminate the need for such individualised efforts.

Building **trust** among data providers is essential for successful data sharing. Stakeholders need assurance that their company and client privacy will be safeguarded while engaging in data sharing. The issue of trust is significant; many entities in the domain of mobility data express concerns about security of their commercial secrets, which is cited as a barrier to data sharing by half of the respondents (Figure 8). Trust, or distrust extends beyond factual security and is also a matter of perception, as one data service provider expressed during an interview. Being associated with being trustworthy extends beyond individual precautions and is related to the overall image of the entity providing the data sharing. Communicating the possibilities of mitigating these risks and overall trustworthiness of data sharing is crucial in gaining stakeholders' confidence in the EMDS, a topic further discussed in Chapter 8.

[51] DATEX II (2023), "Welcome to DATEX II", https://www.datex2.eu.
[52] NeTEx (2023),"NeTEx. Network Timetable Exchange", https://netex-cen.eu.
[53] OpenTripModel (2023), "OpenTripModel is a simple, free, lightweight and easy-to-use data model, used to exchange real-time logistic trip data on the web", https://www.opentripmodel.org.

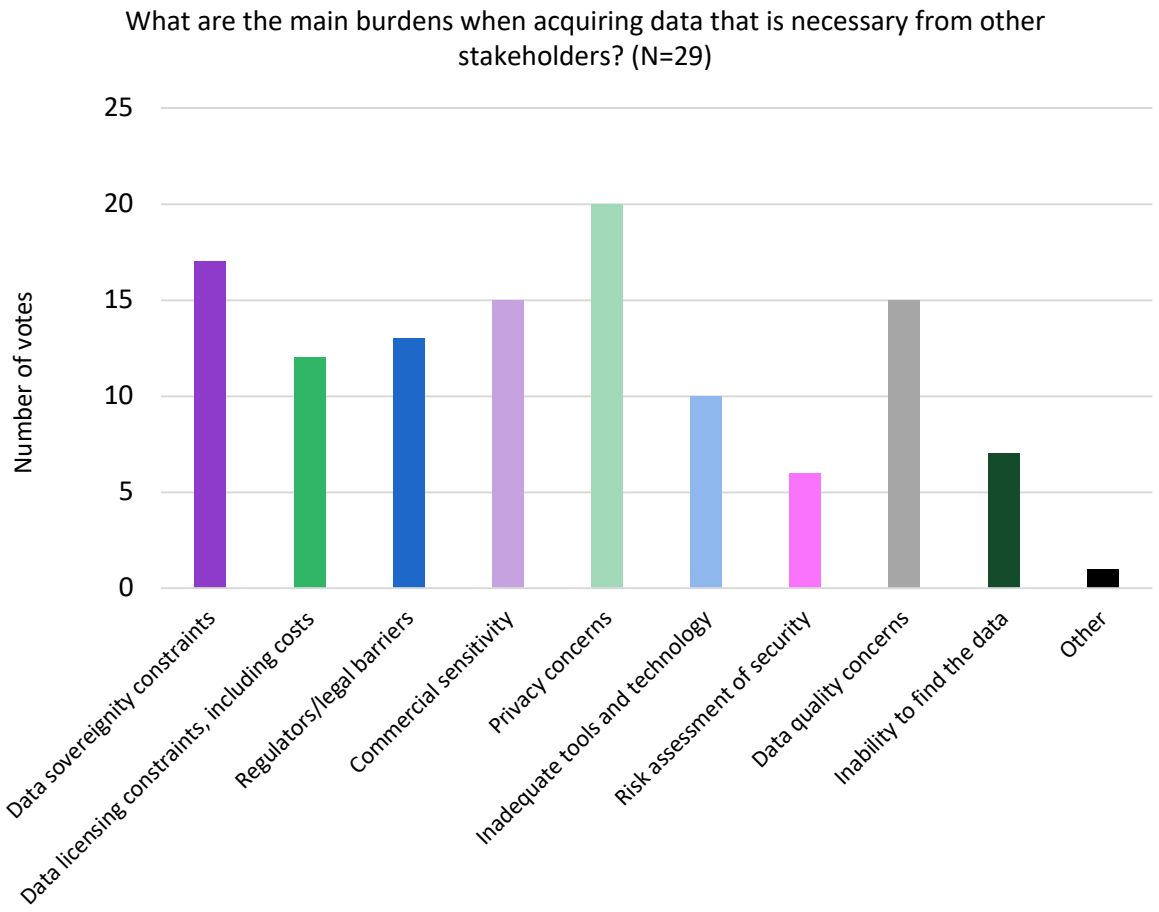


Figure 8: Main barriers acquiring data.

Determining effective incentives for data sharing is important. However, the type of entity and data owner significantly influences the incentives that would motivate them to provide data. In Lombardy, for instance, the local airport is directly incentivised to share data with the train station, and vice versa, as both display each other's data at their respective venues to bring a more seamless travel experience to their customers, creating a classical win-win situation. In addition, some transport operators in Lombardy are obliged to provide APIs as part of their public service obligations. In the case of larger companies, the incentive to share data is often financial, but not exclusively, as argued by an interviewee from a public data platform. While requesting payment for data usage can be effective, there is a growing interest among larger companies in establishing robust relationships with start-ups. Instead of providing monetary support to start-ups, an effective approach involves fostering relationships by sharing valuable data with them.

Enhancing technological support and addressing the lack of data expertise are crucial aspects of addressing organisational hurdles that hinder active participation, especially among potential data providers. As noted in the interview with members of NAPCORE, many potential data providers may not even be aware that they possess valuable data. To address this issue, comprehensive communication strategies involving relevant stakeholders have been proposed. Initiatives such as creating informative videos explaining the significance of NAPs and data sharing have been initiated under NAPCORE. Furthermore, national bodies are actively exploring ways to facilitate data provision. Although tangible outcomes have yet to materialise, these efforts are ongoing and being carefully examined within dedicated workgroups which highlight the need to raise awareness. Further, a lack of

data expertise can become a problem when companies refrain from data sharing because they are unable to actively engage in a data space. As previously underscored (Figure 8), about one third of the questionnaire respondents highlighted "inadequate tools and technology" as a hurdle to acquiring data. Existing data sharing initiatives are already trying to address this in various ways. One example is the so-called "Connector-as-a-Service"[54], which enables plug-and-play participation in a data space and is already developed and used in initiatives such as Catena-X and the MDS, initiated and based in Germany. Users gain access to sovereign data exchange within minutes, without the need to understand the underlying technology or build solutions themselves. Such easy-to-implement solutions could facilitate access and participation of many stakeholders who might otherwise be too reluctant or lack the internal expertise to participate in data sharing.

2.4. Recommendations

Conclusion

The EMDS places a central focus on facilitating enhanced forms of data sharing, both within and across various application domains. This strategic emphasis will create a wealth of innovative opportunities within the mobility and logistics sector. From analysis on data sources gaps and overlaps it becomes evident that a significant challenge to address is the marked heterogeneity in the data source needs. Furthermore, it is worth noting that the concept of data sharing within mobility and logistics is still evolving. Currently, a significant proportion of stakeholders predominantly engage in the sharing of persistent (static or semi-static) data. However, further insights strongly indicate that a future EMDS should also support multilateral sharing of streaming data as these emerging forms are actively being implemented in various application domains to realise the necessary value creation. Looking ahead, an optimal outcome to strive for is the convergence of solutions and the minimisation of divergence in the context of data sharing. Therefore, to support of the EMDS development, it is imperative to consider the recommendations identified by the gaps and overlaps analysis, which should help inform the design of the building blocks.

Recommendations

Meet data accessibility needs

Despite efforts to enhance data availability, there remains a substantial need to increase the discoverability and availability of mobility-related data while reducing acquisition barriers. Further research is required to identify key use cases and their respective data needs. This can lead to more effective use of existing data sources, approaches, and tools under the EMDS, addressing data needs whilst simultaneously tackling identified barriers to data acquisition. To achieve the best outcome, it is important to select cross-border use cases that can showcase the level of data sharing required to meet the data needs and address the key barriers for an EMDS. Priority cross-border use cases should be determined through stakeholder consultation and receive support under EMDS community management and use case acceleration, enhancing the sustainability of this endeavour. It is recommended to develop targeted strategies to fill data gaps, potentially through existing data collection initiatives in the mobility or logistics sector or via partnerships as part of a committee or working group structure under the EMDS.[55] Notably, efforts should be intensified to ensure that data on the identified data needs, such as road traffic and infrastructure, traffic related data from sensors, and inter- and multimodal data, is taken into account. In addition, as new user needs, use cases, requirements and specifications emerge with the adoption of new types of data sharing, it is helpful to document ongoing data source gaps related to meet the needs of the mobility-related use cases.

[54] More on the functionality of a connector can be found in Section 6.5.

[55] More on the business and governance building blocks needed under the EMDS can be found in Part III of this report.

This can help in monitoring gaps and serve as a way to measure progress, which can help policymakers and other stakeholders in addressing persisting data gaps. Furthermore, it is strongly encouraged to support use cases that can showcase the different types of data sharing. This is necessary to reach a reasonable level of confidence in data sharing to be supported by the EMDS and thus prove its added value. Most notably, given that a majority of stakeholders have experience in sharing of persistent (semi or semi-static) data, it is advised to look deeper into how use cases can be supported by the other identified types of data sharing. In general, given the variety of data source needs, there is an essential need for flexible metadata that captures various data characteristics under the EMDS. This metadata should be used to navigate to hard attainable and understandable data. Fostering the establishment of such an approach creates possibilities to address existing or new data gaps identified by use case owners.

Propose guidance for data quality

Diverse data formats, definitions, and data granularity within the mobility and logistics domain pose barriers to establishing a coherent understanding of what constitutes good quality of data. To enhance data quality, it is crucial to intensify harmonisation efforts. Establishing a working group to assess how data quality can be defined and harmonised under the EMDS is an initial step. This working group would foster discussions among a wide range of stakeholders, including those from the private sector, public sector, research, and academia, to explore dimensions of data quality and other relevant data characteristics. Furthermore, defining guidelines with a use-case-driven approach ensures the coverage of diverse data types across application domains. A potential approach is to define a common set of dimensions, such as reliability, coverage, and completeness, that can be adopted to determine data that can be regarded as fit-for-purpose. In addition to fostering discussion on data quality, skill sharing of members of the EMDS should be prioritised, granting access to essential harmonisation and data quality assurance efforts. A vital facilitator in this regard is to promote transparency among data holders, encouraging them to disclose how data was collected and prepared (e.g. the procedures followed) as well as metadata of their data sources. On a technical level, this will assist in better differentiating by type of data and support in meeting specific data needs. At a strategic level, this transparency elevates this strategic value of data for specific stakeholders.

Increase efforts towards common sets of standards for the disclosure of data

Currently, most activities are either limited or organised per application domain in the mobility sector. Close collaboration between both public and private entities will be required to address existing divergences in data types. To advance this goal, basic data models and vocabularies for mobility and logistics data should be harmonised under the EMDS, enhancing comparability and consistency of data sources. The availability of comparable and consistent data will make data-driven innovations or insights more reliable such as machine learning or AI applications, or the development of new or underdeveloped metrics or indicators, such as the SUMI. Further development of data standardisation and the use of standardised data sets and models will be necessary within the context of the EMDS, accelerated via the committee structure proposed as part of the EMDS governance. This is where the use of common data formats can be encouraged, and support for a common underlying approach can be discussed. These guiding principles should help in the implementation of a common data format, both within and across application domains, improving linkage of common data formats and paving the way for interoperable and more consistent data. Chapter 7 elaborates on data formats in mobility and logistics, emphasising the importance of designing the right interoperability building blocks that will support consistent sharing of mobility and logistics related data.

Avoid redundancies through improved knowledge sharing

The optimisation of knowledge exchange and promotion of capacity building represent crucial steps in reducing redundancy and maximising the value derived from data exchange within the framework of the EMDS. Many initiatives are dedicated to improving data access and availability. A strategic way forward would be to formulate strategies aimed at mitigating duplicated efforts by fostering collaboration among stakeholders who share similar objectives. This approach allows for the harmonisation of efforts in addressing use cases within the EMDS framework. Such collaboration not only serves to incentivise various niches and sub-domains within the field of mobility to work effectively together but also enhances interoperability at the crossroads of distinct application domains. Moreover, learning from these redundant efforts can be more precisely focused on understanding the prerequisites for initiating data sharing. Equally important is the exploration of cross-sectoral opportunities for data sharing, as this serves as a catalyst to motivate stakeholders, showcasing the potential for mutually beneficial outcomes. A fundamental takeaway is the significant time and effort required to engage in meaningful dialogue with a comprehensive and representative group of stakeholders within the EMDS. Recognising the significance of comprehensive stakeholder management and engagement in eliciting requirements is paramount.

Leverage synergies by building upon existing data sharing initiatives

Leveraging synergies can boost data accuracy, resilience, and fusion opportunities. The EMDS should examine existing data sharing initiatives strategically to enhance mobility and logistics applications within its scope. The ANEM project[56] exemplifies this approach by addressing algorithm sharing for local processing of sensitive data and combining differential privacy technologies within the mobility sector. The implemented solution utilised IDS components, namely data space connectors, to facilitate the secure transfer of data among three key entities: (1) data provider, (2) synthetic data generation solution provider employing differential privacy to safeguard the original data, and (3) data analytics solution provider. Consequently, the original protected data remained confidential, while data analytics were conducted on the generated synthetic data. In the field of event-driven smart contracting for data flow control, the logistics sector has played a pioneering role, notably through the architectural and methodological developments led by the FEDeRATED project, the associated DTLF data sharing strategy for logistics and initial deployment of the approach. The relevance and applicability of these examples may extend to other application domains within the mobility sector, provided a thorough examination of their feasibility within the EMDS framework for distinct sub-domains. Not all usage patterns and applications for data sharing can currently be foreseen as it is conceivable that an adequate data sharing infrastructure may lead to new types of applications and business models. Therefore, the mobility and logistics data space initiatives should take a leadership role in defining a harmonised approach as part of the deployment initiatives. Emphasis should be placed on forms of data sharing that support multilateral sharing of streaming data, local pre-processing of sensitive data, and event-driven smart contracting for data flow control, given their technological developments and their relevance for the EMDS. This requires alignment with the DSSC blueprint development team and the SIMPL project to ensure they become an integral part of the metadata brokering building blocks in the common European data spaces.

[56] ANEM is a regional project implemented in Catalunya with the objective of offering a differential privacy service through a data spaces ecosystem. The project was coordinated by Mosaic Factor and implemented in collaboration with the i2CAT Foundation and the Universitat Politècnica de Catalunya. See: CIT UPC (2023), "ANEM. Models and techniques of data anonymisation with applications in the mobility sector", https://cit.upc.edu/en/portfolio-item/anem-models-and-techniques-of-data-anonymisation-with-applications-in-the-mobility-sector/.

III. Organisational and business building blocks

Parts III and IV of the report identify building blocks that can contribute to the long-term convergence of existing and new data sharing initiatives in the mobility sector and explore suitable frameworks for managing federated data sharing and data spaces in this sector.

The report uses the broader definition of building blocks from the DSSC taxonomy, which includes both technical assets and organisational, business, and non-operational capabilities. Moreover, the term "building blocks" is used for any capability or activity that will help the mobility and logistics sector to be developed, deployed, and evolved towards the EMDS as part of the overarching ambition of the common European data spaces.

Part III of this report focuses on the DSSC organisational and business building blocks (Figure 2), business, governance and legal. Chapter 3 includes an account of the value proposition (describing the "why?") and the broad understanding of the key activities and funding opportunities that are needed to deliver the value to the stakeholders. The subsequent Chapter 4 delves into the governance framework (describing the "how?") and proposes a governance structure for the EMDS taking into account the complexities within the extensive landscape of mobility data sharing initiatives. Finally, the legal frameworks that underpin and affect data space operations are addressed in Chapter 5.

3. Business and funding models

3.1. Introduction

The success and economic sustainability of a common EMDS depends on value added for the multiple stakeholders in the ecosystem. This requires the alignment of its mission with the expectations and needs of the stakeholders. The PrepDSpace4Mobility project involves the analysis of business and funding models for existing data sharing ecosystems. It formulates a proposal for establishing the EMDS that aims to motivate multiple stakeholders in the mobility and logistics sector and beyond to share data, and which also aims to facilitate the development of innovative applications. This chapter offers insight about the added value that a common EMDS brings to multiple stakeholders in the ecosystem and describes how to position potential business and funding models in the data space landscape to ensure the sustainability of a common EMDS in the long term.

The relevant business models for data spaces address both the individual stakeholders and the creation and maintenance of a data space. This report focuses on the business model concerning data space creation and maintenance, without pursuing a profit objective.[57]

Within the mobility and logistics sector, data sharing already takes place through various methods, e.g. peer-to-peer connections, platforms or data lakes harvesting and redistributing data back to consumers, or by using the services of global hyperscalers. A strong business model and value proposition for a common EMDS are essential for attracting stakeholders and for also convincing those who are already engaged in conventional data sharing to embrace the data space paradigm.

The first part of this chapter offers insights into the complex stakeholder landscape of the mobility and logistics sector and the role of the different stakeholders in a common EMDS (Section 3.2). In addition to discussing their concrete needs and requirements, it proposes how a common EMDS can create value for the stakeholders and outlines the key activities expected (Section 3.3). The second part of this chapter focuses on different potential funding models (Section 3.4). The conclusion, recommendations, and building blocks for a common EMDS are presented in Section 3.5).

3.2. Stakeholders and value proposition

Data spaces represent a collaborative federated approach to data sharing. A common EMDS needs to cater to multiple stakeholders in the mobility and logistics sector with different needs and requirements. This section provides an overview of stakeholders and the value proposition that the EMDS may represent for them.

Stakeholders

Various stakeholders have been identified in the EMDS context:

Consumers and citizens

Civil society should be regarded as the ultimate beneficiary of the EMDS. Citizens should benefit from a digital and green transformation in the mobility and logistics sectors in general, and as consumers of mobility and other services, they should have access to an improved range of services and applications. Consumers' travel mode preferences and data usage patterns shape the development of mobility services, as well as considerations of data privacy.

[57] EU Open DEI project (2021), "Design Principles for Data Spaces. Position Paper", https://design-principles-for-data-spaces.org.

Mobility and logistics companies

These companies include public transport operators, airlines, shipping companies, trucking firms, railways, ride-sharing companies, coaches, taxi services, bike/scooter-sharing companies, and more.

These companies are the core of the mobility and logistics sector, responsible for efficiently moving citizens and goods. They seek access data offered within the ecosystem of the EMDS not only to develop new services or applications but also to produce and process valuable data that may be shared with others.

Public authorities

Public authorities (e.g. cities, public transport authorities, urban planners, infrastructure providers, road authorities, customs, etc.) may be responsible for urban planning, traffic management, the transportation infrastructure or monitoring and approving mobility and logistics processes. They want to access data offered within the ecosystem of the EMDS not only to make informed decisions about transportation infrastructure and city planning but also to produce and process valuable data that may be shared.

Data provider and aggregator companies

These companies and organisations collect, aggregate, and provide mobility and logistics data. This includes informational data (e.g. on traffic, location and transit schedules) and operational data (e.g. on transportation documents, loading levels and carbon footprints). They produce and enrich valuable data that may be shared within the ecosystem of the EMDS.

Enabling data sharing infrastructure service providers

These service providers are also referred to as intermediary roles. They provide the governance and technical capabilities for developing, deploying and operating a data sharing infrastructure or data space.

Suppliers and manufacturers

Suppliers and manufacturers (e.g. car manufacturers, bus, trucks, train and plane manufacturers) produce vehicles, equipment, and technology used in the mobility and logistics sectors. They seek to access data offered within the ecosystem of the EMDS not only to improve their products and services but also produce and process valuable data for some of which sharing is mandated under the Data Act. For example, smart vehicles produce extensive data arising from their use.

Technology companies and solution providers

These companies develop and supply technology solutions, such as GPS navigation systems, IoT, tracking software, data analytics for mobility and logistics solutions and autonomous vehicle technology. They seek to access data offered within the ecosystem of the EMDS not only to improve their products and services, but also to produce and process valuable data that may be shared.

Start-ups and innovators

Small ventures and entrepreneurs seek to access data offered within the ecosystem of the EMDS to create new solutions and business models in the mobility and logistics sector and beyond that drive innovation and disrupt traditional practices.

Research institutions and academia

Universities and research institutions conducting research on transportation approaches, trends and data analytics seek to access and analyse data offered within the ecosystem of the EMDS to contribute to the improvement of mobility and logistics services as well as to data management.

Other actors/crisis management

First responders and emergency services play a crucial role in responding to accidents and incidents involving mobility and logistics operations, generating valuable data that may be shared within the ecosystem of the EMDS.

While this section focuses on stakeholders within the mobility and logistics sector, it is worth noting that other sectors, such as energy, tourism, and healthcare, will also benefit from enhanced data discoverability via the EMDS.

Value proposition

The value proposition addresses the needs and requirements of multiple stakeholders in the ecosystem, describing how a common EMDS creates and captures value for them. The widespread adoption of the data spaces concept depends on the creation of value for all stakeholders involved while maintaining a reasonable level of effort and cost. This notion of value extends beyond mere monetary gain encompassing societal, environmental, or other benefits important to the multiple stakeholders.

The core value proposition of a common EMDS is to enable accessible, interoperable, and trustworthy data sharing and usage between stakeholders in the European mobility and logistics sector as well as with those in other sectors. Data sovereignty and trust are now of essence for the European mobility and logistics sector to develop and implement an intelligent and sustainable transportation system. A common EMDS will provide a technical infrastructure and governance mechanisms catering to the specific needs of the multiple stakeholders involved, which are further discussed in the following chapters.

In addition to the main value proposition, differentiated value propositions for the business models of individual actors can also be considered. The business model of a data space should enable its participants to create value according to their respective use cases and their business models, utilising the common EMDS as a springboard to create new products and services.

The DSSC suggests the following business case patterns and benefits for individual actors[58]:

Pattern	Business Rationale	Business Case Implication	Example
A	Cost Sharing	• Ecosystem members share data to cope with a shared requirement (compliance, process efficiency, transparency) • Every member saves money and time by sharing the burden	Catena-X, SC SN
B	Joint Innovation	• A customer innovation can only be realized by ecosystem members working together • No single ecosystem member has all the necessary data	Mobility Data Space, EDNA-X
C	Combined Forces	• Ecosystem members team up to prevent monopolies from emerging • No single ecosystem member has the necessary resources and commitment to do this alone	gaia-x, EuPro Gigant
D	Shared Marketplace	• Ecosystem members team up to provide quality-assured, easy access to data of a domain of common interest (open data, business partner data etc.) • Transaction costs go down for all ecosystem members	Catena-X, Mobility Data Space
E	Greater Common Good	• Public and private sector share data for a greater common, societal goal (e.g. climate protection)	Mobility Data Space

Figure 9: DSSC summary of business case patterns for data spaces.

[58] Data Spaces Support Centre (2023), "Starter Kit Version 1.0", https://dssc.eu/space/SK/35520539/3+Business%3A+Value+and+Models.

The DSSC suggestions (Figure 9) involve cost sharing, referring to a business case where multiple stakeholders capture value through sharing data-sharing costs. The EMDS could also foster value creation through joint innovation. In such cases, at least two stakeholders within a common EMDS, such as a scooter-sharing company and a public transport operator, collaborate to innovate a new service which improves last-mile services to attract people who live in the outskirts of a major city. Participants of a common EMDS could also combine forces to strengthen their market position or to deter untransparent or monopolistic behaviour of large firms, for example in the provision of digital mobility services. In addition, the EMDS could serve as a shared marketplace or foster data sharing for the greater common societal good, exploiting commonalities and economies of scale and scope across multiple mobility, logistics and adjacent data space instances as part of its joint funding model.

3.3. Key activities of a common EMDS

Central to the success of the business model is the definition of the actions and services that the EMDS must undertake to meet the value proposition and the needs of the stakeholders. In the most general sense, the business model of a data space is essentially multi-faceted, encompassing activities that span technical, strategic, and organisational dimensions. This section provides an overview of the key activities which will be discussed in more detail in the following chapters of this report.

The most extensively discussed aspect comprises the technical dimension. The core offering of a data space is a state-of-the-art technical infrastructure that allows the easy and scalable connectivity for numerous stakeholders. Providing easy technical access for stakeholders with limited technical skills or resources is a crucial activity for a common EMDS. This may include Small and Medium-sized Enterprises (SMEs) or small public authorities.

The strategic dimension supports the realisation of the members' business models by helping them to find partners to share data, know-how, and resources, allowing them to leverage any kind of benefit through innovation, efficiency increase, synergies, cost sharing, and asset monetisation. Moreover, a data space inherently offers a business community enhanced opportunities to form partnerships around data. For example, SMEs might be able to interact with larger players which were previously inaccessible to them, and larger players have a platform to connect with highly specialised data and service providers, creating opportunities that were previously beyond their scope.

The collaborative aspect is closely linked to the organisational aspects of a data space business model focusing on the criteria of trust, governance, and participation. A well-regulated, transparent, and continuously learning organisation is crucial. This involves decision-making policies which allow each stakeholder to shape the evolution of the data space.

Stakeholder expectations toward data space services

Expert workshops and the interviews provided a better understanding of the more specific expectations and needs of the stakeholders within the ecosystem and prospective participants of a common EMDS. These insights can serve as a foundation to determine the key activities of a common EMDS. In one of the workshops, the experts were divided in three separate different groups and asked to rank the services of a data space according to their own requirements by priority. Presented with choice of twelve services as options, the following rankings were derived, as shown in Table 7:

Table 7: Ranked responses on preferred data space services.

Rank	Services a data space administration should provide to its members (N=35)
1	Policies definition/enforcement
2	Operate the tech platform (engage/control a contracting entity)
3	Coordinate the specification of tech components/standards

Rank	Services a data space administration should provide to its members (N=35)
4	Enable all members having “a voice”/democratic decision-making
5	Provide trainings/consultation about data space matters
6	Coordinate the development of tech components
7	Coordinate the implementation of use cases (for selected subgroups of members)
8	Internal conflict resolution
9	Engage in specifying use cases
10	Organisation of internal forums/conferences
11	Organisation of public conferences
12	Active external networking

It can be concluded from these results that the definition and enforcement of policies are important to potential participants of a common EMDS. This means, they place a high value on the organisation of the data space as well as on transparency, clear definition and control of processes. This finding emphasises the importance of focusing on governance activities and the development and enforcement of a set of principles, standards, and policies tailored to the needs and requirements of the multiple stakeholders of a common EMDS. Additionally referring to governance activities, the experts value having “a voice” and opportunities for the participants to influence the evolution of the organisation.

The experts of the workshop particularly highlighted the importance of the technical infrastructure and the governance of technical standards. The main activities of a common EMDS, in accordance with the core value proposition, should encompass enabling interoperable data sharing through a common interoperable technical infrastructure in line with the emerging technical grounding for data spaces (Chapter 6). For example, discoverability through a joint metadata catalogue substantially improves the findability and accessibility of mobility and logistics data. To date, this data exists in fragmented data silos maintained by their respective owners and is often not available through the web. In addition, the data is difficult to locate for various actors due to the diversity of descriptions provided in different natural languages and formats, e.g. when attempting to identify mobility data from several European cities across multiple boarders for urban city planning applications. A common EMDS metadata catalogue allows proper documentation of metadata and descriptions alleviating participants from the arduous and time-consuming task of searching for existing data sets through search engines and open data portals.[59]

The lower rankings of the other services, such as engaging in specifying use cases and active external networking, do not imply that these aspects should be neglected in a common EMDS. For example, even if not identified as a key activity, the EMDS should still aim to help stakeholders in the mobility and logistics sectors build stronger communities. Enhanced interaction and collaboration between participants can foster joint innovation and synergy that creates value for the participants, as discussed in the previous section.

[59] Farrell, E., Minghini, M., Kotsev, A., Soler Garrido, J., Tapsall, B., Micheli, M., Posada Sanchez, M., Signorelli, S., Tartaro, A., Bernal Cereceda, J., Vespe, M., Di Leo, M., Carballa Smichowski, B., Smith, R., Schade, S., Pogorzelska, K., Gabrielli, L. and De Marchi, D. (2023), “European Data Spaces - Scientific Insights into Data Sharing and Utilisation at Scale”, EUR 31499 EN, Publications Office of the European Union, Luxembourg, JRC129900.

Barriers for stakeholders to register for a data space

During the interviews, experts from entities currently not participating in a data space were asked about factors that hindered them from connecting to an existing mobility data ecosystem. The open-ended questions encouraged the experts to respond in their own words and allowed for meaningful insights. The following responses were received, clustered into the categories “governance and trust”, “data features”, “technical” and “value added” as depicted in Table 8.

Table 8: Clustered expert responses on barriers for registering for a data space.

Cluster	Responses (N=14, 2 were not evaluable)
Governance and trust	• Security concerns and uncertainties regarding whom to trust • Complexity of standards landscape • Long and complicated internal decision-making and general hesitation to share data
Data features	• Not enough concrete information on data content • Worries that data in a data space is less up to date than from the original source
Technical	• Lack of technical knowledge • More technical tools required • Lack of technological maturity of the data ecosystem • Existing data ecosystems do not comply with key technical standards
Value added	• Many initiatives and brand names (“who does what?”) • Benefits of participating are unclear, incl. at national level • Lack of support for key use cases, e.g. event-driven for logistics

This set of responses are not representative but provide an insight into the sentiment among potential future EMDS participants. Most concerns dealt with the ease of use of the supporting technology (4 responses). The experts expressed doubts that the technical infrastructure might be immature or too complex to work with. They were also concerned about the governance framework and trust (3 responses), as well as the value added for the participants (3 responses). In general, the responses indicate a lack of understanding and awareness of the benefits of a data space. These findings underscore the need for key activities of a common EMDS to include an information dissemination and communication concept. Such a concept should be directed at stakeholders in the ecosystem who are not familiar with the data space concept.

In addition, during an expert workshop, participants were asked about factors that may serve as obstacles to the operation of a data space, causing them to hesitate to proactively initiate a data space. The responses to the open-ended questions have been clustered into “financial”, “effort”, “knowledge”, “strategy” and “other” operational obstacles, as listed in Table 9.

Table 9: Clustered expert responses on obstacles to operate a data space.

Cluster	Responses (N=14, 2 were not evaluable)
Financial	• Lack of resources • Need for significant pre-investment • Difficult to monetise for a commercial entity • Scale or networks effects are needed to make it work
Effort	• Major effort involved • Heavy administrative load
Knowledge	• Lack of (technical) knowledge

Cluster	Responses (N=14, 2 were not evaluable)
Strategy	• For most businesses, the data space is not the goal but the means to achieve something • Waiting to become a member of a larger broadly organised data space, or join/create a specific data space under the umbrella of a larger one • Data is not the major business focus/not applicable • No mandate for creating a data space
Other	• Very early stage of development

The obstacles listed in the table are consistent with the findings from the interviews. Both show that parties who act as potential data providers or consumers are unwilling to independently set up a data space or interact with their potential partners. The concerns of most experts revolve around the difficulty of accurately assessing the effort and costs involved in advance. In addition, the financial and strategic obstacles mentioned suggest that single players are interested in sharing data for their business, but do not view data sharing as part of the business. These findings suggest that interested stakeholders may expect that larger actors (e.g. public parties) with sufficient public and private resources to take the initiative to set up a common EMDS. Smaller actors, primarily interested in providing and/or consuming data, can be onboarded at a later point in time and assigned the status of non-managing members. This first-mover hesitance suggests both the infancy of the data economy in Europe and a clear mandate for public seed funding for the EMDS and other big national or sub-sectorial initiatives.

3.4. Funding models

The discussion of a business model also involves considerations related to funding of data spaces. This section addresses the different funding models that are commonly used by data spaces and could also be applied to a common EMDS. Funding models are closely related to governance models, discussed in the next chapter.

Findings from stakeholder consultations

Results of a survey that asked participants for the financing models favoured by other data sharing initiatives are presented here. The results, shown in Figure 10, indicate a strong reliance on public funding. Membership and transaction fees are frequently considered or used to complement public and private funding sources. In addition, the ten respondents who answered “Other” pointed to their mixed public/private funding scheme.

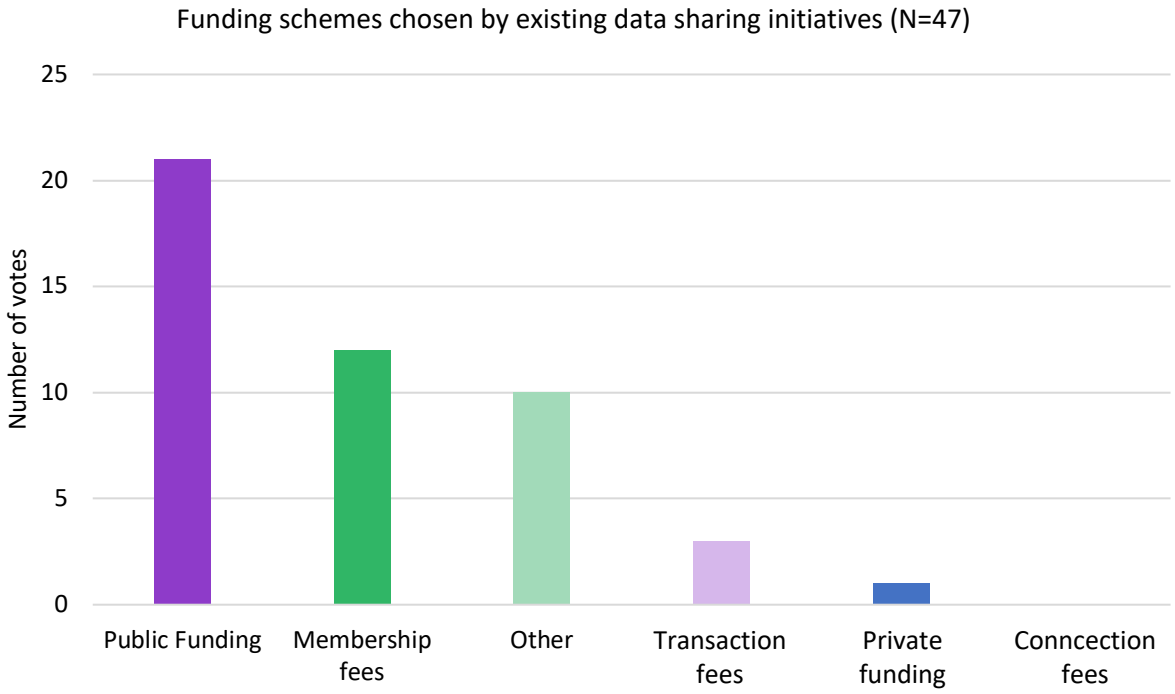


Figure 10: Responses on funding models of existing data space initiatives.

The survey participants were also asked about the type of organisation they represent. As shown in Figure 11, in alignment with the findings on funding schemes, public organisation types were the most frequent among the data sharing initiatives surveyed. In addition, larger initiatives adopted a large-scale scope (especially Catena-X, MDS, Fintraffic and EONA-X) all dedicated to a non-profit principle. Interestingly, the private, commercially active companies were all SMEs.

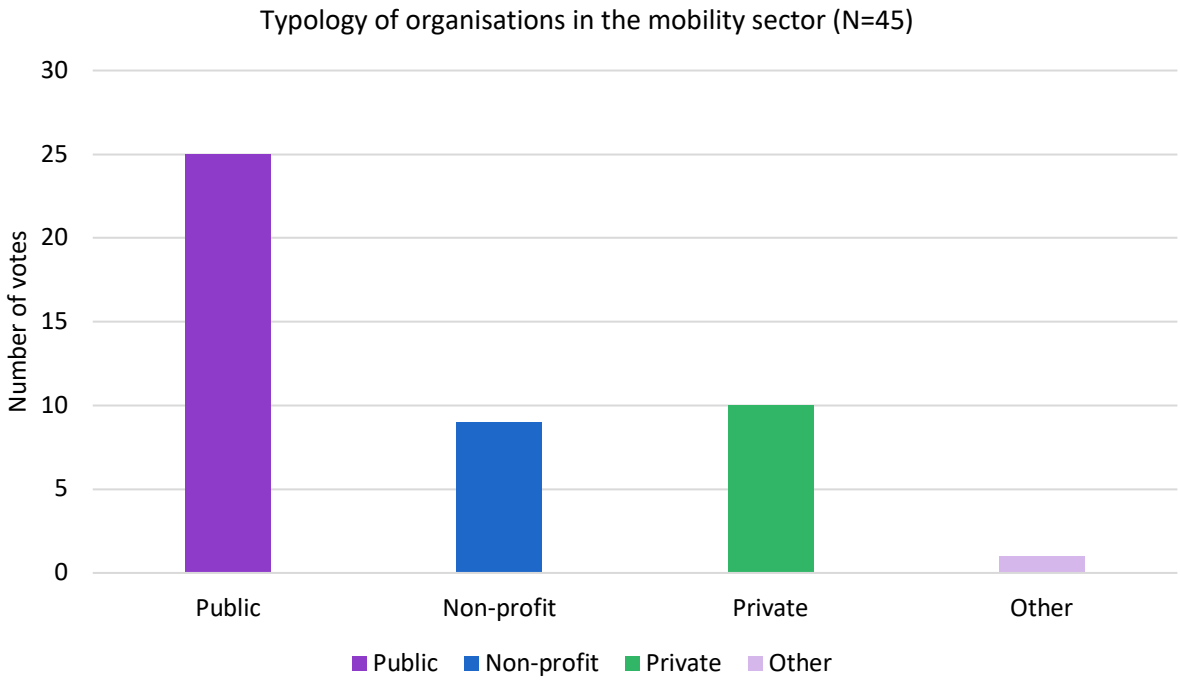


Figure 11: Responses on organisation types of existing data space initiatives.

Besides asking experts from active data space initiatives about their funding and organisational models, potential participants at the expert workshop were also surveyed regarding their preferences or the organisational type of a common EMDS. The results indicate a clear preference for organisational types that are predominantly associated with non-profit objectives, specifically associations and foundations (Figure 12).

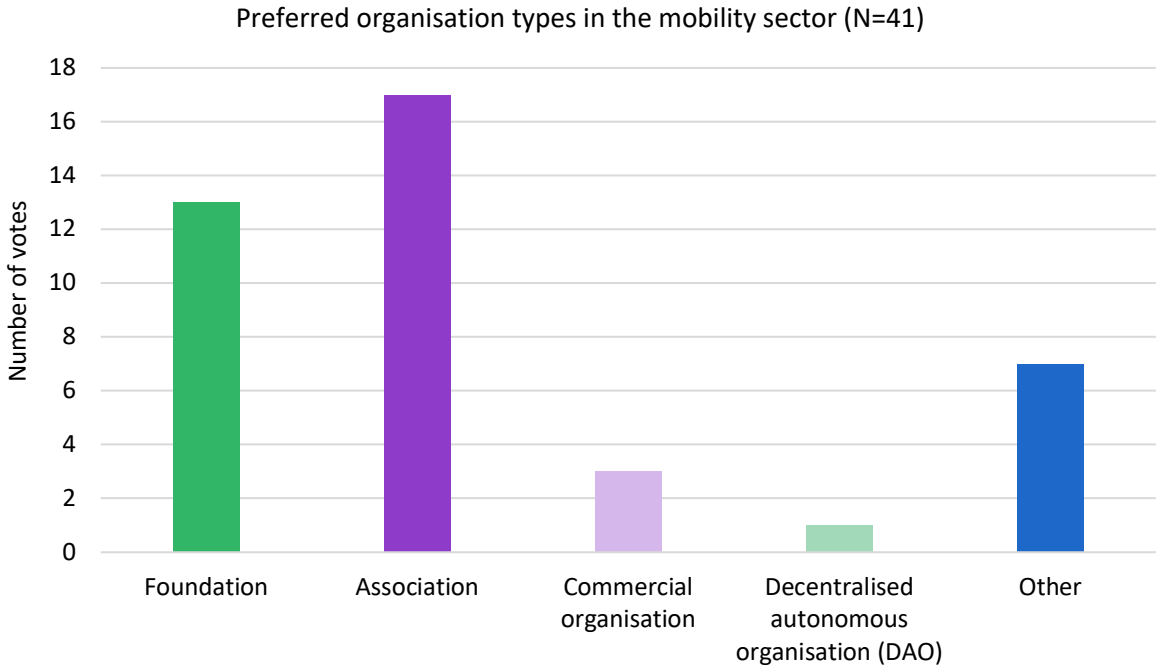


Figure 12: Responses on preferred organisation types for a common EMDS.

Best practices of funding models

These results offer important first insights into different funding models used by existing data sharing initiatives. Some are purely profit-oriented organisations while others rely solely on public funding. Additionally, there are some initiatives with mixed public-private funding. In this paragraph, the best practices of funding models are discussed and the suitability for a future common EMDS.

Only a minority of the initiatives meet the classification criteria for data spaces as per the DSSC definition. This limits the extent to which their business models can serve as examples for EMDS funding models. The analysis also considers commercial, profit-oriented companies that provide a Data-Space-as-a-Service and cater to customers using their services (e.g. Sovity GmbH, Nexyo GmbH, Vesputi GmbH, Dawex).

Generally, a profit-oriented approach could be a viable option for a common EMDS. Profit-oriented data space providers might be incentivised to invest in quality, security and innovation to create long-term value for their customers. However, there are also risks that warrant consideration. First, members need to shoulder these investments collectively, which often only works if short-term monetary benefits can be expected. Second, concerns about financial viability move to the forefront of daily business considerations, potentially jeopardising these important long-term investments. In addition, there is a constant need to strike a delicate balance between attractiveness of fees and business viability, which leaves the initiative vulnerable to membership attrition before long-term benefits can be realised.

Moreover, the administration of a data space by a single actor carries the risk that, in the event of financial or economic crises, that actor may not have the means to shoulder all the financial challenges. This scenario could also apply to a Private Limited Company when operated by a single entrepreneur,

because, in such cases, the associates are not obligated to provide financial support in case of any financial difficulties.

The situation differs slightly for a single actor under public law, as they cannot, by default, become insolvent. For example, a representative from Fintraffic, a company wholly owned by the Finnish state, explicitly highlighted that Fintraffic cannot go bankrupt. The representative further emphasised that this form of sustainability instils trust among the Finnish mobility stakeholders in the initiative[60]. However, the risk remains that a state-owned company fails to operate sustainably and could eventually face dissolution or privatisation.

Fintraffic's Traffic Data Ecosystem[61] and all Gaia-X's lighthouse data spaces share another key property explicitly embedded in their business model: a non-profit philosophy. The non-profit policy is typically established in the charter of the respective initiative. This serves as another pillar to ensure neutrality towards the businesses of the data space participants and to enhance their trust in the administration of the data space. The survey results discussed above showed that most respondents preferred an organisational form associated with non-profit orientation, such as an association or a foundation. This further validates the observation. It is recommended that a common EMDS adopts a non-profit philosophy, signalling to stakeholders that their interests are at the heart of all activities, free from any focus on gains for the data space governance authority.

Moreover, public funding should be particularly considered when a data space is considered a common good that aims at facilitating social innovations. In general, European stakeholders may not necessarily perceive the data space concept as preferred option for data sharing. Existing hyperscaler technologies are also able to efficiently support most commercial use cases. The collaborative approach in a data space may imply more individual efforts and enable more long-term collective benefits. This requires convincing arguments and proven success stories that stakeholders turn to a data space over an existing hyperscaler technology[62]. Financial incentives can be a valuable tool to attract a specific group of participants (e.g. SMEs, start-ups, non-profits, or small municipalities/public authorities), and support pursuing a specific societal and economic fairness goal. Public funding could reduce the required membership or subscription fees, either over an extended period (or permanently) for all participants, or only as a temporal incentive for a specific group.

For a common EMDS, public funding plays an important role because different EU Member States pursue strategies, ranging from the provision of a full public infrastructure alongside the physical infrastructure to adopt a seed funding approach of self-sustaining marketplaces. In addition, public funding becomes even more relevant if the business model of a common EMDS aims to become a European data space model that supports the EC and national governments in promoting best practice standards and compliance with data legislation. Such a data space model could serve as a demonstration of how to achieve compliance with the complex body of EU and national regulations while simultaneously pursuing societal and economic goals.

A common EMDS will encounter similar challenges that are faced by larger data space initiatives. It must not only integrate multiple stakeholders with different needs and requirements into a unified ecosystem but also existing national initiatives, such as those from Finland, Germany, and France, as well as existing European flagship projects (Chapter 4). Importantly, along with the political commitment to establish the common European data spaces as model implementations, this technical

[60] Fintraffic, on the other hand, is a financially potent company with an annual revenue close to €250 million, coming from various services sold to mobility stakeholders (predominantly air traffic control and naval control) bound to Fintraffic by legal obligations. The part of Fintraffic's activities dedicated to data exchange is still a minor business branch which is financed by transaction fees.

[61] See Fintraffic (2023), "Vision and objectives", https://www.fintraffic.fi/en/fintraffic/vision-and-objectives.

[62] There are certain parallels to the collective action problem in economics. This describes a situation in which individuals would be better off collaborating but fail to do so because of conflicting interests between short term individual profit or high initial investments and the long-term benefits reaped.

and organisational pioneering work demonstrates the possibility of sustainable data sharing despite complex EU data and sector legislation. This emphasises public funding as an important vehicle for a common EMDS in the initial stages (and possibly beyond), enabling learning, growth and maturation while facilitating the successful implementation of sustainable use cases. The public funder can gradually withdraw as soon as full organisational and financial self-sustainability seems attainable.

Besides models based on either private or public funding, there is the strong tendency to cover the costs through contributions from both the government and the shareholders as well as members of the data space. Major existing German initiatives in mobility (Catena-X and MDS) were initiated as mixed public-private funded projects. However, when these initiatives reach a mature status with sufficient members and established use cases, they plan to switch to a fully member-funded model. Membership fees can be structured on a sliding scale depending on various criteria. For example, Catena-X applies a scale of membership fees depending on the annual revenues of its members, with larger companies paying higher fees than smaller ones. Other data spaces feature a dual-tier membership structure to cater for diverse members. One tier is reserved for members assuming leading roles in the organisation (e.g. as members in the executive board, steering and designing technology/governance, executing decided actions, often accompanied by in-kind contributions). The second tier caters for those that wish to be data providers or consumers only (e.g. EONA-X and MDS). Moreover, the MDS is attracting interested members with free membership until the end of 2024. The organisation's expenses are covered by contributions from the founding members (50%) and public funding from the German federal government (50%). These observations highlight the important potential impact of the funding model. Introducing a tiered membership fee structure can serve as a powerful tool to attract and support SMEs as well as other potential members who may still have concerns to participate.

A strong preference has been identified for a mixed public-private funding in the mobility and logistics stakeholder consultations at public events. Participants believed that the inclusion of a private component, either in the form of membership fees or subscription fees, was justified due to the economic benefits that members might gain from participation. However, the public contribution was considered as a safeguard to ensure that profit orientation would not dominate the business model and that neutrality of the EMDS would be assured. Some participants preferred a triple funding model, combining private funding, public funding, and activity-related funding through transaction fees. This model would have a broad base of funding by levying charges on both active and inactive members. It is partially applied by Pontus-X, a non-profit cross-sectoral data space, where they charge a moderate membership fee (max. 1000 euro per annum) and a minor community fee for each transaction. However, the financial viability of this model is difficult to foresee as it remains unclear if the income generated is sufficient to offset the costs for the parties involved. The increasing popularity of various commercial offers of data spaces-as-a-service still shows that cost-efficient data spaces provision could be achievable, offering profit opportunities for both the data space provider and its members. Importantly, all examples of data space initiatives discussed above have only been in existence for a few years and their long-term financial viability has not yet been fully demonstrated.

3.5. Recommendations

Conclusions

The analysis showed that stakeholders in the ecosystem still have multiple concerns about participating in a data space initiative. The business model of a common EMDS faces the challenge of establishing a sustainable and resilient framework that sufficiently addresses the diverse needs and requirements of stakeholders of the mobility and logistics sector and beyond. Several interviews, stakeholder consultations, and data space self-descriptions have confirmed that the value proposition for a common EMDS revolves around enabling secure and sovereign data exchange. This requires key activities to be focused on maintaining a cutting-edge technical infrastructure and appropriate

governance mechanisms. In addition, the funding model is a key consideration in the establishment and maintenance of a common EMDS. The following recommendations address stakeholders' needs and conditions for participating in a common EMDS.

Recommendations

Offer a data sharing ecosystem that supports discoverability, data sovereignty and trust

The core of a common EMDS business model lies in its value proposition. To ensure the success of the EMDS, it is essential to offer a robust set of technical and organisational measures that address the needs and requirements of the participants. These measures should promote the discoverability and accessibility of a wide range of data services, allowing data sharing between numerous participants; instil trust among the participants and ensure confidence in all data resources and services offered; empower data providers to define their own usage conditions and enable adherence to these conditions.

Act as a neutral agent for all participants

There is a strong preference among stakeholders for an impartial governance authority as the data space administration that manages all aspects of collaboration within the community of data space members. Fair and unbiased decision-making plays a key role for participants in the management of different aspects of a data space (e.g. organisation, technical infrastructure, communication). Several existing and matured data space initiatives have adopted this approach. For example, they have established an executive board whose members are elected by the partners. Entities intending to act as a governance authority are supposed to abstain from participating in data exchange activities. This is particularly the case with commercial enterprises providing a Data Space-as-a-Service to their customers. They provide and organise the platform and offer additional services but are not involved in the use cases of their paying customers.

Provide an up-to-date technical infrastructure aligned with the generic EU data space approach

Providing a technical environment that enables scalable data sharing is of essence for fulfilling the defined value proposition for a common EMDS (see Part IV of this report). To facilitate interoperability, the technology must be aligned with the technical building blocks identified in this project (Chapters 7, 8, 9), and with the generic building blocks recommended by the DSSC. A common EMDS may adopt the Gaia-X/IDSA/Eclipse Dataspace Components (EDC) technology already used by the Gaia-X lighthouse projects in the mobility sector from the beginning, if it aligns with the DSSC. The use of such European standard technology would allow a future common EMDS to connect to other data spaces and offer its members a continuously growing network of potential partners[63]. Ensuring the viability of the business model relies on providing an up-to-date technology, which requires continuous efforts to maintain its relevance over the long term. This circles back to other aspects of the business model, namely to the promise of sound governance and member participation. To continuously maintain a technological strategy that meets the requirements of the participants' use cases, the data space should coordinate and facilitate the identification and implementation of technical services by organising communication and consultation between the participants. It should also participate in any overarching (cross-platform and cross-sector) initiatives which drive the evolution of the data space technology. Discussions around business and technical requirements need to be enriched with legal

[63] The providers of data spaces often emphasise the use of IDS- or Gaia-X-compliant software to operate the data space as a quality indicator, e.g. EONA-X, Catena-X/Cofinity-X, MDS, Nexyo GmbH, Sovity GmbH and FENIX. Public actors in some EU countries have also pledged to adopt the technology. The German NAP, operated by the Federal Highway Research Institute BASt, has already installed an EDC connector. MobiData BW in Federal State Baden-Württemberg, the Urban Mobility Platform in Hamburg and NRW and Mobidrom in North Rhine-Westphalia, are planning to connect to the MDS and implement an EDC connector. Moreover, the Tourism Data Space in Austria and other data initiatives within the mobility sector in the Netherlands intend to also use the EDC.

and compliance considerations. These need to be dealt with through agreed-upon processes of risk, requirements and change management to be traceable and influenceable for the participants. Mature data space initiatives (e.g. Catena-X/Cofinity-X, MDS, EONA-X and Fintraffic) have all established technical committees or working groups to plan the technical evolution of their respective initiatives.

Enable easy onboarding of participants

Crucial to both the technical and the strategic dimension of an EMDS business model is offering low-threshold access to the data space by providing easy-to-use technical components and instructions on how to get started. Many interested stakeholders mentioned a lack of technical familiarity as an important barrier for participating in a data space. This issue seems to be particularly relevant for SMEs and start-ups. The most effective offer of easy technical onboarding is the "Connector-as-a Service". This enables a data space connector (e.g. an IDS connector or EDC connector, Chapter 6) to be readily prepared for download and installation and configuration within the premises of the participant. This service is one of the most advertised features by existing commercial data space providers (nexyo GmbH, Sovity GmbH, Cofinity GmbH, Dawex and MDS). If the concept is not fully understood and convincing, interested stakeholders in the ecosystem may be reluctant to take the risk of allocating resources to participate. This barrier could be overcome by temporarily offering free-of-charge services to a specific group of participants (e.g. SMEs and start-ups). For example, the MDS attracted data providers and consumers by offering free participation in the data space, while the founding members and public authorities funded the establishment and development phase of the MDS ecosystem[64].

Support the evolution and uptake of standards for data and application quality

The key activities of a common EMDS should also include ensuring the quality of services and data. While data space participants value the availability of large amounts of data, they are often concerned about the formats of the data. It is crucial for a common EMDS to prioritise the governance of the quality of data, define generic criteria and facilitate ready-to-use data offers. Harmonisation of data models and data exchange APIs (Chapter 7) will be a key aspect. This can be achieved through the implementation of a data governance board or a comparable institution within the data space, unless general directions and guidelines are developed at EU level, for example, by the EDIB. Such a procedure is certainly also applicable when sharable applications and services are offered to the participants via an app store. Similar to the certification of participants via verifiable credentials, Catena-X/Cofinity-X has implemented a certification schema that defines criteria for approving proposed services.

Facilitate the implementation and acceleration of use cases

A further key activity of the EMDS should be to facilitate and coordinate the identification as well as implementation and acceleration of use cases. Data drives innovations that can be translated into use cases and concrete applications in the mobility and logistics sector. Successful examples implemented and accelerated use cases can be an important factor for stakeholders in the ecosystem to participate in a common EMDS to access desired data. In addition, ideas for promising use cases might attract stakeholders who possess the desired data. Such matchmaking activities can be facilitated by implementing appropriate formats of collaboration within the community of common EMDS participants and effectively communicating these benefits to potential participants. These activities should focus on but not be limited to the mobility and logistics sectors and should also explore cross-sector opportunities for use case development. Such formats could include use case fairs, brainstorming sessions, datathons or hackathons, such as those organised by the MobiDataLab project, or permanent working groups. EONA-X, for example, has a working group that focuses on identifying use cases, managing the formation of use case specific task forces, and assessing and evolving use

[64] However, this situation is expected to change by 2025, following the cessation of public funding. The MDS is then planning to sustain itself solely through member contributions.

cases following an agreed process. The increased interaction and engagement, in turn, facilitate the building of a strong community that can help a common EMDS in fostering loyalty, attracting participants and driving growth.

A common EMDS should swiftly be embedded into the European mobility and logistics sectors, given the complex landscape of existing and emerging data space initiatives and major opportunities for developing use cases and to interconnect with adjacent sectoral data space initiatives including tourism, smart cities, built environment, sustainability, energy, and more. There are major opportunities to capitalise on both economies of scope and scale, as the value of the EMDS increases with the participation of more stakeholders. By fostering an ecosystem that connects these diverse stakeholders and promotes data sharing across various data spaces, there is potential to pave the way for innovative solutions and novel business models. However, the market has not naturally forged such links, hence the need for a proactive EMDS.

Support the adoption and sustainability of the data space through public funding

In general, the costs of setting up the technical and organisational structures of a data space should be covered by the participants who benefit from the service provided to them. Commercial data space providers usually establish membership or transaction fees, and this can also be the case for non-profit associations with different legal forms. However, public funding can be a useful tool for facilitating a common EMDS, especially in the initial stages. First, there is political will to enforce the implementation of data spaces over alternative concepts, such as legacy data exchange and hyperscalers, and the direction of this development can be steered by the conditions under which public funding is provided. Second, the data space concept has not yet been fully validated in practice, and many potential participants are still hesitant to engage in data spaces. Public funding can help to mitigate the financial risk for interested private stakeholders.

3.6. Building blocks

Figure 13 shows the individual building blocks recommended for business and funding models.

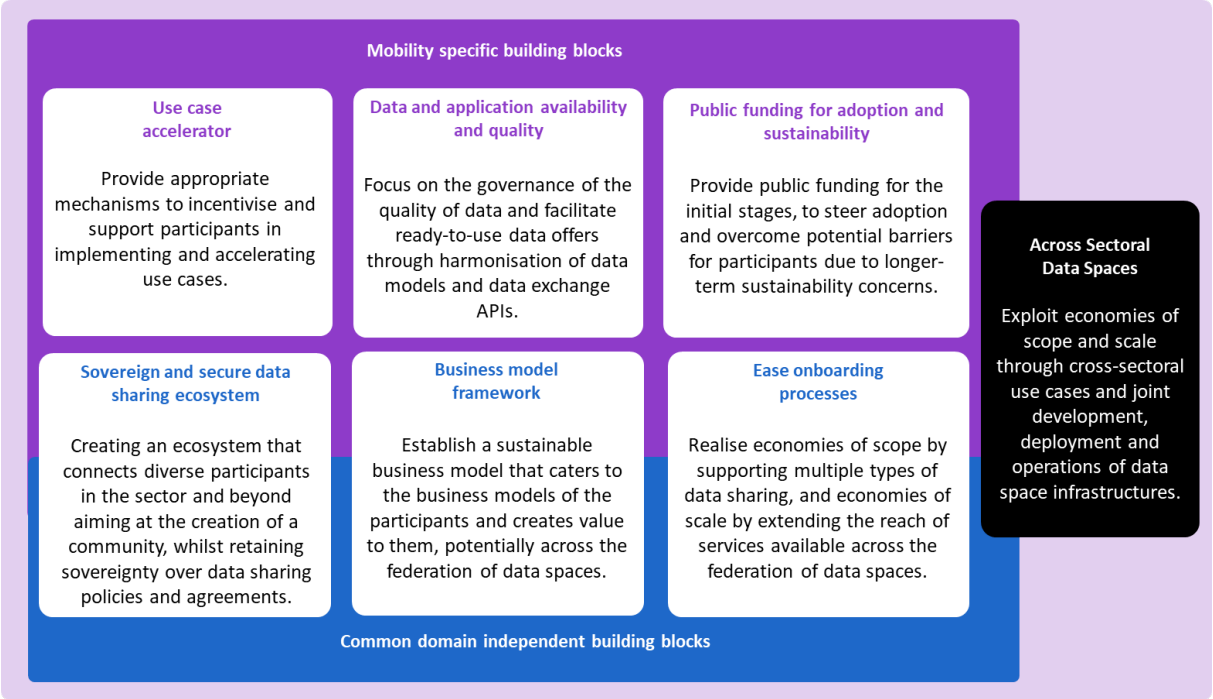


Figure 13: Building blocks for business and funding models.

4. Governance framework

4.1. Introduction

At the heart of any successful data space initiative lies the task of developing a robust, efficient and adaptable **governance framework**. The governance framework serves as the foundation upon which the entire data space operates, encompassing the rules and practices that govern how data is managed, shared and utilised. The establishment and maintenance of this framework are crucial for enabling its participants, data services, IT resources, data sovereignty, trust and discoverability, and ensuring these under the conditions of compliance with legislation, ethical standards and interoperability. Governance frameworks are expected to implement the DGA, DA and other regulations by default. These are derived from the concerns of responsible data governance and further explored in the next chapter covering legal aspects.

Within the context of a data space initiative, the term "**data space authority**" assumes a key role. It refers to the entity or partner responsible for creating and upholding the **governance framework**. This body not only plays a key role in shaping the data space's structure but also takes on the vital responsibility of overseeing its ongoing operations. A **key task for the EMDS is harmonisation and interoperability** between the different active data spaces in mobility and logistics and specifies the elements that are vital for cross data space collaboration.

This chapter provides an overview of the key aspects of data space governance for mobility and logistics, summarising several fundamental considerations for the EMDS. Further, it proposes an overarching framework characterised by a multi-level and bi-directional governance structure, complemented by the organisational and technical governance that ensure at least the following capabilities for interoperability:

- Data sovereignty and trust;
- Data value creation (data and participant discoverability).

Section 4.2 presents the fundamental considerations that make collaboration around data particularly challenging in mobility and logistics. These should be considered as input for the EMDS governance structure and framework. Section 4.3 further elaborates on the requirements for the EMDS governance framework and identifies existing governance frameworks and agreements that can be built upon. Section 4.4 delves into the specifics of the EMDS governance framework, covering the organisational and technical aspects. Section 4.5 presents the conclusion, recommendations and the proposed building blocks for the EMDS governance framework and structure.

4.2. Fundamental considerations for EMDS governance

A variety of factors make collaboration around data particularly challenging in the mobility and logistics sectors. These factors need to be taken into account when designing an appropriate governance framework. Stakeholder consultations, questionnaires, and exchanges with experts point to five fundamental considerations for a future governance framework of the EMDS:

- Balancing public and private interests;
- Addressing power asymmetries and data monopolies;
- Reconciling societal values and financial viability;
- Incentivising cooperation in mobility and logistics;
- Managing an ecosystem of sovereign actors and data spaces.

Balancing public and private interests

The key success factor for data collaborations is the strategic alignment between actors. However, reconciling these interests is complex. Achieving a balance between the interests of public and private entities while coordinating across different geographic levels and diverse stakeholder landscapes will become a central challenge for the EMDS.

The EMDS might also encounter difficulties in reconciling a common strategic vision between stakeholders. For example, when private organisations take the lead in shaping the governance and operational model of a data space, there is a potential risk of excessive focus on data monetisation and business-driven use cases. While such endeavours can result in efficiency improvements and environmental benefits, as seen in logistics where enhanced information in supply chains reduces resource and fuel consumption, there are scenarios in mobility where data-driven services from private providers (e.g. free floating car and scooter sharing schemes) might divert people from more sustainable modes of transport (e.g. walking, cycling or public transport).[65]

Addressing power asymmetries and data monopolies

A significant challenge in the governance of data spaces is dealing with power imbalances among stakeholders, including between shareholders and members, and between stakeholders and the data space entity itself. This challenge arises because members often possess more substantial resources compared to the data space entity or the instance they are a part of, potentially leading to a situation where the data space becomes overly dependent on its powerful members. This risk has been voiced by several existing data spaces, as it can result in greater influence being wielded by powerful actors seeking to impact organisational decisions and prioritise specific use cases.

The financial capabilities of a member can also significantly influence their willingness to join a data space, with wealthier members experiencing relatively lower costs of participation. In scenarios where data spaces need to establish a sustainable operational model rapidly, they may become susceptible to the interests of financially robust member organisations. In such cases, it may seem expedient for a data space organisation to initially attract a few prominent key players with substantial resources and expertise to ensure sustainability. Later, they usually have more resources to actively engage and onboard smaller organisations, such as start-ups and small municipalities, which often have limited IT and expert resources. These smaller entities typically require additional support for successful onboarding. Support for municipalities with the MDS, for instance, has been recently introduced through dedicated federal public funding.

However, attracting key powerful players initially may give rise to biases or path dependencies in the governance of data spaces. While funding models are discussed in more detail in Chapter 3, it is crucial to recognise that economic disparities in the early composition of data space membership can influence governance dynamics. Although democratic decision-making may be a core principle in the early stages, the specific makeup of the membership can introduce biases into initial organisational choices that may prove challenging to reverse later. In the development of online spaces and the internet, as well as online marketing more recently, large companies have been able to shape regulations, norms, and even the technical infrastructure in ways that benefited their business models. Existing data spaces such as the MDS in Germany acknowledge similar risk on a smaller scale and are

[65] For example, studies have pointed to situations where users of e-scooters primarily view these modes of transport as an alternative to walking rather than other motorised transportation modes. Evidence shows that shared micro-mobility seldom acts as a complementary element to public transport and that their emission is comparable to public transport. See International Transport Forum (2020), "Good to Go? Assessing the Environmental Performance of New Mobility", Corporate Partnership Board Report, OECD/ITF 2020. Another study confirms that adopters come mainly from public transport, walking, and cycling instead of replacing individual motorised vehicles. See Orozco-Fontalvo, M. et al. (2022), "Dockless electric scooters. A review of a growing micro-mobility mode", International Journal of Sustainable Transportation 17(4).

correcting potential biases by introducing support for smaller organisations via programmes backed by public funding. Furthermore, ensuring a balanced shareholder and membership landscape, along with a thorough requirements analysis and stakeholder dialogue, is important to address potential risks and to remain relevant for the use cases of smaller and less powerful organisations.

Reconciling societal values and financial viability

Data and digital business models are often driven by network effects. The more data a data space can offer, especially valuable data enriched with metadata descriptions from participants, the greater its potential value. This, in turn, can create opportunities for increased monetisation and foster the emergence of a new ecosystem of product and service providers.

Significant network effects are notably evident in traffic management, as demonstrated by platforms such as Waze and Google Maps. As more vehicles are monitored through these apps, the quality and accuracy of traffic data, including patterns and delays, improves. Consequently, drivers benefit from enhanced information, including more accurate time estimates and route suggestions. This also creates increased possibilities for targeted location-based advertising. However, the extensive collection and utilisation of such data in these apps also raise important privacy, ethical or antitrust concerns. Current debates around data collected automatically by vehicles also point to the need for harmonised and secure processes. These could be facilitated by data spaces. For example, stakeholder consultations carried out by the EC in 2022 regarding complementary legislation on the availability of in-vehicle data at the EU level pointed to a high interest in opt-out possibilities and transparency of the data shared by vehicle systems.[66]

Such complexities present a clear mandate for the EMDS governance framework to strike a balance between the application of strong ethical principles, individual privacy protection, and financial viability. It should ensure that data ethics dominate decision-making and technical choices by proposing rules and guidelines for responsible data sharing and usage. In addition, transparency and accountability should be core principles, and robust mechanisms for compliance and enforcement should be in place.

That said, while privacy and the protection of sensitive data are paramount, the framework should not stifle innovation. It should support initiatives to develop tools for data policy enforcement (e.g. further developing smart contracts) and privacy-enhancing technologies. Further, there are interesting opportunities for exploring new business models that prioritise privacy and data security, for example via specific techno-legal implementations. The technical means for implementing trust and security mechanisms in the EMDS are further explored in Chapter 8.

Incentivising cooperation in mobility and logistics

The EU's mobility sector encompasses various transport modes, each with distinct characteristics and governance models. These differences arise due to the unique operational requirements and market dynamics of each mode. The governance landscape is characterised by distributed governance structures, where decisions and regulations are made at supranational, national, and local levels. This distributed governance framework blurs the lines between public service obligations and market regulations, resulting in a complex environment for collaboration. Furthermore, there are significant differences between application domains, such as logistics, long-distance and urban transport, as they each present varying governance models and face diverse challenges.

[66] See European Commission (n.d.), "Access to vehicle data, functions and resources", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources/F_en.

Data spaces typically take the form of meta-organisations comprised of diverse members with varying interests, rather than a shared common interest among members. The term “meta-organisation” refers to organisations that coordinate entities, often with a non-profit orientation. The greater the diversity within this group, the more challenging it becomes to identify shared preferences and synergies. This presents significant difficulties when it comes to setting organisational priorities or selecting which governance or use cases to support.

Nevertheless, this diversity also carries certain advantages, particularly when complementary strengths can be leveraged. Through collaboration, diverse actors can combine resources and expertise to enhance data collection, analysis and dissemination. This, in turn, results in improved decision-making, more innovation and increased efficiency, leading to cost savings.

However, since these benefits often remain abstract or do not yield immediate financial gains, many stakeholders are hesitant to engage in collaborative relationships, especially when the positive outcomes primarily benefit society rather than the individual parties involved.[67]

Managing an ecosystem of sovereign data spaces

The mobility sector is rife with operational data sharing initiatives[68], signalling a vibrant ecosystem where data spaces are "living entities" in a constant state of evolution. These data spaces can emerge, merge, split, or even dissolve due to various factors such as resource constraints, obsolescence, or failure to meet evolving needs.

The EMDS faces the challenge of managing an ecosystem of diverse data ecosystems that are sovereign and autonomous in their organisational and technological choices. However, these ecosystems need to function in an interoperable manner and be supported in that ambition by the EMDS. The multi-faceted nature of mobility and logistics – intersecting with domains like energy, tourism, and the built environment – makes interoperability even more crucial. If certain aspects of trust and discoverability of data are not harmonised, this pose barriers to making data sources mutually accessible and reliable.

The EMDS has a vital role to play in harmonising this complex ecosystem. It must champion interoperability not just within the personal mobility and logistics sectors but also align with or extend this to adjacent sectors (energy, tourism, construction, etc.). This involves a proactive approach to bridging various (sectoral and geographical) regulations, implementation choices, and emerging data initiatives across countries and sectors.

In the broader context of evolving European data spaces, the ultimate goal is to form a federation of interoperable data spaces. This federated approach is referred to in this report as the concept of "inter data space interoperability”.

4.3. EMDS governance framework

The considerations described in the previous section point to fundamental requirements on the governance structure and framework of the EMDS. Traditional governance models, characterised by centralisation and rigid hierarchical structures, are increasingly misaligned with the objectives of extensive cross-border data exchange and rapid innovation. The dynamics and complexity of this landscape necessitate a shift towards more cooperative and agile governance models that can bring resilience and flexibility.

[67] See Encyclopaedia Britannica (2023), “Collective action problem”, https://www.britannica.com/topic/collective-action-problem-1917157.
[68] EU PrepDSpace4Mobility CSA (2023), “Data Ecosystems Inventory”, https://mobilitydataspace-csa.eu/inventory.

Ultimately, the governance framework chosen must reconcile fundamental requirements and build on the existing frameworks and best practices under development. Further, the EMDS governance framework should also take into account learnings from existing data spaces and use cases.

Requirements for the EMDS governance framework

As highlighted above, the EMDS ecosystem may encounter difficulties in reconciling a strategic vision and ambition between stakeholders. Steps to realise this aim involve transparency and open dialogues between public and private stakeholders from the beginning. Further, a balance in the ecosystem could be achieved by establishing appropriate governance mechanisms that:

- Ensure that **data ethics and data sovereignty** dominate decision-making and technical choices by proposing rules and guidelines for responsible data sharing and usage. In addition, transparency and accountability should be core principles, and robust mechanisms for compliance and enforcement should be in place.
- Define clear guidelines and specifications for data sovereign exchange, ensuring that **societal benefits are prioritised**, and regularly assessing the impact of data-driven services on societal and sustainability goals, possibly expressed in the basic principles, vision, and mission of the EMDS.
- Encourage participation from a diverse range of stakeholders, including start-ups, small municipalities and organisations with varying resources.
- Ensure a **balanced allocation of resources** for community management and support during onboarding and for various use cases. This approach can help address power imbalances and promote fairness and inclusivity.
- Propose guidance and ongoing **evaluation of potentially unintended consequences** of use cases to ensure that common principles are being met by participants.
- Establish a **coherent model for multi-level governance**, while acknowledging that data spaces are sovereign in deciding how to tailor their functional requirements and internal governance structure. Hence, where possible, principles of subsidiarity between levels of decision-making should be followed, with clear rules on which decisions are taken at the central level and which elements are under the responsibility of entities federated within the EMDS.

The last principle is of particular importance for the technical framework of the EMDS. Section 4.4 will address the core principle by means of a **multi-level governance** approach that works both “top-down” and “bottom-up”. **Specifications may originate from horizontal frameworks specified at the EU and global level, to** which the EMDS, as well as its federated data spaces, must adhere for interoperability. At the same time, mechanisms must be in place to feed **learnings and new requirements from use cases back into the EMDS governance framework** and from the EMDS to the horizontal frameworks.

For instance, a use case for a national logistics data space might reveal insights on event-driven interactions in container delivery. Consider a situation where changing ownership of a container, requires a new policy structure when the data entitled party changes (e.g. Delivery Duty Paid or Ex Works). This insight is not only valuable to other national logistics data spaces, prompting its adoption by the EMDS for similar use cases across the federation, but it also has implications for the overarching framework governing policy definition and registration. As a result, there needs to be ongoing alignment with these broader frameworks, integrating lessons learned and updated specifications from them.

Such an iterative and responsive approach underscores the core role and essence of the EMDS’ value proposition: By continuously learning across all interoperability levels (technical, semantical, organisational, and legal) of the New European Interoperability Framework (EIF), the EMDS can consistently add value to data spaces built on its specifications.

It is important to note that the considerations mentioned above represent only an overview of common principles that should be observed and need to be further specified with the future participants in the EMDS. The consultation of stakeholders should result in a detailed set of governance requirements building on existing governance frameworks, rulebooks, and agreement frameworks further detailed below.

Defining a governance framework based on existing frameworks

Each data space must develop a governance framework tailored to its use cases and to maximise value for its participants. This includes shaping and managing the data environment and overseeing processes such as development, onboarding, offboarding, and monitoring.

As described in the previous section, the EMDS organisation or governance authority needs to apply the governance framework in a fair and transparent way. It should also maintain commercial neutrality and earn trust with respect to data sovereignty and exchanges, as widely confirmed during project consultations and workshops (Chapter 3). The EMDS should fully adhere to horizontal legislation in the data domain and build upon common principles of good governance in accordance with European values, such as the ones promoted by the Council of Europe.[69]

Many governance frameworks are utilised across data spaces, including the mobility domain. For efficient EMDS governance, ensuring interoperability and avoiding redundancy is key. Leveraging **existing community-driven governance frameworks, rulebooks, and agreement structures** can be beneficial.

In data spaces, the term "rulebook" is commonly used to describe a governance framework. A rulebook encompasses a complete set of governance policies, operational guidelines, and procedures relevant to the creation, deployment, and operation of data spaces. It should clearly outline both mandatory and optional rules, as well as the responsibilities of the roles designated to implement them.

To select a suitable foundation for the EMDS governance framework, existing frameworks can be classified into two categories: those driven by active users and developers and those focused on harmonising advancements in data space technology without direct user governance.

The data sharing initiatives with governance frameworks by active users and developers include the following:

- **The IDSA governance framework**
  The IDSA governance framework addresses data space governance in the guiding principles as part of IDSA Rulebook[70]. Inspired by the Open DEI Design Principles for Data Spaces[71] and its previous Position Paper on Data Space Governance[72], four layers of data space governance are distinguished: (1) data space instance governance, (2) data space ecosystem governance, (3) data space domain governance, and (4) soft infrastructure governance. It provides recommendations on the governance elements that need to be defined.
  The IDSA Reference Architecture Model provides a comprehensive foundation for understanding data spaces and the roles and building blocks within them. The IDSA Rulebook provides a blueprint for bringing the IDS Reference Architecture Model to life. This includes

[69] Council of Europe (n.d.), "12 Principles of Good Governance", https://www.coe.int/en/web/good-governance/12-principles.
[70] International Data Spaces Association (2023), "IDSA Rulebook", White Paper, https://docs.internationaldataspaces.org/ids-knowledgebase/v/idsa-rulebook/front-matter/readme.
[71] Nagel L., Lycklama D. (2021), "Design Principles for Data Spaces", Position Paper, Version 1.0. Berlin.
[72] International Data Spaces Association (2021), " Governance for Data Space Instances. Aspects and Roles for the IDS Stakeholders", Position Paper, Version 0.1., https://internationaldataspaces.org/wp-content/uploads/IDSA-Position-Paper-Governance-for-Data-Space-Instances-Aspects-and-Roles-for-IDS-Stakeholders.pdf.

rolling out services and stipulating central procedures such as admission and withdrawal of members. It focuses on interoperability at the connector level and is managed by active IDSA members through specialised working groups.

- **The iSHARE governance framework**
  The iSHARE framework originated from the logistics sector and encompasses a trust framework[73] for sovereign business data exchange facilitating the establishment and management of data spaces. It specifies agreements on a legal, operational and technical level which allows for governance and interoperability on data sovereignty and trust for participating organisations within a data space and across data spaces. It provides governance and trust framework capabilities to support both individual data spaces (i.e., intra data space interoperability) and interconnectivity between multiple data spaces (i.e., inter data space interoperability). Both concepts are discussed below. Regarding interoperability within data spaces, the framework includes capabilities for participant trust registration and administration, participant discovery (the Data Space Participant Registry), status information as well as Authorisation Registry specification for federated data sovereignty. For interoperability between data spaces, it provides capabilities for data space profile registration, data space participant discovery, and status information across data spaces. An important role is the iSHARE Satellite that fulfils the role of data space authority (see also Section 8.4), which provides a certification procedure to validate the correct and trustful implementation of the data sovereignty protocols and standards. The iSHARE framework emphasises standardised Service Level Agreements (SLAs) to ensure efficient and effective data exchange. These SLAs cover metrics such as uptimes, response times and error rates.

  The iSHARE framework is actively maintained and governed by data spaces that use iSHARE as their trust foundation.

- **The Gaia-X governance framework**
  Gaia-X does not define an overarching governance framework. However, it does define both the Gaia-X Framework[74] and the Gaia-X Trust Framework[75]. The Gaia-X Framework defines the policies for data and infrastructure (e.g. cloud), including Gaia-X Technical Compliance to provide decentralised services on trust, policies and rules for data infrastructure and storage. Currently, Gaia-X accepts self-declarations from data ecosystems on compliance with this framework. The Gaia-X initiative is built on three pillars: the Gaia-X Association for Cloud and Infrastructure (Association Internationale Sans But Lucratif [AISBL]), the National Gaia-X Hubs, and the Gaia-X Community. Gaia-X members, who are responsible for operating data and infrastructures, govern its framework.

- **MyData**
  The MyData initiative[76], led by the Finnish government, provides the means to individuals to manage the usage of their personal data. It facilitates access to personal data while empowering individuals to exercise their rights and transfer their personal data between systems. Mobility is a key area that could benefit from its application (e.g. personal profiles in Mobility-as-a-Service applications). MyData's "Declaration for Personal Data Handling", is a legal declaration pertaining to data service providers (MyData Operators) and outlines rules and practices for personal data handling.

[73] See https://ishareworks.atlassian.net/wiki/spaces/IS/overview.
[74] Gaia-X (n.d.), "Gaia-X Framework", https://docs.gaia-x.eu/framework.
[75] Gaia-X (n.d.), "2. Gaia-X Trust Framework", https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/gaia-x_trust_framework.
[76] MyData (n.d.), MyData, https://www.mydata.org.

- **ANewGovernance**
  ANewGovernance[77] offers a framework for the governance of personal data within the data spaces ecosystem. The Brussel-based association is currently developing a framework consisting of four layers, each represented by an applicable rulebook. The first layer is the EU Rulebook, which provides the data space with a set of regulations and prescriptions from the EC. The second layer is the Member State Rulebook, which extends the EU Rulebook by incorporating aspects of national law. The third layer is the Technical Rulebook, where standard technical building blocks should be defined. Lastly, the fourth layer consists of the rulebook at the level of the data space initiative itself. This should consist of a comprehensive body of internal governance policies, which could be grouped into business, organisational and operational agreements.

In addition to the initiatives listed, there are further initiatives users that aim to **harmonise developments and advance technology**. These are not actively governed by users:

- **DSBA** comprising Big Data Value Association, IDSA, Gaia-X, and FIWARE, jointly created a convergence document to harmonise frameworks and outline the future architecture of data spaces.
- **Dutch Data Sharing Coalition and Dutch AI Coalition** have created manuals and reference guides for data spaces, building upon the work of IDSA and iSHARE. The Data Sharing Coalition Use Case Blueprint[74] supports the design of data sharing use cases and prepares them for scalability. These resources are currently not actively maintained.
- **DSSC** is a research-driven initiative tasked with specifying data spaces and promoting harmonisation supported by the EC. It is expected to produce final blueprints and technical specifications but will cease to exist after the project's completion. The DSSC is currently in the early stages of its activities. It builds on two approaches that have proven helpful in the design of data space governance: the use case blueprint for data sharing by the Data Sharing Coalition[78] and the templates for data space governance agreements derived from both Sitra's Rulebook for a Fair Data Economy and the IDSA Rulebook.
- **SITRA Fair Data Economy Rulebook**[79] is a useful toolkit for creating a decentralised soft infrastructure based on commonly agreed rules. It provides templates and a checklist for business, legal, technology, data and ethical aspects. The Fintraffic data sharing ecosystem has customised this rulebook to suit their specific context.

EMDS specific agreements

The specific governance framework of a data space and the policies therein rely on cooperative agreements among stakeholders. Clear cooperation agreements establish trust and build a solid foundation for governance. They should encompass functional, technical, operational and legal aspects. These agreements might be tailored to specific use cases or broadly applied across one or several sectors.

There are different categorisations for the types of agreements. The IDSA Rulebook[80] outlines functional, legal, operational, technical, and liaison agreements. The iSHARE Framework offers a

[77] aNewGovernance (n.d.), "aNewGovernance. Personal Data is a source of growth and innovation", https://www.anewgovernance.org.
[78] Data Sharing Coalition (2021), "Use Case Blueprint", https://datasharingcoalition.eu/our-approach-and-tools/use-case-blueprint.
[79] Sitra (2022), "Rulebook for a Fair Data Economy", Version 2.0, "Rulebook for a fair data economy", https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy.
[80] International Data Spaces Association (2023), "IDSA Rulebook", White Paper,https://docs.internationaldataspaces.org/ids-knowledgebase/v/idsa-rulebook/front-matter/readme.

universal set of data use terms, ensuring legal data sovereignty across data spaces, an approach also endorsed by the IDSA as an expansion of their recommendations.

The EMDS should consider implementing the following types of agreements:

- **Organisational agreements** that define the governance bodies and roles within a data space. They outline their authority for decision-making and the processes in which they should engage. These processes include membership management, technical evolution, participation in external bodies addressing interoperability, among others. For example, in the EMDS, assurance on specific data quality levels may be needed, e.g. for the arrival information of containers.
- **Functional agreements** that outline the operations of shared services, encompassing SLAs and procedures for monitoring, reporting, and maintenance. The EMDS is expected to gradually adopt these from various use cases. For instance, within the EMDS, certain use cases, such as smart traffic lights, may require higher API availability than the standard Estimated Time of Arrival (ETA), highlighting the phased integration of such arrangements.
- **Legal agreements** that define the legal environment, ensuring compliance with laws such as GDPR, and establish the appropriate framework to support the data economy, particularly concerning contracts formed within the data space. See also the next chapter covering legal aspects, which highlights the need for regulatory compliance assessments to form the basis for such legal agreements.
- **Operational agreements** that regulate policies and processes that must be enforced during data space operations, e.g. risk management, requirements management, and quality management according to a Plan-Do-Check-Act cycle.
- **Technical agreements** that address the adoption of common technology and its concrete implementation and maintenance with regard to trust, reliability, security and especially interoperability with other data spaces. This should align with the building blocks described in Part IV of this report.
- **Liaison agreements** that address the guiding principles, roles and processes for collaboration and alignment with other sectoral data space initiatives to achieve interoperability.
- **Business agreements** that specify terms and conditions regulating the data sharing between participants and establish sector-specific semantics and metadata definitions and standards, liaising with external stakeholders to achieve interoperability. Other functions of business agreements include pricing and payment, audit and compliance, or data quality and origin verification.

Current mobility and logistics data spaces have established terms and conditions. The EMDS can adopt ("inherit") some of these terms to create a unified framework for emerging mobility and logistics data spaces and enhance the broader European data space frameworks, once again, adopting a bi-directional approach.

Defining an EMDS operations model

Next to its governance framework, the **EMDS requires a data space operations model**. This model identifies the various service providers responsible for deploying and operating a data space. The prevailing operational model is the four-corner model, originally developed for the Pan-European Public Procurement Online (PEPPOL) network[81] to standardise and simplify international procurement across borders. It has been successfully deployed in the Smart Connected Supplier Network (SCSN)

[81] Holmlund, Per (2022), "Understanding the Peppol four-corner model of business exchange", Blog post, https://qvalia.com/blog/understanding-the-peppol-four-corner-model-of-business-exchange.

data space[82] for the smart industries sector. Given its success, the four-corner model is a viable consideration for the EMDS to oversee operations within the mobility data spaces federation. This model identifies three distinct types of service providers:

- **Infrastructure-as-a-Service providers** providing intermediary roles that jointly enable a data space, e.g. the intermediary roles as described in the reference architectures in Chapter 10. It is expected that the Infrastructure-as-a-Service providers will emerge to offer their services in a generic manner for multiple sectors, not only for mobility. This approach provides options for economies of scale and ensures interoperability for the federation of data spaces (see recommendations in Section 3.6).
- **Connecting service providers** that connect data providers and data consumers to the data space, for example through specific data apps on a generic data space connector. This is a rather generic IT service and not specific for mobility and logistics. Service providers may emerge that will provide their services in a generic manner for multiple sectors.
- **Value adding service providers** that provide value adding services in mobility and logistics, which may consider becoming part of a data space (see Section 9.5 in the chapter on data value creation).

4.4. Organisational and technical governance

The EMDS, anticipated by mobility and logistics stakeholders to include a stable, neutral, and trusted legal entity, can have a significant impact on operational data spaces in mobility and logistics (Chapter 3). Its governance framework should encompass both organisational and technical governance, as detailed in the following sections.

Organisational governance

Organisational governance entails establishing a multi-level governance framework, organising the EMDS governance authority, and adopting its appropriate legal form.

EMDS multi-level governance

The role of organisational governance for the EMDS involves coordination within the mobility sector to define and govern agreements, protocols, and standards. It also involves organising the mobility community and acting as the governing authority under cross-sectoral data space developments and EU initiatives, such as DSSC, SIMPL, EDIC, and EDIB.

These organisational dynamics require the EMDS to adopt a governance framework which allows it to operate at multiple levels, bridging the gap between mobility data spaces and horizontal frameworks such as IDSA, Gaia-X and others. This should be based on bi-directional exchange of specifications and requirements, as depicted in **Error! Reference source not found.**.

[82] Smart Connected Supplier Network (2023), “Four-corner model”, https://smart-connected-supplier-network.gitbook.io/processmanual/architecture/four-corner-model.

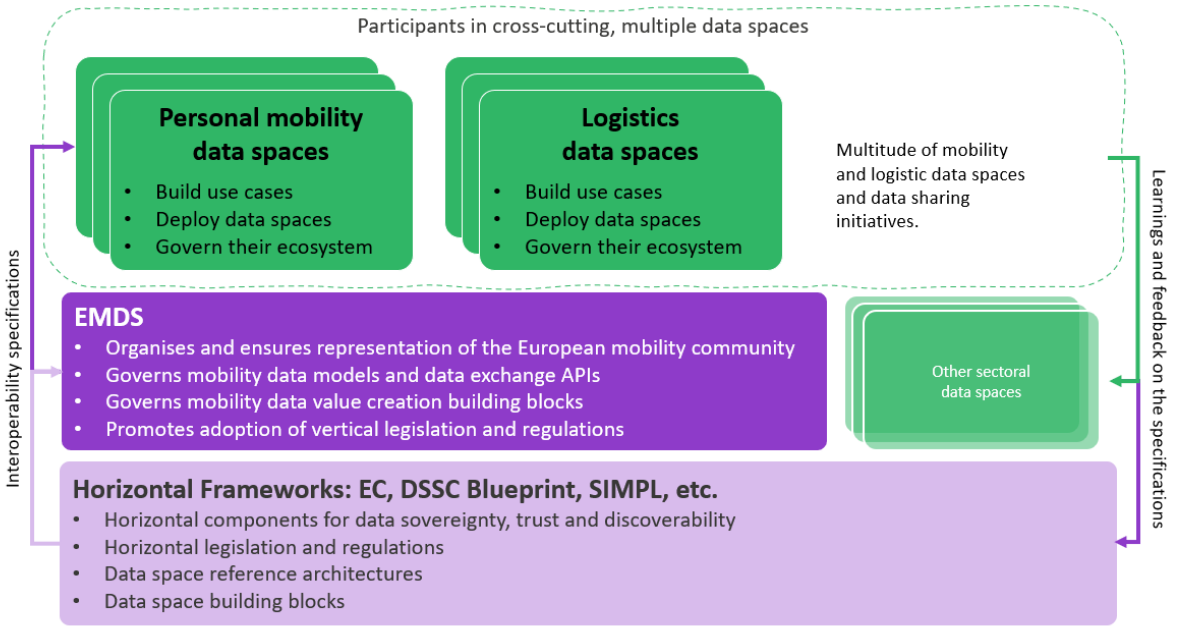


Figure 14: Levels in EMDS requiring multi-level governance.

The levels in the EMDS, as depicted in the figure, also reflect the need for both interoperability standards for developing individual mobility data space instances (i.e. **intra data space interoperability**) and for connectivity between multiple data space instances adhering to the horizontal frameworks (i.e. **inter data space interoperability**). Reference architectures and guidelines for both intra and inter data space interoperability are elaborated in Chapter 10.

Organising the EMDS multi-level governance framework

The fundamental considerations in Section 4.2 underline the need for the EMDS organisational governance to maintain a delicate balance between diverse interests, encourage collaboration, uphold ethical values and adapt to the evolving landscape of sovereign data spaces. This multifaceted approach is essential for achieving the goals of efficient data sharing, innovation, and societal benefit.

The proposed organisational structure for the EMDS governance framework has emerged from the project's consultation activities and analysis of good practices[83]. It is depicted in Figure 15.

[83] Examples include existing data spaces, as well as associations and initiatives such as the European Road Transport Research Advisory Council (ERTRAC), C-Roads and CCAM.

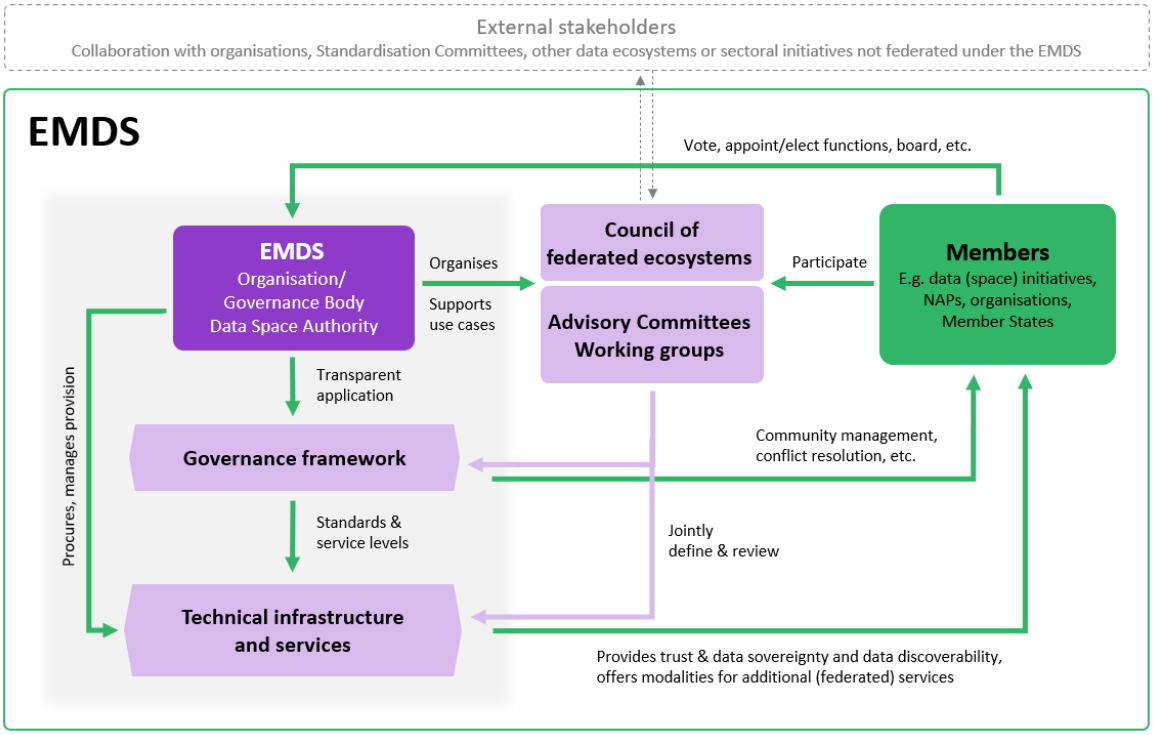


Figure 15: Proposed organisational structure for EMDS governance framework.

The main roles in the EMDS governance framework as depicted in the figure are:

- **Governance body/data space authority**
  The EMDS data space authority is responsible for the strategic oversight and management of the governance framework and operations. It should ensure that the governance framework is applied in the ecosystem. This framework includes the **vision, purpose and direction,** clearly defining the long-term goals and objectives for the EMDS. It provides **data sovereignty principles,** guidelines that ensure data ownership, control, and access rules, and **defines policies** that align with the vision and cater to the needs of the EMDS. The governance framework is discussed further below.
  The EMDS data space authority also manages the **provision or procurement of the technical infrastructure** required for data sovereignty and trust and data discoverability. This infrastructure is specifically intended to support the initiation of the EMDS and EMDS-based data spaces. The technical building blocks are described in Part IV of this report. Recommendations regarding the technical architecture are discussed in Chapter 10.
- **Council of federated ecosystems**
  Such a council could take strategic decisions regarding the governance framework and the technological building blocks used. The key principle to follow here is that this council ensures that real use cases from the data spaces based on the EMDS specifications co-govern these specifications and their further development. This ensures that EMDS specifications and frameworks are grounded in real applications and users. The council also appoints individuals to the advisory committees and working groups responsible for ensuring the interoperability and backwards and forwards compatibility of any changes applied to EMDS specifications and framework.
- **Advisory committees and working groups**
  Members may organise into advisory committees as well as use case-specific working groups that actively pursue and promote standardisation in the ecosystem. These committees and working groups may also allow for reciprocal exchanging and linking with external experts and representatives of organisations, horizontal frameworks, standardisation committees and

other sectoral European data spaces to ensure coordination. The relevant experts should include representatives from at least DTLF, RIS COMEX, NAPCORE, FENIX and FEDeRATED (along with their follow-up activities).
The key responsibility of the working groups is to further enhance the EMDS specifications, inherit new requirements from live and developing use-cases from existing (including national) data spaces, and make these learnings available through new specifications to all other EMDS member data spaces (Figure 14). For example, consider a scenario in which a new use case for urban logistics is initiated, and there is no API specification available for the delivery details of a logistics hub. In this case, an existing data space first develops that specification and contributes it to the EMDS working group. This contribution aids other data spaces aiming to build similar use cases by providing a new specification. The working group then assumes responsibility for governing the change procedure of the specification. It also ensures interoperability with other data spaces and maintains forward and backward compatibility, as well as versioning of the specification.

- **EMDS members**
  The EMDS membership may consist of various types of public and private entities such as active data spaces, federated ecosystems, NAPs, other organisations, as well as Member States. Members may vote decisions and appoint or elect members of the executive board (and possibly other bodies) of the EMDS governance authority.
  To assure a healthy balance, the voting structure of the members to take decisions should be clearly defined so that all members feel heard and jointly responsible for the functioning and effectiveness of the EMDS.

In addition, the EMDS governance authority could fulfil various functions and responsibilities. They are listed in Table 10, together with the priorities attributed to them. Priority 1 include the core functions and responsibilities that relate to the motivation for establishing and maintaining a data space, i.e. its "raison d'être". Priorities 2 include the functions and responsibilities for managing the continuous operations of the data space once it has been established.

Table 10: Functions and responsibilities of the EMDS governance authority.

Functions and responsibilities of the EMDS governance authority	Priority
Stakeholder engagement and communication Cater for the appropriate **communication channels** to regularly engage with stakeholders to understand their needs, address concerns, provide updates on changes, gather feedback and other relevant news, and disseminate information. In addition, enable **conflict resolution mechanisms** to address any disagreements or disputes among stakeholders.	**1**
Partnerships and alliances Identify and engage with potential **strategic partners** who could enhance capabilities or reach to **foster collaboration** among different stakeholders within the EMDS and across multiple data spaces.	**1**
Educational and outreach activities Promote **data space literacy and awareness**, for example, by organising workshops and webinars and providing resources to improve data space literacy among stakeholders. Furthermore, **advocate for data sharing** by highlighting the benefits of shared mobility data to encourage more entities to join.	**1**
Regulatory compliance and dispute resolution Ensure that the EMDS operates within the legal boundaries. To achieve this, **legal compliance** must be non-negotiable. Moreover, staying updated with European and Member State regulations (e.g. related to data protection and mobility and transportation regulations), requires ongoing **legal landscape monitoring**. The EMDS should **liaise with authorities** to act as the point	**1**

Functions and responsibilities of the EMDS governance authority	Priority
of contact between the EMDS and regulatory bodies. Finally, the EMDS should consider the potential benefits of establishing a **dispute resolution mechanism** to address potential conflicts between stakeholders. Although rules and regulations are adopted in accordance with procedures provided by law, a recommended element of the governance structure would function well as a neutral dispute resolution system allowing expert arbitration bodies to assist in resolving conflicts in an impartial, transparent, and timely manner. The existence of a dispute resolution mechanism would not prevent parties from exercising their right to seek redress before a national court.	
Continuous improvement: metrics, KPIs and monitoring Define and agree upon performance metrics of the infrastructural components of the EMDS, which may be expressed through Service Level Agreements (SLAs) on performance parameters regarding, for example, uptime and reliability, throughput, speed, and responsiveness. Additionally, define, monitor, and report the associated **Key Performance Indicators (KPIs)** to assess the reliability, effectiveness, and efficiency of the EMDS and form a basis for implementing improvements.	**2**
IT infrastructure management The EMDS is expected to **provide or procure (temporary) operational IT infrastructure** to the data spaces it federates. While in the long run, a more decentralised setup is preferred, with various actors providing interoperable infrastructure to their clients, a stronger operational role could be of importance for the EMDS, specifically at the beginning when support and testing infrastructure is needed to kickstart various initiatives. Moreover, also in the case that IT infrastructure capabilities are procured to external actors, a role for the EMDS remains in defining and monitoring the key IT infrastructure performance KPIs. To assure trust and reliability, the EMDS IT operation should be governed with strict procedures for information and infrastructure security (e.g. ISO27001). Next to its own operation, the EMDS can **make a set of procedures available to the data spaces that are building on the EMDS** specifications and framework. As a good starting point, various generic frameworks describing the multitude of business and IT management processes have been developed over the last few decades and are now well established. These include COBIT, ITIL, BISL and ISO 27000.	**2**
Audit and compliance Implement **monitoring tools** to continuously monitor and maintain logs of all activities within the data space, including both the data space services and building blocks. Such **audit trails** of data transactions at the metadata level (see Chapter 7 discussing “Data provenance and traceability”) ensure the transparency of all information unless it is classified by law (e.g. for privacy protection or ensuring the fairness of procurement procedures). To verify compliance, information on decisions, implementation of policies, and results should be made available to the public.	**2**
Data lifecycle management Define **data retention policies,** stating how long data can be stored and when it should be deleted, and implement versioning to manage changes, updates, or removals of data. The latter, of course, all under control of the data holder (data sovereignty as the cornerstone of the EMDS). While this is most relevant at the local level, the EMDS could support data spaces by providing legal support for stakeholders that have poor legal skills or resources.	**2**
Resource management Manage the EMDS’ budget and ensure it receives the sustainable financing and human resources required for the operation of the data space.	**2**

Legal form of the EMDS governance authority

With respect to a future legal form, potential participants stated during expert workshops and interviews that they would prefer the EMDS to become either a "**foundation**" or an "**association**" that is non-profit and neutral. However, most of the investigated data ecosystems and initiatives align more closely with the legal structure of a Private Limited Company, depending on the specific national law of the country where their legal headquarters are located. The creation of a Private Limited Company, however, does not contradict the desire for a non-profit orientation since several of these companies are dedicated to the non-profit principle and committed to it in their charter or statutes. Non-profit data initiatives include "Private Limited Companies" such as the MDS (DRM GmbH) and associations, such as the Global Data Service Organisation for Tyres and Automotive Components **AISBL.** AISBL is an international non-profit association under Belgian law (French: "Association internationale sans but lucratif"). Other interesting AISBLs in this domain include Gaia-X and ERTRAC[84]. Other companies hosting data exchange ecosystems, such as Fintraffic, are only allowed to generate minimal profit. Additional examples for existing "limited" associations or societies include the French "Association loi de 1901" (a type of club with legal status, for example EONA-X) and the "Société par actions simplifiée" (SAS, e.g. DAWEX, which is commercial). MinervaS is a "Società a responsabilità limitata", which is the Italian equivalent of a limited company.

The legal type of organisation (non-profit/private limited company) is of minor importance for the setup of a data space organisation, as business goals and value propositions, as well as the appropriate governance, can be realised in either type through dedicated statutes. However, the relative popularity of the variants of a "Private Limited Company" has pragmatic reasons. Limited companies are usually easier to set up and register with reduced formalities than a company on shares. They require less initial funding in many countries, and their internal organisation can be changed quickly. Further, they have fewer restrictions regarding tax declarations and public reporting, and the liability for the associates is limited. Furthermore, the familiarity with limited companies is also widespread, which making it a trusted and widely accepted model for potential partners.

Another argument that might influence the choice of the legal form of the EMDS is the desire for public bodies to engage in the management and operation of the EMDS. If there is a will on the public side (either national authorities or the EC) to play a long-term leading role or exert influence on the evolution of the EMDS, a legal form should be chosen that allows public entities to be associates or shareholders.

The EU has introduced certain legal entity formats with the scope, among others, to facilitate the formation of cross-border enterprises. One of these formats, the **European Economic Interest Grouping (EEIG)**[85], is a type of legal entity in European corporate law, created in 1985 under EC Council Regulation 2137/85. It emerged from the French "Groupement d´intérêt économique" and is designed to facilitate collaborations between businesses across diverse Member States or to aid in forming consortiums for EU projects.[86] It is primarily "designed to minimise the legal, fiscal and psychological difficulties that natural persons, companies, firms and other bodies face in cooperating across borders."[87] It can, therefore, constitute an interesting alternative to complicated cross-border mergers and joint ventures while allowing its members to maintain their independence. An EEIG's actions should complement its member entities' activities without replacing them, and its financial gains or losses are passed directly to its members. It bears full legal and financial responsibility and is subject to Valued Added Tax and workforce social contributions. However, it remains exempt from corporate tax obligations. An EEIG can be formed with capital or use other means of financing. Numerous EEIGs

[84] See https://www.ertrac.org/.
[85] See European Union (1985), "Council Regulation (EEC) No 2137/85 of 25 July 1985 on the European Economic Interest Grouping (EEIG)", Official Journal of the European Union, L 199, p. 1-5.
[86] See https://cordis.europa.eu/article/id/8994-advantages-of-eeigs-european-economic-interest-groupings.
[87] See https://eur-lex.europa.eu/EN/legal-content/summary/european-economic-interest-grouping.html.

operate within the EU, including the European Railway Train Management System Users Group in the rail sector, which collaborates on technical and operational matters in the deployment of European Rail Traffic Management Systems.[88]

The often-expressed wish that public funding might provide the basis of the EMDS, together with frequent concerns regarding the neutrality of private companies administrating the data space, suggests that an entity under public law might be appointed to coordinate and operate the EMDS. With the "DECISION (EU) 2022/2481 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 establishing the Digital Decade Policy Programme 2030", the EU has created the legal framework for an **EDIC**. This framework is designed to facilitate **Multi-Country Projects** within the EU. An EDIC is an international organisation, and as such, a legal entity subject to European law and to the national law of the Member State where the seat of the EDIC is located. The EU Member States that are members of an EDIC are expected to provide at least parts of the financial and in-kind contributions[89]. Its lifetime can be unlimited or limited. The internal organisation can be designed according to the members' joint decisions, and it can apply for EU funding, hire staff, purchase goods or engage contractors (e.g. for hosting an IT platform). An EDIC can ensure debt and the liability of the EDIC's members is by default limited to their respective contributions. In addition, it may pursue non-commercial or commercial activities. An EDIC can accept private members, but their ultimate impact on the evolution of the consortium is limited, since the statutes confer the majority of voting rights to the Member States represented in the EDIC[90]. Concerns have been raised about the potential delays in decision-making and operational inertia resulting from the primacy of Member States' voting rights.

Under these conditions, an **EDIC appears to be a suitable form for coordinating the integration of different data ecosystems into a federated structure**, with the potential to eventually absorb national structures as the European data economy transitions towards an environment that is closer to a single market. Playing such a role within the broader EMDS initiative would be conditional upon sufficiently representative membership within the EDIC (both Member States and organisations). However, since the administration and operation of a data sharing ecosystem (or a federation of data spaces), especially with numerous commercial players, is not a core responsibility of public administrations, an EDIC could serve as a transient stage for funding and controlling the creation of the EMDS until its EU wide integration has been achieved. Following that, full responsibility for the EMDS could be handed over to the entities that primarily benefit from it. This might take the form of a limited company, an AISBL, or an EEIG. However, this scenario strongly depends on the trajectory of the data economy in Europe. Another scenario envisions separate entities, where an EMDS governance authority manages the framework, while an EDIC supports multi-country projects and use cases that support the development of the cross-border data economy in mobility and logistics.

In sum, there are several potential legal forms for the future EMDS. In the current phase, one priority is the integration of several national initiatives into a unified, interoperable European structure. This integration necessitates a shared vision, public guidance, and funding, which could be encompassed in an EDIC. In the long term, once a satisfactory level of integration has been achieved, a legal entity

[88] See https://ertms.be/about-us.

[89] "In order to be a full member of the EDIC, the MS has to commit either financially or non-financially. If they make no commitment, they can only have an observer status. This is to be specified in the EDIC status. EDICs are about creating a European value. If Member States come with in-kind contributions, this is feasible, and can make sense for particular situations, e.g. providing infrastructure for the data spaces." EC (2023), "EDIC FAQ", unpublished communication.

[90] "The EDIC participation is open for the private sector, but not in terms of the voting rights. It is the Member States and their contributions, which are to be federated and brought together in the first place."; on the other hand, an EDIC faces restrictions, if it accepts private members: "It is indicated that an EDIC would normally meet the criteria of the above-mentioned directives to be recognised as an international body and as an international organisation unless its membership includes private entities." See EC (2023), "EDIC FAQ", unpublished communication.

under private law might permanently assume the administration of the community and the operation of the platform.

Possible organisational governance scenarios

The preceding sections have discussed different potential governance trajectories for the EMDS. In this context, the EMDS should be viewed as a broader ecosystem encompassing various actions and initiatives. While this report recommends a variety of roles to be fulfilled by the EMDS, there is uncertainty about the entities that will assume these roles within the EMDS. In discussions with the EC and Member States, several potential scenarios for the EMDS' trajectory were considered, ranging from a strong operational role (1) to a more limited one (5). These scenarios include possibilities of establishing:

1. An initiative or **organisation driven by the EC** with an operational data space authority resembling a fully public authority or an autonomous organisation like EIT Urban Mobility, with a mixed funding model. In such a model, data spaces and key stakeholders and initiatives could maintain supervisory or advisory functions.
2. A Member State driven **EDIC** serving as the foundational backbone of the EMDS. In an EDIC, Member States retain ultimate decision-making power and can establish strong KPIs for the operation of the digital infrastructure that enables data exchanges within the EMDS. Procuring the operation of digital infrastructure facilitated by joint investments at European level would eliminate the need for each Member State to build and operate its own data space. Support for cross-border use cases can speed up harmonisation efforts between Member States and contribute significantly to policy objectives for sustainable and efficient cross-border mobility and logistics. Concerns raised by stakeholders, in the context of this project, include potential delays in decision-making and the possibility of slow reactivity to customer or participant demands.
3. A **European association of data spaces in mobility and logistics** (e.g. AISBL), effectively governed by technical architects of Europe's existing mobility and logistics data spaces, or alternatively, fully **decentralised interlinkage of data spaces across Europe** governed by an agreement between data spaces. This scenario proposes a more decentralised vision, with a prominent role for existing data spaces in connecting their ecosystems and managing interoperability amongst each other while adhering to common European technical frameworks for data spaces. In this scenario, a decentralised data catalogue covering the data offer of all data spaces could be accessed from any of the participating data spaces. Temporary funding for cross data space use cases and harmonisation could speed up the processes to achieve full connection and interoperability.
4. A **governance, regulatory or certification framework** at European level. This scenario does not imply the creation of a legal entity for the EMDS but emphasises a stronger enforcement approach.
5. An **expert working group** responsible for defining and disseminating guidelines for interoperability between different mobility and logistics data ecosystems. This scenario does not imply the creation of a legal entity for the EMDS and relies on voluntary compliance with interoperability and governance frameworks.

The realisation of these scenarios is contingent on the perceived necessity of decision-makers to intervene strongly in support of use cases and the data economy as a whole. An assessment of these scenarios should be conducted in close consultation with key stakeholders and existing data spaces in mobility and logistics. In evaluating these scenarios on the role for the EMDS both the long-term sustainability of EMDS operations model and adequate representativeness of the EMDS (both in terms of represented thematic categories and domains and in terms of represented countries) are key criteria.

Technical and functional governance

A main responsibility of EMDS governance is to enable technical and functional interoperability within the personal mobility and logistics sectors, but also across cross-sectoral adjacent data spaces.

Technical and functional interoperability can be categorised into three levels.

- **Data sovereignty and trust**: the foundation of interoperability
  Through **unified trust frameworks,** standardised validation can be provided for participants. This ensures that only verified entities can participate in data exchanges, eliminating the uncertainty associated with unverified data exchanges and strengthening confidence among participants. Trust frameworks must incorporate legal parameters to ensure that data usage policies are not merely guidelines but enforceable protocols. This legal binding fortifies the trust infrastructure, ensuring that participants adhere to agreed-upon terms. The EMDS should govern legal aspects for interoperability such as usage terms of data, liability on data misuse, and more. The combination of **legal and technical enforceability** is a key aspect of EMDS governance.
  The fundamental technical capabilities for data sovereignty and trust should be regulated at the European level ensuring that data entitled parties have full autonomy and control over their data across all sectoral data spaces. Moreover, central trust frameworks for all sectoral data spaces at European level are important for interoperability and can significantly lower costs. Technical building blocks for data sovereignty and trust are further elaborated on in Chapter 8.
- **Discoverability and metadata brokering**: the compass of the data realm
  This encompasses two crucial aspects. The first is the support for **self-descriptions** that form the basis for the data spaces' **data services catalogue**, guiding participants to the right data services and APIs. Standardised access requests enable seamless interactions, even in a vast ecosystem like the EMDS, thereby streamlining data sharing processes. **Metadata brokering** enables the translation of data models. Hence, metadata brokers play a vital role in translating and facilitating interactions between data space participants. They enable the adaptation of data requests and responses, ensuring smooth communication regardless of underlying differences in data models, structures or standards.
  The second key aspect is facilitating **participant discovery** through standardised APIs connecting to participant registries in the trust framework. This approach harmonizes the process of discovering the data services provided by participants at service providers, along with the location of the participant's policy registry or registries.
  The basic capabilities for discoverability and metadata brokering should be governed at the European level, aiming for a harmonised structure for the discovery of both data services and participants across all sectoral data spaces. Discoverability and metadata brokering are further elaborated in Chapter 9.
- **Data interoperability**: Making data understandable across the EMDS
  Agreed-upon data models and data exchange API are required for actual data services and use cases. They are the basis for data sovereignty and trust specifications, as well as for discovery and metadata brokering specifications. Data interoperability is governed through joint repositories that enable participating data spaces to conform to common data standards and protocols.
  These mobility specific data models, which serve as the basis for mobility use cases and data services, should be governed by individual mobility data space instances under the guidance of the overarching EMDS. Data interoperability is further elaborated in Chapter 7.

The following sections elaborate on the governance mechanisms for all three key aspects: data sovereignty and trust, discoverability and metadata brokering and data interoperability.

Governing data sovereignty and trust

Data sovereignty and trust necessitate key decisions as it is crucial for all participants to adopt an agreed-upon and aligned approach. Trust in data sharing can only be established with a harmonised framework on data sharing authorisation policies that preserve the autonomy and sovereignty of data entitled parties and data spaces, particularly regarding access and usage control. A **harmonised trust framework, governed by the overarching EMDS,** can safeguard the autonomy and sovereignty of participants both within individual mobility data space instances and across the federation of sectoral data spaces. In fact, this is the core rationale for the existence of data spaces[91]: **Autonomy and sovereignty of the data entitled parties** unlock the potential for smarter data utilisation across value chains and verticals and unlock the potential of data sharing and the data space.

Autonomy and sovereignty are achieved through a harmonised set of principles across the EMDS and the individual mobility data space instances:

- The **data entitled party has autonomy** (sovereignty) in controlling who can access their data (access control) and what can be done with that data (usage control).
- This associated governance structure has a dual nature. Firstly, **legal agreements** are a basic requirement to guarantee that, in cases where someone uses data in a manner that differs from the usage policy or usage license defined, they are legally liable for the consequences of that action. Secondly, where feasible, **technical enforcement** can further enhance trust in the data sharing processes and data space infrastructure. For instance, by using a data space connector, every data transaction can be validated against the policy registry of the data entitled party, thereby preserving sovereignty and autonomy in every step of the data sharing process. It is important to note that data spaces also have autonomy. They have the freedom to take decisions that deviate from the overarching EMDS approach and standards if necessary to achieve the specific goals of the mobility data space.

Therefore, these principles must be regulated in a harmonised manner as part of the governance framework of the EMDS to enable data spaces to build on these principles and standards. The adoption of a harmonised trust framework for data sharing is the key starting point, potentially achieved by leveraging the strengths of the various horizontal trust frameworks such as developed by Gaia-X, IDSA and iSHARE. Table 11 lists the key items for a trustworthy and legally compliant trust framework for data-sharing within the EMDS.

Table 11: Key items for governing data sovereignty and trust.

No.	Key items for governing data sovereignty and trust
1	**Define trust and legal principles** Clearly articulate the fundamental principles that guide trust and legal compliance, emphasising transparency, security, data sovereignty and user rights. Define a set of core API specifications to validate the authorisation rights of a data entitled party in a harmonised process.
2	**Realise infrastructure trust with the Gaia-X framework** Ensure infrastructure sovereignty, e.g. by adopting Gaia-X's labelling structure for (cloud) infrastructures. This serves as a quick reference for participants to understand the trustworthiness and capabilities of different infrastructure components. Periodically certify and audit infrastructure components to ensure they uphold the standards set by the labels.
3	**Ensure trustworthy data space connectors through IDSA's certification process** For instance, IDSA's approach to certifying connectors can be implemented, ensuring they are compliant with the core principles of the EMDS. The compliance of data space connectors should be monitored

[91] iSHARE Foundation (2023), "Cookbook for Data Spaces", https://ishare.eu/inspiration/cookbook-for-data-spaces.

No.	Key items for governing data sovereignty and trust
	and regularly verified, and they should work with the data governance and trust principles as described above. This also means that SMEs without connector infrastructure should be sovereign on their data shared through third party connectors.
4	**Ensure legal interoperability with the iSHARE agreement framework** Use a unified approach to establish a foundational legal and licenses framework that all participants adhere to, creating legal interoperability across data spaces. Consider using iSHARE's trust framework for this purpose.
5	**Establish a trust and legal committee** Establish a central body responsible for overarching trust and legal principles, strategies and monitoring.
6	**Provide a process for conflict resolution and mediation** Establish a clear process for resolving disputes related to trust and legal issues. This ensures that conflicts are addressed promptly, maintaining the integrity and trustworthiness of the EMDS and the individual mobility data space instances.
7	**Create transparency and support reporting** Periodically release reports detailing the trust and legal compliance statuses of participants, infrastructure and data space connectors. This transparency reinforces trust among participants. Create mechanisms for participants to report any breaches of trust or legal compliance, ensuring quick responses and solutions.
8	**Organise training and capacity building** Organise sessions where participants can understand the legal framework, their rights and obligations. Host workshops or webinars detailing best practices for maintaining data trustworthiness and the principles of the EMDS.
9	**Engage with external legal bodies** Engage with international and regional legal bodies and experts to ensure that the EMDS trust and legal framework remains up to date with evolving laws, especially related to data protection, mobility and technology.
10	**Do iterative reviews and updates** Just as with data standards and interoperability, the trust and legal committees should periodically review the framework, considering new legal precedents, technological advancements, feedback from participants and evolving societal needs.

Governing discoverability and metadata brokering

To maximise the value participants derive from the data, a key aspect is discoverability. Therefore, this aspect is an integral part of the governance framework for the future EMDS. The facilities and the choices of standards should be designed to allow parties to work together across the federation of data spaces by discovering and accessing data assets.

There are two key approaches for the value creation aspect that need to be decided upon and harmonised across the different data spaces that will build on the EMDS:

- **Semi-public data sets** are shared against conditions (e.g. "if you pay x, then you can access this data"). This falls under the data sharing type "Sharing of persistent (static or semi-static) data" described in Section 2.2. In this context, a **federation of catalogues** in combination with **marketplace capabilities** creates value by allowing discovery and access to the data and services that are provided by stakeholders participating in the data space and stakeholders participating in other data spaces that are part of the federation of interoperable data spaces. Federated catalogues and marketplace building blocks are discussed in Chapter 9 focusing on technical building blocks for data value creation.

For EMDS governance, harmonisation of catalogue and marketplace capabilities is important. Roles and responsibilities should be defined to facilitate the discovery of EMDS-relevant data for different subgroups and specific use cases. This will allow the data spaces in the EMDS to initiate new use cases easily and effectively by providing access and visibility to all the relevant metadata.
The marketplaces serve as the contract management building block, responsible for registering the contracts (including the agreed-upon policy) for individual data sharing transactions. These contracts are synchronised with the policy registry of the data entitled party. The data entitled party retains full control of their data in a harmonised way. For example, if party A paid for this data service with these conditions, they are entitled to access that data over the agreed-upon time period.

- **Classified data sets/services** are only accessible on explicit consent by the data entitled party (e.g. “these attributes from this event may only be shared with this organisation under the condition that another event happened, for this period”). This may apply to data sharing types involving "Sharing of (real-time) streaming data" and "Event-driven smart contracting for data flow control" as described in Section 2.2. These policies are generated by the data entitled party and registered in the policy registry of the data entitled party. This can be achieved through manual intervention or through authorised software applications that create those policies on behalf of the data entitled party.

The discovery of these data sets and services usually begins with the **participant registries** in the data space’s trust framework, where the participants register their capabilities. They form the link to the available services of that participant within the specific data space. in addition to the participant-based discovery, data discovery can also be achieved by means of linked data concept. For instance, a transaction might include the link (pointer) to allow a follow-up data service to be invoked. This may be relevant for instance in cases of event flow for handling containers throughout their overarching transport itineraries and associated chain of stakeholders.

The final and crucial aspects of discovery required for both classifications of data sharing is a harmonised way of:

- Finding trusted participants in a federated manner across data spaces, which are part of the trust framework across data spaces;
- Locating the “Access and usage control policies” of a data entitled party in the data space, along with pointers to their policy registry for request access to a specific data service.

As a part of the EMDS, the governance of the structure of this discovery, and the harmonisation of the APIs are a key aspect to the interoperability on trust and value creation across the EMDS, as elaborated in Chapter 8 and Chapter 9, respectively. Various Dutch data spaces in logistics (like the Dutch Basic Data Infrastructure, DVU and DMI) are currently harmonising these aspects under a common trust framework. Their approach could be assessed on applicability for the EMDS as well.

Governing data interoperability

Both the use of data standards and the interoperability between the different domains are crucial. Nevertheless, governance of these prerogatives is complex, especially when balancing autonomy and interoperability. Therefore, a **governance process for data interoperability** is proposed, customised for the EMDS. By implementing such a governance process, the EMDS can maintain a cohesive set of core data standards while allowing individual mobility data space instances the flexibility to innovate and cater to specific needs, ensuring both interoperability and adaptability. Table 12 provides an overview of the associated governance procedures for data exchange interoperability.

Table 12: Governance procedures for data interoperability.

No.	Governance procedures for data interoperability
1	**Establish the EMDS base specification** Define and manage a set of open source foundational data standards, formats, and protocols that every participant in the EMDS can adhere to when aiming for interoperability with other EMDS data spaces. This approach could follow the examples of SmartDataModels.org or the BDInetwork.org repositories. Moreover, agreed-upon interoperability protocols can set a baseline for ensuring that data can move seamlessly throughout the broader EMDS and its federation of mobility data spaces.
2	**Data space autonomy with customisations** Individual mobility data space instances can define additional standards or nuances catering to their specific needs and to realise their use-cases. However, these should be considered as extensions of the core EMDS standards and not conflict with them. Any proposed changes or additions by the individual mobility data space instances should be **communicated** to the central EMDS standards committees. This ensures that innovations can be evaluated for potential integration into the broader EMDS standards.
3	**Versioning and evolution** Implement a versioning system for the EMDS standards. When the EMDS or individual mobility data space instances introduce significant changes, they should be reflected as a new version. Thereby, participants can identify the version of the standards they're adhering to and track changes over time. This process is governed by the EMDS working groups.
4	**Interoperability testing and validation** Establish c**entral testing** environments where individual mobility data space instances can test their implementations against the core EMDS standards to ensure interoperability. Encourage and enable individual mobility data space instances to develop similar testing environments for their specific standards.
5	**Documentation and knowledge sharing** Maintain a central repository documenting core EMDS standards updates. This repository should also reference or link to standards set by individual mobility data space instances. Establish platforms or forums for individual mobility data space instances to share their experiences, challenges, and best practices regarding data standards and interoperability. This fosters collaborative learning and innovation.
6	**Dispute resolution and mediation** In case of disagreements between individual mobility data space instances, the central EMDS, or among individual mobility data space instances themselves regarding standards, a clear mediation process should be in place. This ensures that conflicts are resolved while upholding the integrity of the EMDS. This falls under the responsibility of the Council of Federated Ecosystems and its Working groups.
7	**Periodic review and updates** The central EMDS standards committee should periodically review the base specification, considering feedback from individual mobility data space instances, technological advancements, and changing mobility sector needs.
8	**Education and training** Organise workshops, webinars and training sessions to educate participants across and within the EMDS, or within the individual mobility data space instances, on the standards and their importance. This can also be a platform for introducing new standards or updates.
9	**Engagement with external standards bodies** The mobility sector is not isolated. The EMDS governance framework should facilitate engagement with other standard-setting bodies relevant to data and technology to ensure alignment with broader cross-sectoral and technological trends.

4.5. Recommendations

Conclusions

Data space governance lies at the core of the mobility data space initiatives and the EMDS. It serves as the cornerstone for overseeing data spaces comprehensively while also ensuring compliance with legislation, ethical standards, and interoperability between data spaces. This encompasses data services, models, IT resources, data sovereignty, trust, and discoverability.

The EMDS operates within a complex environment, and as such, it demands a corresponding governance framework. This chapter has addressed these intricacies and provided several recommendations and insights pertaining to what is commonly referred to as 'multi-level governance' for the EMDS.

Recommendations

Align with the EC data space strategy through the DSSC and the EDIB

Various frameworks are available for defining organisational governance and management processes. As these are often generic, the EMDS should take the lead in making key decisions and providing guidance ensuring its members align with processes developed generically across data spaces. This alignment encompasses frameworks provided by horizontal frameworks, the DSSC blueprint, and the EDIB (Section 1.3). The EMDS should refrain from developing its own processes. The horizontal frameworks and the DSSC will provide a comprehensive perspective, making it easier for the EMDS to select the appropriate sets of guidelines. This approach, aligned with the harmonised strategy presented in the DSSC blueprint, aims to integrate the strengths and insights from various EU reference architectures and frameworks related to federated data sharing and data spaces (e.g. IDSA, iSHARE, Gaia-X). The goal is to offer a robust, inclusive, and evolving governance framework for the EMDS.

Adopt a multi-level governance system for the EMDS

The envisioned structure of the EMDS consists of numerous autonomous data space instances interconnected through federation. A multitude of mobility and logistics data spaces will emerge, each driven by various use cases, specific applications, and different regulations, all converging towards a common goal: federation, interoperability, and alignment. These federated data spaces and platforms, as well as an overarching (European) EMDS authority, will govern this, possibly adhering to a geographic or thematic logic. Given the autonomy of the individual data spaces in selecting which specifications to adopt, it is crucial to ensure that they remain aligned with the overarching goals. As a general principle, the EMDS may endorse the principle of subsidiarity, allowing decision-making at the most immediate level, i.e. individual mobility data spaces. The role of the EMDS would be to facilitate a synergistic approach to the federation of the mobility data spaces, accommodating a balanced representation of all stakeholders including transport providers, mobility infrastructure managers, passengers, logistics entities, and more. In its decision-making, however, the EMDS should consider the investments made by existing data space initiatives, ensuring recognition and integration where feasible. A multi-level governance system needs to be adopted.

Focus on data sovereignty, trust and discoverability as key capabilities to be governed across a federation of data spaces on both legal, organisational and technical aspects

Interoperability and federation of data spaces extend the reach and scope of accessible data and allow new business and funding models and services to be developed across sectors and regions. Data sources in mobility and adjacent data space instances should be mutually accessible. Therefore, data space interoperability and federation of data spaces are key aspects for realising the EU´s ambition of the common European data spaces. The key capabilities to make data sources available in the federation of data spaces are data sovereignty, trust, and discoverability (through metadata

brokering). They play an important role in the governance of the federation of data spaces. It is worth noting that this encompasses legal, organisational and technical aspects to be governed as part of the EMDS multi-level governance framework.

Address the complexities in mobility and logistics data sharing collaboration in the EMDS multi-level governance framework

The collaboration conditions for data sharing in mobility and logistics are challenging. These conditions need to be considered in the in the EMDS multi-level governance framework. They include balancing public and private interests, addressing power asymmetries and data monopolies, incentivising cooperation in mobility and logistics, reconciling societal values and financial viability, and managing an ecosystem of sovereign data spaces. The governance framework, decision-making, community management and use case support should address adequate representation of diverse stakeholder types.

Foster collaboration on federation and harmonisation across sectors through a joint council of participating data spaces

Mobility and logistics are intrinsically cross-sectoral. This suggests that the interface and connectivity between data spaces are vital not only between mobility and logistics data spaces but also between proximate sectoral data spaces in smart industry, cities, tourism, etc. A joint council of participating data spaces would foster collaboration on federation and harmonisation across various data spaces such as energy, transport, tourism and agriculture. A common knowledge management base offered as open source would ensure widespread access and collaboration and should be made freely available to participants through the council. Alignment with the DSSC and the community-governed frameworks would guarantee its adherence to the overarching EU approach.

Build upon existing best practice governance frameworks

Several decentralised and multi-level governance approaches have already been adopted for federated data sharing ecosystems. These approaches should be assessed for their suitability in the context of multi-level governance for the EMDS. Examples such as PEPPOL, BDI and Catena-X may provide valuable insights for a decentralised governance approach, with each Member State contributing to its implementation. Best practices from these initiatives should be evaluated for their applicability to the EMDS governance framework.

4.6. Building blocks

Figure 16 shows the individual building blocks recommended for governance.

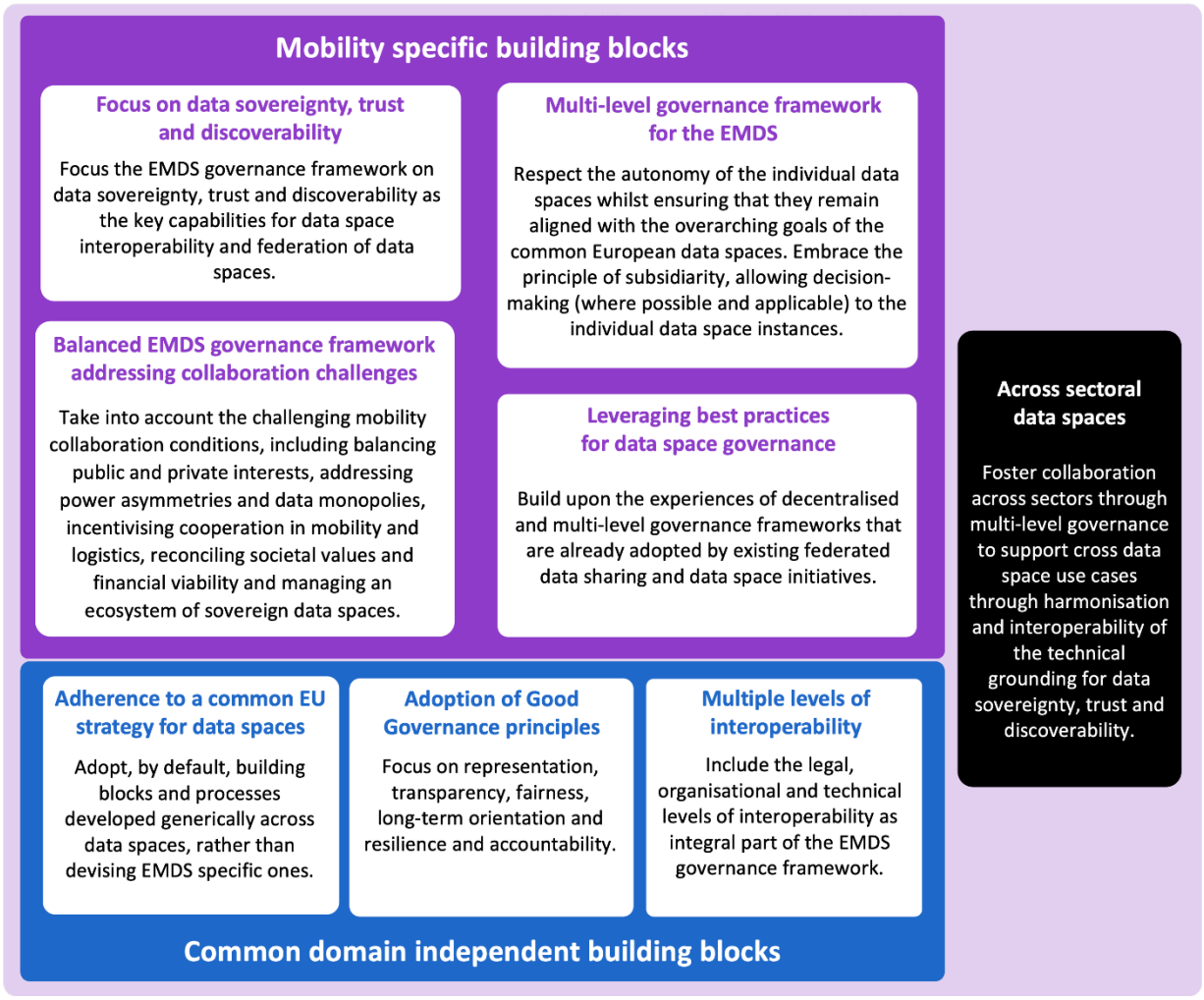


Figure 16: Building blocks for governance.

5. Legal aspects

5.1. Introduction

Legal considerations are central to the organisation and governance of data spaces, with the DSSC recognising regulatory compliance and contractual frameworks as essential legal building blocks.[92] This chapter focuses on exploring the legal perspective of the EMDS, outlining key frameworks related to data spaces and mobility data. The analysis recognises the importance of horizontal EU legislation on data, as well as the necessity of considering sector-specific legislation to tailor data governance to the objectives and constraints of mobility. The purpose of this chapter is to provide recommendations to inform the governance framework and support the smooth functioning of the EMDS.

The following Section 5.2 explains the horizontal EU legislation, encompassing legislative instruments applicable across different sectors and sectoral data spaces. Mobility specific legislation is addressed in the subsequent Section 5.3. Finally, Section 5.4 presents the conclusion, lists the recommendations, and provides the building blocks of the legal aspects for the EMDS.

5.2. Horizontal EU legislation

The European Data Strategy acknowledges that data has become a valuable asset in the digital economy and aims to ensure that Europe maximises the benefits of data-driven innovation while protecting citizens' rights and societal values.[93] It sets out a framework for fostering the European data economy by establishing common European data spaces, promoting data sharing, and strengthening data governance aligned with EU values. In addition to funding the development of sectoral data spaces in strategic areas, this action also includes the adoption of several cross-sectoral legislative instruments.

Innovative cross-cutting legislation such as the **DGA** and the **DA proposal** has been introduced with a specific focus on supporting the European data economy and creating a new legal framework for data. These instruments aim to address some of the barriers identified in the Data Strategy, such as the lack of trust, and provide minimum governance rules to facilitate data space interoperability across sectors. It is important to note that the European Parliament and the Council of the EU reached a political agreement on the DA on June 28, 2023. [94] The final text is pending official approval by the co-legislators, thus any references to the DA in this report pertain to the proposal.

Figure 17 provides an overview of all the main legislative instruments introduced by the Commission to strengthen or complement the data economy:

[92] DSSC (2023), "Building Block Taxonomy", forthcoming.
[93] European Commission (2020), "A European strategy for data", 27 February 2020, https://data.europa.eu/en/news-events/news/european-strategy-data, p. 12 and 16.
[94] European Commission (2023), "Data Act: The European Commission has reached a political agreement on the European Data Act", 29 June 2023, https://data.europa.eu/en/news-events/news/data-act-european-commission-has-reached-political-agreement-european-data-act.

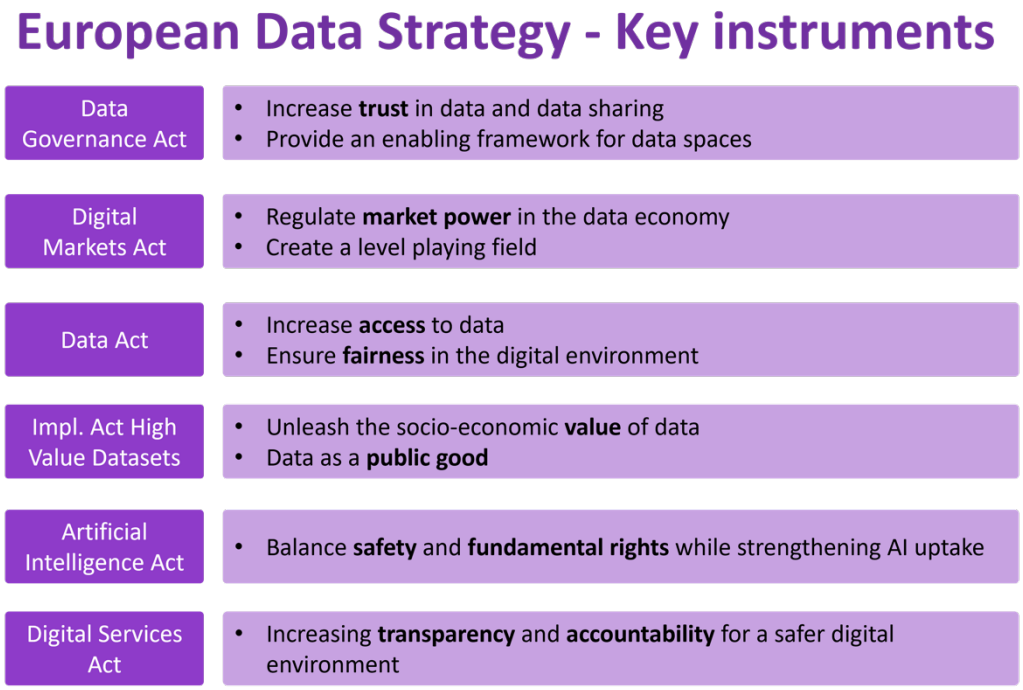


Figure 17: Overview of key legal instruments; source: adapted from European Commission.

Data spaces are novel data infrastructure promoted by the EC to "overcome legal and technical barriers to data sharing" and to comply with EU rules and values.[95] As such, data spaces currently exist as developing data infrastructures with ill-defined and expanding boundaries.[96] Data spaces are expected to intersect with numerous legal frameworks in addition to those specifically designed to support the European data economy. There are currently legacy legal frameworks such as **personal data protection** and **intellectual property rights** which require careful consideration for the operation of data spaces.[97] In such legislation, data is not the direct subject matter; instead, these legal regimes protect broader interests that indirectly encompass data.[98]

Within the mobility sector, data sharing is contingent upon diverse data sources that encompass a wide range of categories, such as traffic data, passenger data, geolocation data, and machine-generated data. Each of these categories of data may be subject to different legal frameworks governing their collection, storage, and use. The legal implications of these data categories require careful consideration and adherence to applicable regulations to ensure compliance and protection of privacy, intellectual property rights and other relevant legal considerations.

The DSSC is developing a comprehensive mapping of the relevant legal frameworks for data spaces (Figure 18).[99] The mapping illustrates the range of legal frameworks that may be relevant to data

[95] European Commission (2022), "Commission Staff Working Document on Common European Data Spaces", SWD 45 final, p. 2.
[96] A proposed definition has been offered by the Data Spaces Support Centre, see Data Spaces Support Centre(2023), "DSSC Glossary", https://dssc.eu/wp-content/uploads/2023/03/DSSC-Data-Spaces-Glossary-v1.0.pdf.
[97] Margoni, T., Ducuing, C., Schirru, L. (2022), "Data Property, Data Governance and Common European Data Spaces", Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht, http://dx.doi.org/10.2139/ssrn.4428364.
[98] Franceschi, A., Lehmann, M. (2022), "Data as Tradeable Commodity and New Measures for their Protection", The Italian Law Journal, https://iris.unife.it/bitstream/11392/2339106/2/592-data-as-tradeable-commodity-and-new-measures-for-their-protection.pdf.
[99] Data Spaces Support Centre (2023), "Legal Aspects of Data Spaces, Regulatory Compliance Building Block – Public Consultation", September 2023, https://2023.mydata.org/session/workshop-by-the-data-spaces-support-centre-2.

spaces, and notes that sectoral legislation may also apply. Based on this mapping, several key challenges for the EMDS emerge, including:

- Navigating the patchwork of substantive rights and obligations pertinent to data;
- Keeping up with the **evolving EU legal landscape** on data;
- The resulting issue of **legal interoperability**.[100]

Although it is not possible to provide a complete legal analysis given the early stage of the EMDS, this section is based on the mapping and, where possible, provides specific examples of its relevance to the EMDS. For more information on EU legislation in the digital sector, refer to the data set compiled by Bruegel.[101]

Data-related legislation

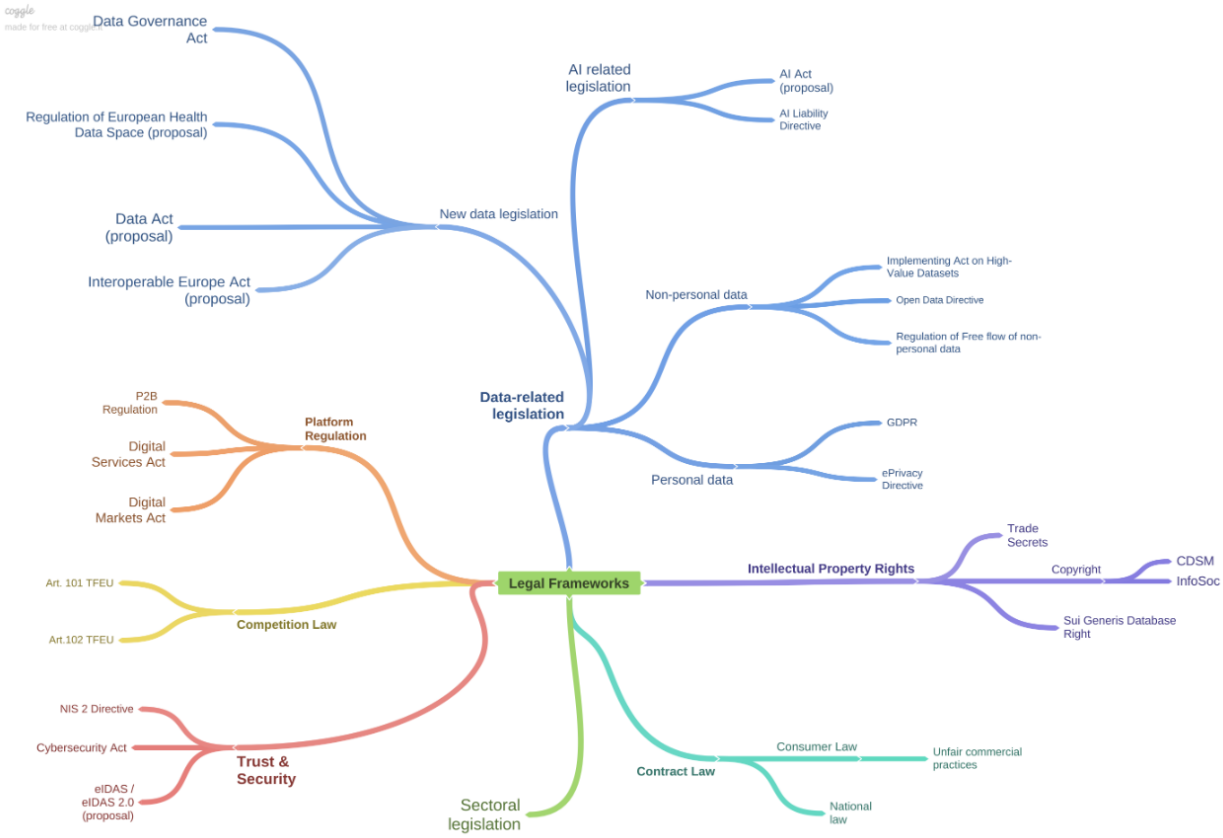


Figure 18: Legal Mapping – legal framework applicable to data spaces.

Data law[102] plays a fundamental role in the data governance framework for data spaces. The EU has been proactive in establishing a robust framework to safeguard personal data and regulate data flows. Data-related legislation is an evolving area of law and encompasses several sub-categories, namely personal data, non-personal data, artificial intelligence and sector-specific regulation establishing governance rules for common European data spaces (e.g. **proposed European Health Data Space**

[100] Data Spaces Support Centre (2023), "Starter Kit for Data Spaces Designers", Version 1.0, https://dssc.eu/wp-content/uploads/2023/03/DSSC-Starterkit-Version-1.0.pdf.
[101] See Bruegel (2023), "Overview of EU Legislation in the Digital Sector", Table 1, https://www.bruegel.org/sites/default/files/2023-07/Tables_Scott_Kai.pdf.
[102] On further information on the emergence of an EU data law see Streinz, T. (2021), "The Evolution of European Data Law (chapter 29)", The Evolution of EU Law, 3rd Ed., Craig, P., and Búrca, G. de (eds), Oxford University Press.

Regulation). It also includes the EU's new regulatory interventions to support the European data economy, namely the **DGA** and the **proposed DA**. The cluster will continue to evolve as some pieces of legislation are still proceeding through the legislative process, while others are already in the process of implementation. This highlights the need for a comprehensive, adaptable approach to data governance within the EMDS, capable of accommodating the various legal requirements and considerations associated with different data categories. By addressing the legal implications of diverse data categories, the EMDS can ensure effective and compliant data exchange and utilisation within the mobility sector. The impact of some of these pieces of legislation to the EMDS is presented below.

Compliance with the **GDPR** is essential for guaranteeing trust within the EMDS. Mobility data could qualify as personal data necessitating the application of the rules and principles established by the GDPR. Transportation, for example, is a fundamental aspect of modern society and mandatory for most individuals. Daily journeys are being increasingly tracked by various sensors, and patterns created from past individual and group behaviours.

Data, especially geolocation data, can reveal details about personal routines, workplaces, family residence, political affiliation, and more. If not immediately identified, individuals can become identifiable through journey data, as these are often unique and consistent over time. The European Data Protection Board draws specific focus to geolocation data as a category that warrants special attention as it can be particularly revealing of one's lifestyle and habits.[103] Other types of data may also potentially qualify as personal data such as real-time traffic data, vehicle data, and public transport data.[104]

Therefore, it is crucial for vehicle and equipment manufacturers to exercise caution and refrain from collecting location data unless necessary for specific processing purposes. Collecting "offence-related data" such as combining real-time vehicle speed with precise geolocation data or data indicating a violation of traffic rules, like crossing a white line[105], is also problematic as it can affect different individual's rights and freedoms.

One interesting illustration of the potential dangers is the case of the London bike-sharing initiative. In this project, the city authorities released a data set containing information about users' bike trips. The data set included unique customer identifiers along with the starting and ending locations and timestamps for each journey. These data made it possible to trace the travel patterns of cyclists throughout London. By analysing the most common routes and the dates and times of journeys, individuals' residential and workplace locations could be defined, thereby compromising their anonymity.[106] Studies have shown that as few as four data points including for example time and location, can lead to the identification of 95% of individuals in a data set.[107]

The EMDS should therefore understand the legal implications under the GDPR of collecting and processing mobility data. Therefore, it should pay significant attention to how personal data will be governed and how technical and organisational mechanisms are implemented to ensure compliance with GDPR. More specifically, it should give particular focus to defining data controllership; implementing the principles of purpose limitation and data minimisation, especially when data flows

[103] Ibid, p. 60-61.
[104] See MobiDataLab project (2021), "D2.3 "State of the art on Mobility and Transport data protection technologies", https://cordis.europa.eu/project/id/101006879/results.
[105] European Data Protection Board (2020), "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", Version 1.0, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, p. 3, 27-28.
[106] MobiDataLab (2023), "D2.1 Legal and Regulatory Data Sharing Gap Analysis", https://mobidatalab.eu/wp-content/uploads/2023/01/MobiDataLab-D2.1-LegalRegulatoryDataSharingGapAnalysis-v1.1.pdf.
[107] Open Data Institute (2018), "Personal data in transport: exploring a framework for the future", https://theodi.org/wp-content/uploads/2018/06/OPEN-Personal-data-in-transport-.pdf.

through different contexts; using the appropriate legal basis, particularly managing consent; and implementing these aspects by design and by default. In relation to privacy by design mechanisms, one of the main strategies to protect people's data is to anonymise or pseudonymise data using random identifiers. Re-identification methods are often not straightforward, however, though numerous approaches can be effectively exploited to do so, particularly with advancements in computer processing capabilities and the growing availability of additional data sources.[108]

Another important legislation within this cluster for the EMDS is the **DGA**. The DGA was the first of a set of measures announced in the 2020 European strategy for data. It is grounded in the belief that more economic operators and organisations promoting societal interests should have the capability to harness the potential value of data in both the economic and societal domains. The DGA is therefore necessary to improve the conditions under which data is shared within the internal market. It aims to help create a harmonised framework for data exchanges and lay down certain basic requirements for data governance. More specifically, the DGA (Article 1 (1), DGA) sets forth:

> "(a) Conditions for the re-use, within the Union, of certain categories of data held by public sector bodies;
>
> (b) a notification and supervisory framework for the provision of data intermediation services;
>
> (c) a framework for voluntary registration of entities which collect, and process data made available for altruistic purposes;
>
> (d) a framework for the establishment of a European Data Innovation Board."

Due to their importance for the future EMDS, the first two points are briefly described below.

The first aim is closely related to the limits of the **Open Data Directive**. Its main goal was to promote the use of open data and stimulate innovation in products and services through practical arrangements for facilitating the re-use of existing data held by public sector bodies of the Member States and public undertakings under certain conditions (Article 1, 1, Open Data Directive).

The Open Data Directive recognises the value of open data for society and identifies mobility as one of the thematic categories of **high-value data sets** that should be prioritised (Annex 1). These data sets must be available free of charge, machine readable, provided via APIs, and provided as a bulk download, where relevant (Article 14(1)). According to its Recital (16), open data policies play an important role in fostering social engagement, and kick-start and promote the development of new services based on novel ways to combine and make use of such information. They encourage the wide availability and re-use of public sector information for private or commercial purposes, with minimal or no legal, technical or financial constraints, thus promoting the circulation of information not only for economic operators but primarily for the public. The specific data sets that should be made available are detailed in the **Implementing Regulation (EU) 2023/138** that lays down a list of specific high-value data sets and the arrangements for their publication and re-use.[109]

The scope of the Open Data Directive does not include, however, data that is subject to rights of third parties, such as personal data and data protected by intellectual property rights (Article 1, (2), (c) and (d), Open Data Directive). Many of these data are not, therefore, immediately available for re-use, even for research or innovative activities. The need to comply with certain technical and legal requirements for making these protected data available is usually time- and knowledge-intensive, which has led to the insufficient use of such data.[110] The DGA does not create an obligation to allow

[108] International Transport Forum (2021), "Reporting Mobility Data Good Governance Principles and Practices", https://www.itf-oecd.org/sites/default/files/docs/reporting-mobility-data-governance-principles-practice.pdf.
[109] Commission Implementing Regulation (EU) 2023/138 (2023), "Laying down a list of specific high-value data sets and the arrangements for their publication and re-use", (Text with EEA relevance), C/2022/9562.
[110] Recital (6), DGA.

for the re-use of data held by public sector bodies, but specifies that Member States should support public sector bodies to make optimal use of privacy enhancing techniques and other safeguards to make as much data as possible available for sharing.[111]

The second important issue tackled by the DGA is the regulation of data intermediation services, which are particularly relevant for the EMDS. In line with the spirit of recent legislation, the EU's primary intention behind the creation of data spaces is to support data sharing. This intention is echoed in the very essence of data intermediaries who are to be neutral entities designed to build trust and support the uptake of data spaces. Specifically, the DGA's data intermediary introduces obligations and puts in place a notification procedure for specific types, including: (a) intermediation services between data holders and potential data users, (b) intermediation services between data subjects and potential data users, and (c) services of data cooperatives.[112] The requirements laid down by the legislation would affect the business model for the intermediary and should be carefully considered within the EMDS.

The EC's objective of creating a single market for data highlights the importance of supporting data transactions. Meanwhile, the new legislative interventions create new legal definitions aimed at clarifying rights and responsibilities with respect to data. However, despite these good intentions, there is still some uncertainty about the precise implementation of the recently established data intermediation services under the DGA, particularly with regard to their application within certain data spaces. The DSSC is developing a data space intermediary building block which may provide additional clarification on this matter and should be closely monitored by the EMDS. The recent Joint Research Centre report also provides an interesting analysis of the landscape of data intermediaries and aims to provide conceptual clarity on the topic, as well as their potential to promote inclusive data governance.[113]

The EMDS should closely follow the research in this area and could contribute by examining data intermediaries operating in the mobility sector. For instance, it can leverage the ecosystem inventory that was created as part of this project. Using this inventory as a foundation, the EMDS can organise workshops focused on this topic, involving relevant stakeholders in the discussions. Within the EMDS, guidance on the legal requirements for members of the data space should be provided to dispel uncertainty and build further support for data spaces. Therefore, clear guidance on the legal requirements for data space operators, data intermediaries and participants is crucial.[114]

It is also important to mention the impact that the **DA proposal** could have on the EMDS. The DA has been proposed to promote data sharing by setting rules on the rights to the data itself. In particular, it introduces rules for standardised access to product or related service data to the user of that connected product or service; data sharing between data holders and data recipients; data sharing with public authorities in cases of public interest; switching between data processing services; protection against unauthorised access to data; and interoperability standards for data use. Of particular importance for data spaces, the Regulation provides essential requirements for the interoperability of data spaces (Article 28) and for smart contracts to implement data sharing agreements (Article 30).

---

[111] Specifically, Chapter II, DGA, applies to data held by public sector bodies protected on grounds of: a) commercial confidentiality, including business, professional and company secrets; b) statistical confidentiality; c) the protection of intellectual property rights of third parties; or d) the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024.

[112] Article 10, DGA.

[113] Micheli, M., Farrell, E., Carballa Smichowski, B., Posada Sanchez, M., Signorelli, S. and Vespe, M. (2023), "Mapping the landscape of data intermediaries", Publications Office of the European Union, Luxembourg, JRC133988.

[114] For more information on the challenges and consequences of falling into the scope of the DGA's data intermediation services, see Bobev, T. et al. (2023), "White Paper on the Definition of Data Intermediation Services", CiTiP Working Paper Series, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4589987.

The DA will have an important impact on the mobility sector. Sharing data with public authorities in cases of public interest, for example, can have implications for mobility-related issues like traffic management, urban planning, and environmental regulations. This provision could enable more informed decision-making by public authorities based on accurate, real-time data from the mobility sector. Furthermore, Article 28's emphasis on the interoperability of data spaces is also crucial. The sector involves a wide array of stakeholders, including vehicle manufacturers, traffic management systems, navigation services, among others. Ensuring that data can be exchanged and used across these various entities is essential for optimising services.

The legislative process of the DA is still ongoing, and its text is not yet finalised, although an agreement has been reached between the EU Parliament and the Council.[115] However, based on the Proposal, questions arise, for example, on its application to networks such as the ITxPT, a non-profit association that "enables an open architecture, data accessibility and interoperability between IT systems. The members of ITxPT develop the IT architecture for public transport and other mobility services together, based on standards and best practices".[116] ITxPT's specifications have become a *de facto* standard and have already been used in procurement of IT solutions for public transport.[117] It could be understood that some components of the network, such as smart screens at bus stops, would not be covered by the definition of products under the DA, and some confusion might arise when actors play dual roles as data holders and data users "like a public transport authority with a product broadcasting schedules on buses it owns and leases to a public transport operator".[118] It will then be advisable to assess the right applicability of the DA to the EMDS once the final text becomes available.

Finally, the proposed **Interoperable Europe Act** is closely aligned with the objectives of the EMDS and demonstrates the potential synergies between these initiatives. The proposed Regulation is based on four pillars, each of which is in line with the key principles of the EMDS. Firstly, it establishes structured EU cooperation on cross-border interoperability in the public sector, thereby promoting cross-border cooperation, which is crucial in the field of mobility. Secondly, it introduces mandatory assessments, i.e. practical assessments for setting up or modifying an existing network and information system, including peer reviews by experts. Thirdly, it encourages the sharing and reuse of solutions through the Interoperable Europe Portal, thus promoting the spirit of encouraging knowledge and experimentation, a principle fundamental to both the proposed Regulation and the EMDS. Finally, the Interoperable Europe Act's commitment to innovation and support measures, exemplified by the GovTech Incubator, which refers to public-private partnerships, is perfectly in line with the ethos of the EMDS, which seeks to promote public-private collaboration. In essence, the Interoperable Europe Act and the EMDS share a common vision of promoting interoperability, collaboration and innovation to avoid fragmentation and break down data silos.

Platform regulations

This category is closely linked to the data-related regulations mentioned above and is another area of law that has recently been enriched by the EU legislator, namely the newly introduced **DMA** and **DSA**. These interventions focus on regulating specific dominant players in an effort to create a level playing field in the digital economy.

The DMA entered into force on 1 November 2022 and became applicable on 2 May 2023. It focuses on so-called "gatekeepers", which are identified through a specific list of criteria related to a strong

[115] European Council (2023, June 27), "Data Act. Council and Parliament strike a deal on fair access to and use of data", https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/data-act-council-and-parliament-strike-a-deal-on-fair-access-to-and-use-of-data/.
[116] ITxPT (n.d.), "Open IT architecture and interoperability", https://itxpt.org/.
[117] Burden, H., Stenberg, S., and Olsson, M. (2023), "Proposed EU Regulations' Impact on Data Utilisation: A Multi-Case Study within Public Transport", RISE Report No. 2023:47, RISE Research Institutes of Sweden AB, p. 7.
[118] Ibid, p. 27.

position in the market and an intermediation position.[119] The DMA is a novel approach to tackling the anti-competitive threats posed by online platforms. It focuses on providing *ex ante* obligations that can be applied before any wrongdoing takes place, complementing traditional EU competition law. The intention of the act is to address some shortcomings of the competition regime with respect to the data economy, and so it intertwines elements of data protection with competition law concepts. It seeks to directly prohibit certain exclusionary practices of online platforms by imposing obligations (see Article 6) such as requiring gatekeepers to provide free-of-charge, continuous, real-time data portability to business users and to implement interoperability. The intention is to limit gatekeepers' exclusive control over data and to allow business users to access and reuse data generated by them or by end users.

The DMA will likely only apply to a small number of core online platforms offering gateway services between consumers and businesses.[120] The EMDS will likely not be considered a gatekeeper. Nevertheless, participants in data spaces, whether individuals or organisations, may use the core platform services of gatekeepers and therefore it is pertinent to consider the DMA. More specifically, it may be beneficial to consider the potential impact on EMDS participants of the data access, data portability and interoperability provisions covered by the DMA.

Consideration should be given to the potential interest of gatekeepers' in joining a data space and the legal implications associated with their participation. For instance, Amazon Web Services recently joined Catena-X, an automotive-based data space.[121] Given Amazon's status as a gatekeeper, it is advisable to conduct further research on the legal ramifications of gatekeepers' involvement in data spaces. The EMDS should evaluate whether these stakeholders are likely participants and carefully weigh the implications.

The DSA, in comparison, focuses on setting out a framework for greater transparency, accountability and regulatory oversight of online services.[122] The DSA exists in addition to the e-Commerce Directive, the main legislation that regulates intermediary services.[123] It adopts a layered approach of obligations relating to providers of intermediary services, providers of hosting services, online platforms and marketplaces, and very large online platforms and search engines. This captures online intermediaries and platforms such as online travel and accommodation platforms, which may utilise, for example, deployed MaaS applications.[124]

Some services may fall under the DMA and DSA but for different reasons and with different types of provisions. The DSA specifically focuses on making a safer digital space by introducing new rules to protect users from harmful and illegal content. The DSA entered into force on 16 November 2022 and will apply from 17 February 2024. It introduces transparency obligations to empower individuals to make clearer choices and increase control over data.

---

[119] Note that a company is considered to be a gatekeeper under the DMA if it meets the following conditions for a minimum period of three years: an annual EU turnover of more than €7.5 billion, a market capitalisation of more than €75 billion and a user base of 45 million monthly active end users and at least 10,000 annual business customers. See Article 3 (1), DMA for further information on the criteria.

[120] On 6 September 2023, the European Commission designated the first six actors that are to be considered gatekeepers under the DMA: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, see European Commission (2023, September 6), "Digital Markets Act: Commission designates six gatekeepers", https://digital-strategy.ec.europa.eu/en/news/digital-markets-act-commission-designates-six-gatekeepers.

[121] Kolodziej, M. and Vazquez, Patricio (2023, March 27), "Enabling data sharing through data spaces and AWS", https://aws.amazon.com/blogs/publicsector/enabling-data-sharing-through-data-spaces-aws/.

[122] European Parliamentary Research Service (2021), "Digital Services Act", Briefing, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf.

[123] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, OJ L 178, 17.7.2000, p. 1–16.

[124] Antoniola, M. (2023), "The Future of Mobility Data Spaces. The role of Local Governments", *Network Industries Quarterly*, 25(2), https://cadmus.eui.eu/bitstream/handle/1814/75776/NIQ-Vol-25-Issue-2-june-2023.pdf?sequence=1, p. 17.

The **Platform to Business Regulation** was enacted in 2019 to establish fairness and transparency between online platforms and businesses using them. It includes provisions similar to consumer laws, promoting transparency, notifying changes in terms, and providing redress options. These services must ensure clear terms, notify changes, and describe data access conditions to business users. The Regulation does not contain obligations to share data but may contribute to data sharing by providing business users with a more solid and predictable framework for operation. The application of this framework will depend on a number of factors, such as the setup of the EMDS, the different EMDS actors and their legal characterisation as well as the relationships the EMDS plans to establish. Depending on the setup of the EMDS, it will have to be clarified who falls under the category "platform" and which actors are considered "business users". This determination will be made on a case-by-case basis.

In summary, the establishment of a data space may require the development of an entire ecosystem, potentially including some form of online platform to facilitate the exchange of data between participants. It is not yet established whether an existing platform(s) would be used, or a new platform created for the EMDS. Various models can be considered based on business and technical decisions. The application of platform regulations to data spaces, and more specifically to the EMDS, is still unclear as it will depend on the nature of the data space (including size, market dominance, financial information, etc.). The legislation presented above shows that various categories of online platforms and services, such as intermediaries, hosting services, online intermediation services, very large online platforms, and core platform services, are subject to specific legislation. Given the current nascent nature of data spaces, it is unlikely that many of these will be directly applicable to data space initiatives. However, this assessment should be revisited as data spaces deploy and scale (and possible federation between multiple data spaces occurs), with different stakeholders becoming involved.

More importantly for the EMDS itself, it is imperative to ensure that data intermediation service providers are compliant with the DGA and that they fulfil the obligations set out therein. The cluster of platform legislation is also important for the business cases that will use the EMDS. The MDS, for example, notes business cases that include online platforms such as CARUSO and FREE NOW participating in the data space.[125] Therefore, the specific use cases for the EMDS should carefully assess the applicability of this cluster of legislation to both their activities and the potential opportunities it offers in terms of relationships with gatekeepers.

Intellectual Property law

The EMDS should take into account and respect the conditions for data sharing, including intellectual property rights. Intellectual property law is a prime example of a legacy legal framework in the data economy. It encompasses patents, trademarks, designs, copyright and related rights. Intellectual property law can confer rights over data, often through **copyright** and the ***sui generis* database right**. It is the responsibility of each data space participant to ensure legal compliance and to have an authorisation and/or legal basis for data sharing.

Copyright law protects creative works such as text, images, video and sound that may be shared in EMDS. To determine whether copyright applies, it is important to check if the data in question fall within the scope of subject matter eligible for copyright protection. It must be original, reflect the author's own intellectual creation and be fixed in a tangible form. Article 2 of the **InfoSoc Directive** outlines information that is not eligible, such as ideas, procedures, methods of operation, and mathematical concepts. Accordingly, data containing purely factual information is not normally eligible for copyright protection. This includes data captured through sensing or tracking technologies, with the sharing of real-time streaming data being of particular importance to the EMDS.

[125] Mobility Data Space (2023, July), "The Mobility Data Space data marketplace", https://mobility-dataspace.eu/fileadmin/05_presse_medien/Pressemitteilungen_EN/2023-07-17_MDS-Press_Kit_EN.pdf.

In addition to copyright protection, the EU's **Database Directive** (Directive 96/9/EC) harmonises the legal protection of databases in the EU Member States. It grants copyright-like rights, known as the "*sui generis* database right," to creators that have made "qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents". The database right provides the maker with the right to prevent unauthorised extraction or re-utilisation of the whole or a substantial part of the database contents. Article 1 of the Database Directive defines databases as "collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means".

Therefore, a key legal requirement is "substantial investment". By "investment", Recital (40), provides that it may "consist in the deployment of financial resources and/or the expending of time, effort and energy". Regarding database rights, the EU Database Directive protects the systematic arrangement of data collections, granting exclusive rights to investors for 15 years. However, it does not protect the data itself. Providers of structured data should consider if they can claim database rights, granting licenses and safeguarding against modifications that could create new rights. It is also important to note that databases which do not qualify for *sui generis* protection may freely be determined based on contracts.[126] Where there is both originality and substantial investment, both forms of protection can co-exist.[127]

The proposed DA provides further clarification on the *sui generis* database right in relation to the sharing of IoT-generated data. In particular, chapter X of the proposed DA contains a single article, Article 35, which confirms that the *sui generis* database right does not apply to "databases containing data obtained from or generated by the use of a[n] [IoT] product or a related service".[128] By including this exemption, the EU seeks to address the legal uncertainty surrounding IoT data and safeguard users' rights to access and use their data as introduced under the DA.[129]

Trade secret protection can exist alongside intellectual property rights and can be used to protect confidential business information and maintain a competitive advantage.[130] Trade secrets can encompass various types of data, including individual data items and databases, as long as they meet the requirements of secrecy and have commercial value. It can sometimes be difficult to determine whether a piece of data meets the threshold for secrecy. One example would be information related to the exact location of potholes, information which is known to many citizens, but which could give a company a competitive advantage, particularly if the cost of acquiring the data is substantial.[131] Assessing whether such data qualifies as a trade secret underscores the inherent difficulty in making this determination and the need to assess it on a case-by-case basis.

Generally, neither data generated by sensors nor real-time streaming data are considered trade secrets. However, there could be cases where the insights derived from sensor data, the algorithms used to process it or the specific configurations of sensor networks could potentially be considered trade secrets if they meet the criteria for trade secret protection. Trade secrets are often reserved for elements of the manufacturing process or supply chains. It could be possible for a company to develop

[126] See Borghi, M. and Karapapa, S. (2015), "Contractual Restrictions on Lawful Use of Information: Sole-Source Databases Protected by the Back Door?", 37(8), European Intellectual Property Review.
[127] Margoni T. (2016), "The Harmonisation of EU Copyright Law: The Originality Standard" in Mark Perry (ed), Global Governance of Intellectual Property in the 21st Century: Reflecting Policy Through Change (Springer International Publishing) 94.
[128] Art. 35 of the Data Act proposal.
[129] Art. 4 and 5 of the Data Act proposal.
[130] European Commission (2018), "Commission Staff Working Document. Evaluation of Directive 96/9/EC on the legal protection of databases", SWD147 final, p. 43.
[131] Josef Drexl et al. (2016), "Data Ownership and Access to Data - Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate", Max Planck Institute for Innovation and Competition, p. 21.

a highly accurate prediction model for traffic patterns, and protect the methodology and data employed as trade secrets to maintain their competitive advantage.

To benefit from trade secret protection, EMDS participants must assess and document the commercial value and secrecy of the specific data, along with the protective measures employed, prior to sharing in the data space. Through implementing appropriate technical measures such as access control mechanisms and organisational measures such as data sharing agreements in the EMDS, the data provider should remain able to define access rights to the data and put in place confidentiality agreements to prevent unauthorised access by third parties, so that the protection of trade secrets is maintained when the data is shared. Trade secret protection provides enforceable rights against unlawful use and misappropriation of data. Therefore, it does not confer a property right but rather puts in place a liability regime. It is important to emphasise to EMDS participants that trade secret protection depends on strict preservation of *de facto* secrecy to maintain trade secret protection.

The matter of trade secrets concerning data is to be further clarified in the upcoming DA concerning data access and usage.[132] There is a noticeable emphasis on strengthening the protection of intellectual property and trade secrets, particularly in the automotive sector.[133] Therefore, the EMDS and its participants should carefully consider the role of intellectual property and trade secrets and monitor developments with the DA.

Competition law

At the centre of competition law is the premise of enacting rules to protect the process of fair competition, that is "ensuring that firms operating in a free market economy do not, by acting anti-competitively, prevent the market from functioning optimally".[134] EU competition law is largely regulated under **Articles 101 and 102 of the Treaty on the Functioning of the EU (TFEU)**. The recently updated guidelines on the applicability of Article 101 TFEU on Horizontal Cooperation Agreements and the Horizontal Block Exemption Regulations are also relevant and should be carefully considered. It is worth noting that vertical agreements in mobility sub-sectors such as the automotive sector may also benefit from a block exemption, which is a "safe harbour that exempts a whole category of motor vehicle distribution and repair agreements from the prohibition of Article 101(1) TFEU."[135] The Motor Vehicle Block Exemption Regulation was recently reviewed by the Commission and they adopted both the Regulation prolonging the Motor Vehicle Block Exemption Regulation until 31 May 2028 and the Communication amending the Supplementary Guidelines in April 2023.[136] Similarly, there is the block exemption for liner shipping consortia which permits cooperation, including information exchange, under certain conditions, namely, a market share limit of 30%, to encourage "greater utilisation of containers and more efficient use of vessel capacity."[137] The potential application of such exemptions should be carefully assessed on a case-by-case basis.

---

[132] European Commission (2021), "Inception Impact Assessment Data Act initiative", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2021)3527151.

[133] DIGITALEUROPE (2021), "DIGTALEUROPE Access to In-Vehicle Data Position Paper", https://cdn.digitaleurope.org/uploads/2023/08/DIGITALEUROPE-Access-to-Vehicle-Data-Position-Paper_10.08.2023-FINAL_V4.4.pdf.

[134] Jones, Sufrin and Dune, *Jones and Sufrin's EU Competition Law: Text, Cases and Materials*, Oxford University Press, 2023 pp 2.

[135] European Commission (n.d.), "Legislation (Motor vehicles)", https://competition-policy.ec.europa.eu/sectors/motor-vehicles/legislation_en.

[136] For further information on the review see European Commission (n.d.), "Review of the Motor Vehicle Block Exemption Regulation", https://competition-policy.ec.europa.eu/sectors/motor-vehicles/review-motor-vehicle-block-exemption-regulation_en and European Commission (2023), "Commission Staff Working Document. Stakeholder Consultation – Synopsis Report", https://competition-policy.ec.europa.eu/system/files/2023-04/2023_MVBER_synopsis_report_en_0.pdf.

[137] European Union (2009), "Recital 5. Commission Regulation no 906/2009", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0906.

The EMDS is expected to bring together mobility actors to share data. However, their often competitive relationships may raise questions regarding the appropriate governance structures for collaboration and cooperation. Competition law requirements may, depending on the circumstances, result in prohibitions on sharing certain data with specific entities, or obligations to cooperate and share data. The conditions for access to the data space also need to be carefully considered in the EMDS.

Article 101 TFEU refers to the prohibition of agreements, concerted practices that restrict competition (by object or effect), with an effect on trade between Member States. That is, unless restriction is justified by efficiencies that are greater than the harm satisfying the conditions under Article 101(3). Companies must be careful not to distort markets by making agreements that restrain competition or result in coordinated behaviour. Data sharing could be considered illegal under Article 101 TFEU if it involves the exchange of sensitive information between market participants that are competitors or potential competitors. This exchange of information may lead to an awareness of each other's market strategies, thereby influencing their economic behaviour which under fair competition should be determined independently. Other exchanges of information will require a case-by-case assessment of the likely impact on competition to determine whether they fall afoul of Article 101 TFEU. If the information exchange is limited to what is necessary for genuine cooperation between actual or potential competitors and leads to efficiencies that can easily be passed on to consumers, it is more likely to be permitted.[138]

'Information' is defined as "i) raw data); (ii) pre-processed data, that has already been prepared and validated; (iii) data that has been manipulated in order to produce meaningful information of any form, as well as (iv) any other type of information, including non-digital information".[139] According to the Horizontal Cooperation Guidelines, information exchange can take various forms: data can be directly shared between competitors or indirectly through a common agency (for example, a trade association) or a third party such as a market research organisation or the companies' suppliers or retailers[140] (so-called "*hub and spoke*" or "ABC" collusion). Particularly relevant for the data economy are the latter given the EC's focus on intermediaries to facilitate data sharing. The guidelines note that information exchange is also possible online through a platform or online tool, integrating conclusions of the *Eturas*[141] case which concerned collusion through a third party not via human coordination, but rather through automated means.

With regard to data exchange, the guidelines further recognise that data sharing may generate efficiency gains.[142] In particular, data sharing that has genuine pro-competitive effects (such as improved efficiency, customer service, and new products, services or technologies) will generally not be considered a "hardcore restriction" of competition.[143] Especially important for the EMDS, the guidelines note that data sharing for sustainability purposes may help organisations to meet their sustainability obligations under EU or national law. The guidelines provide measures to mitigate competition law violations, such as the use of trustees, confidentiality rules and technical measures. This is in line with the intentions of the EMDS to support data sovereignty and ensure that participants retain control of their data and are able to set access controls. It is the responsibility of each participant

[138] Batchelor, B. and Kafetzopoulos, A. (2023, June 8), "New EU Competitors Cooperation Framework. Stricter on Information Exchange, Broader on Joint Sustainability Agreements", Skadden alert, https://www.skadden.com/insights/publications/2023/06/new-eu-competitors-cooperation-framework.
[139] European Commission (2023), "Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements", Annex to the communication from the commission, p. 367.
[140] Ibid, p. 368 and 401 onwards.
[141] Case C-74/14, "Eturas and Others" (2016), ECLI:EU:C:2016:42.
[142] European Commission (2023), "Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements", Annex to the communication from the commission, p.373.
[143] These are considered as particularly harmful and severe restrictions, which are likely to restrict competition and harm consumers or are not indispensable to the attainment of efficiency-enhancing effects.

to consider competition law implications and ensure data is shared for legitimate purposes in the EMDS.

The Horizontal Cooperation Guidelines provide practical examples, self-assessment steps and a liability risk framework to guide companies and associations considering information exchange. The guidelines warn against anti-competitive data sharing and emphasise the importance of context and market characteristics but do not provide guidance on the specificities of each sector. It should be noted that the revised guidelines were only adopted on 1 June 2023, so further review and analysis of their potential implementation in the context of data spaces and the mobility sector should be closely monitored and considered for the EMDS.

Article 102 TFEU, which addresses abusive practices by dominant companies, can be applicable to data sharing practices. Abusive behaviours in data sharing may include refusal to share, discriminatory treatment, exploitation through unlawful processing, or unfair terms. For example, Company A, such as a MaaS service provider, may want access to certain data held by Company B, such as bike-sharing information. Company A could approach Company B and ask to enter into a data sharing agreement. However, if Company B, which holds the commercially valuable data and is in a dominant position, abuses that position by refusing to grant access by allowing data sharing only on unequal or discriminatory terms, this may raise concerns under Article 102. The definition of dominance in this context, including the determination of relevant markets, remains an open question. If certain conditions are met, such as the indispensability of data or the elimination of effective competition in the downstream market, competition authorities may compel the dominant company to provide access to data under the "essential facilities" doctrine.[144]

Trust and security

Trust and security, especially the implementation of robust cyber resilience measures, are fundamental to data spaces. Such measures are crucial for guaranteeing confidentiality, integrity and availability of information within data spaces, thus strengthening privacy, building trust among stakeholders, protecting people and assets, and mitigating legal and reputational risks. More specifically, verifiable credentials[145] and the development of the European Digital Identity are expected to play an important role in supporting the functioning of data spaces. Work from the DTLF reveal the potential opportunities for the mobility and logistics sector, specifically the automation of customer onboarding and faster driver license verification, and its possible role in logistics for sharing different types of electronic documents between business-to-business and business-to-government (e-CMR, e-AWB, etc.).[146]

Critical sectors, such as mobility, increasingly depend on data and digital technologies. However, while digital connectivity brings opportunities, it also exposes society to cyber-threats.[147] The first EU-wide legislation on cybersecurity was the Directive on Security of Network and Information Systems across the EU (the NIS Directive), which laid down rules on improving cybersecurity levels in the Union. The EU cybersecurity strategy for 2020-2025[148] proposed the review of the NIS Directive, which resulted in

[144] For more information see Graef, I. (2015), "Market Definition and Market Power in Data: The Case of Online Platforms", World Competition: Law and Economics Review, 38(4), https://ssrn.com/abstract=2657732, p. 489.
[145] For more information on the technical architecture for data spaces see Data Spaces Business Alliance (2023), "Technical Convergence Paper, Discussion Document", Version 2.0, https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.
[146] Vedler, R. (2023), Principles for Creating a Sustainable eFTI Technological Environment.
[147] European Parliamentary Research Service (2023), "The NIS2 Directive. A high common level of cybersecurity in the EU", https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.
[148] European Commission (2020, December 16), "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient", https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

the NIS 2 Directive.[149] The **NIS 2 Directive** entered into force on 16 January 2023 and Member States have until 17 October 2024 to incorporate it. Together with the NIS 2 Directive, the Commission proposed the review of the Resilience of Critical Entities Directive,[150] which expands the scope and depth of the 2008 directive to cover eleven sectors, including transport.

Another important legal framework connected to cybersecurity is the electronic IDentification Authentication and trust Services **(eIDAS) regulation**[151], which lays down conditions for electronic identification and trust services and is currently under revision.[152] Developments in the area of digital identity, in particular online identification, authorisation and authentication, are of particular interest for data spaces and are likely to play a key role in enabling them. Complying with the legal framework on trust and security is crucial for the EMDS, especially considering transport as a critical sector. First, the safety of passengers, goods and infrastructure is paramount as cyberattacks can compromise safety controls, and even lead to accidents. Second, these attacks can disrupt operations and impede their continuity, which has far-reaching impacts on economies and societies. Finally, public confidence is essential for data spaces, especially when they are deeply rooted in essential services like the EMDS. Cyberattacks can erode public trust in the safety and reliability of the EMDS, especially when personal data are involved.

It is important to mention that the legal requirements related to trust and security should be aligned with the implementation of the "Data sovereignty and trust" technical building block. Complying with these requirements is the first step to guaranteeing that data space participants exercise sovereignty in relation to data they share and that data subjects trust that they will be able to exercise control over their data.

Contract law

The characteristics of existing data contracts are primarily shaped by prevailing market norms and national contract laws. This is mainly due to the lack of harmonisation of contract law at the EU level. However, it is important to clarify that while there is no comprehensive EU contract law, certain aspects such as consumer protection and unfair commercial practices have been harmonised. Furthermore, there is currently no enacted legislation that directly addresses the sharing and use of data or the contractual interactions between parties involved in data contracts. This will change with the introduction of the DA, which will be the first piece of legislation in this area.

Contracts play a crucial role in the EMDS as they concretely establish the legal framework for data sharing and govern the rights and obligations of parties involved. Contracts define the terms of data exchange, including data access, ownership, usage rights, confidentiality, and data protection measures. They help establish trust among stakeholders, ensure compliance with applicable laws and regulations, and may provide a mechanism for resolving disputes. Contracts in the EMDS facilitate the smooth functioning of data transactions, promote accountability, and protect the interests of all parties involved, thereby fostering a secure and collaborative environment for data sharing and innovation.

---

[149] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[150] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[151] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[152] Data Spaces Business Alliance (2023), "Technical Convergence Paper. Discussion Document", Version 2.0, https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.

The DSSC Glossary defines data transaction as "[a]n act between two or more transaction participants which has as its object the data usage and/or the rights permitting data usage. Data transaction relates to the technical and legal arrangements necessary to enable the proper use of data by the data recipient."[153] Contracts play a crucial role in ensuring clear terms and conditions for the data transaction, including rights, obligations and responsibilities. They also foster trust among the involved parties by providing greater control over how the data will be used.

The proposed DA is expected to have important implications for data contracts, as it contains measures on the access generated through use of connected devices. The DA is expected to limit the contractual freedom of parties in defining the content of data contracts, by imposing obligations that impact the structure and content of data contracts. Specifically, it aims to rebalance the negotiating powers of SMEs by preventing the abuse of contractual imbalances in data contracts relating to data access and use. Further research could consider the role of neutral data intermediaries, as established through the DGA, to support such access rights set forth in the DA. Specifically how data intermediaries could be enablers for data reuse in the EMDS.

As shown by the review of legal clusters, the legal landscape is complex and fragmented. The approach to data and the associated objectives varies between legal frameworks, ranging from promoting the free flow of data to strong protection efforts. In the absence of a clear default legal status for data, contracts are often used to fill the gap, with the party in physical control of the data able to make contractual arrangements. During the questionnaire and interviews carried out in the project, various respondents noted the role of contracts in ensuring data sharing. For example, Creative Commons licences are increasingly used by organisations to maximise the re-use of data and databases. As noted earlier, it may be difficult to determine whether data and databases are restricted by copyright or database rights, so the CC0 Public Domain Dedication can be used to make it clear that the data can be freely re-used.[154]

Data contracts must, therefore, align with applicable legal and regulatory frameworks, including data protection, intellectual property, competition, and consumer protection laws. Ensuring compliance with these laws and addressing any potential conflicts or gaps in the contract is crucial to mitigate legal risks and disputes. Data contracts may be susceptible to ambiguity or incomplete terms, leading to misunderstandings or disputes between parties. Vague definitions, unclear rights and obligations, or inadequate specifications of data usage can create challenges in interpreting and enforcing the contract.

Several initiatives already provide useful guidelines, principles and templates on data contracts. The DSSC is currently building on these initiatives to develop a Catalogue of Contractual Modules that could also be applied for the EMDS and further adapted to the mobility context:

- SITRA Rulebook for a Fair Data Economy[155]
  - Constitutive Agreement
    - General terms and conditions
    - Governance model
    - Accession Agreement
  - Data set Terms of Use
    - Description of the Data Network

[153] Data Spaces Support Centre (2023), "DSSC Glossary", https://dssc.eu/wp-content/uploads/2023/03/DSSC-Data-Spaces-Glossary-v1.0.pdf.
[154] See Creative Commons (n.d.), "Open Data", https://creativecommons.org/about/program-areas/open-data.
[155] See SITRA (2022), "Rulebook for a fair data economy", https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy/. The example set forth by the SITRA Rulebook is currently being further explored by the International Data Spaces Association in the context of IDS.

- Draft Common Frame of Reference [156] – Principles of European Contract Law [157]
- ELI-ALI Model clauses[158]
- Orgalim Legal guide on industrial data [159]
- iSHARE Legal Framework
- IDSA Rulebook[160]
- Support Centre for Data Sharing's Report on development of set of recommended contract terms
- EU initiatives: DA (Article 34)

Specifically, within the mobility sector, the Maas Alliance Working Group recommends standardised data license agreements, such as Open License[161] used by the French National Access Point,[162] or the rulebook[163] used by the Finnish National Access Point[164] for mobility data spaces.[165]

Furthermore, there are also efforts to shift towards contract automation to better facilitate data spaces. Notable work in this area can be attributed to the Legal TestBeds developed under Plattform Industrie 4.0[166], a specific example being the sample contract template they have developed for Terms of Use and made available under a Creative Commons Licence CC BY 4.0.[167] It sets out a number of key principles and the sample contract could be adapted by other data spaces such as the EMDS.

During the interviews conducted, a project manager of the MDS noted that they provide sample clauses to facilitate contract negotiations and are exploring the potential of automated payment processing for the future.[168] Smart contracts have the potential to play a crucial role in supporting the EMDS, particularly for logistics, given the importance of event-driven real-time data flows. Smart contracts are self-executing agreements written in code that automatically execute predefined actions when specific conditions are met. In the context of the EMDS, smart contracts can facilitate data sharing, data transactions, and interactions between different stakeholders, such as mobility service providers, data aggregators, and consumers.

One key advantage of smart contracts is their ability to automate and streamline processes. They eliminate the need for intermediaries or centralised authorities, reducing transaction costs and delays. Smart contracts can define the terms, conditions, and rules for data sharing agreements, ensuring that all parties involved adhere to the agreed-upon terms. This transparency and automation contribute to trust-building and facilitate seamless data transactions.

---

[156] Trans-Lex. "Draft Common Frame of Reference (DCFR) - Outline Edition (2009)", https://www.trans-lex.org/400725/_/outline-edition-.
[157] Trans-Lex. "Principles of European Contract Law - PECL", https://www.trans-lex.org/400200/_/pecl.
[158] Cohen, N. and Wendehorst, C. (2021), "ALI_ELI Principles for a Data Economy. Data Transactions and Data Rights", https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf.
[159] See Orgalim (2021), "Orgalim legal guide on industrial data", https://orgalim.eu/legal-publications/orgalim-legal-guide-industrial-data.
[160] See International Data Spaces (2023), IDSA Rulebook, White Paper, https://docs.internationaldataspaces.org/idsa-rulebook-v2/front-matter/readme.
[161] etalab (2018), "Open License 2.0", https://www.etalab.gouv.fr/wp-content/uploads/2018/11/open-licence.pdf.
[162] Ministère Chargé des Transports (n.d.), "French national access point to transport data", https://transport.data.gouv.fr/.
[163] For the adaption of the Sitra rulebook for their mobility data ecosystem, see SITRA (2022), "Traffic Data Ecosystem Rulebook", Version 0.93 draft, https://1drv.ms/b/s!AgxxevMq0vX8goInf_p4bXOMJMj6gQ?e=Pc3VGv.
[164] Fintraffic, Traffic Data Ecosystem (n.d.) "Traffic Data Ecosystem", https://www.fintraffic.fi/en/trafficecosystem.
[165] MaaS Alliance (2022), "Mobility Data Spaces and MaaS", https://maas-alliance.eu/wp-content/uploads/2022/10/MaaS-Alliance-Whitepaper-on-Mobility-Data-Spaces-1.pdf.
[166] See Legal Test Bed (n.d.), "We are making Industry 4.0 legally compliant", https://legaltestbed.org/en/start/.
[167] See Plattform Industrie 4.0 (2021, May 5), "Term of Use for an Industrie 4.0 Platform", Sample contract template, https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/RTB_contract_template.html.
[168] Mobility Data Space (2023), "The Mobility Data Space data marketplace", https://mobility-dataspace.eu/fileadmin/05_presse_medien/Pressemitteilungen_EN/2023-07-17_MDS-Press_Kit_EN.pdf.

Moreover, smart contracts can enhance data security and privacy. They can incorporate encryption and authentication mechanisms, ensuring that data shared within the EMDS is protected and accessed only by authorised parties. Smart contracts can also enable data owners to have greater control over their data, specifying how it can be used, shared, and monetised. This empowers individuals and organisations to maintain control and privacy rights over their data. Additionally, smart contracts can enable interoperability and data standardisation within the EMDS. They could define data formats, protocols, and interfaces, ensuring compatibility and facilitating data exchange between different systems and platforms. This promotes collaboration, innovation, and the development of new mobility services and solutions.

However, challenges and considerations exist when implementing smart contracts in a mobility data space. Technical complexities, legal compliance, and ensuring accuracy and reliability of the code are important aspects to address.[169] It is important for the EMDS to consider how the DA will impact the utilisation of smart contracts. Parties responsible for smart contract compliance must meet essential requirements, with vendors or deployers conducting assessments, issuing an EU Declaration of Conformity, and assuming responsibility for compliance. Adherence to harmonised standards is allowed for easier compliance. Recent DA revisions eliminated certain requirements from earlier drafts, such as equivalence with non-smart contracts and protection of trade secrets. Consequently, when the official DA text is available, additional research is needed to comprehend its implications on smart contracts within data space governance.

Nevertheless, it is recommended that dispute resolution mechanisms need to be established to handle potential conflicts arising from smart contract execution. Overall, the potential of smart contracts in supporting the EMDS lies in their ability to automate processes, enhance security and privacy, foster interoperability, and facilitate trustworthy data transactions. Further research and development are needed to explore the full potential of smart contracts, address technical and legal challenges, and ensure their effective integration within the EMDS.

5.3. Mobility specific legislation

The EC's compiled summary of EU legislation in the transport sector serves as a valuable foundation for exploring mobility specific legislation.[170] The provided list of categories includes air transport, road transport, rail transport, and more, giving an initial glimpse of the extensive legislation within the mobility and transport sector. These categories also underscore crucial considerations within the EMDS, such as mode-specific regulations and safety concerns. Mode-specific regulations establish distinct standards and requirements for various modes of transportation. However, it is important to consider that mode-specific regulations, while necessary for safety and efficiency, may lead to a fragmented landscape within the mobility sector. This diversity of regulations can impede data sharing across the entire mobility sector, and they should be carefully considered depending on the use cases applied within the EMDS.

As part of the EC's Digital Decade policy programme, digitalisation targets have been set in several areas, including mobility, specifically the support for "secure and sustainable digital infrastructures, the digital transformation of business and the digitalisation of public services."[171] Data, technology and

[169] For more information see Casolari, F. et al. (2023), "Correction to: How to Improve Smart Contracts in the European Union Data Act", DISO, 2(9), which outlines five challenges associated with smart contracts within the context of EU law: limited adaptability concerning both content and functioning, reliance on oracles that might introduce errors, susceptibility to software bugs and architectural modifications, issues related to immutability and privacy, and enforcement difficulties.
[170] For more information, see EUR-Lex (n.d.), "Transport", https://eur-lex.europa.eu/summary/chapter/transport.html?root_default=SUM_1_CODED=32.
[171] European Parliament (2021), "Shaping the digital transformation: EU Strategy explained", News, https://www.europarl.europa.eu/news/en/headlines/society/20210414STO02010/shaping-the-digital-transformation-eu-strategy-explained.

infrastructure are clearly at the heart of the policy, and are foundations of the mobility sector. At the same time, mobility, and, more specifically, the transportation sector, is increasingly demanded to become more sustainable, globally competitive and resilient. The European Green Deal and the EU Strategy for sustainable and smart mobility, for example, emphasise the need for emissions to be cut in order to face climate change challenges.[172] These digitalisation and datafication efforts also require that current mobility legislation be reviewed to ensure it effectively supports these opportunities and addresses societal challenges. This process is already underway, with a systematic review of legislation in progress and some updated provisions entering the implementation phase. These efforts emphasise the EU's proactive approach in shaping a regulatory framework that facilitates seamless data exchange and fosters technological advancements across the transportation sector.

There are a number of actions (recently completed or ongoing) that aim to further support digitalisation and data sharing in the mobility and logistics sector. Some of the key activities in this area are listed below:

- Ongoing Revision of Directive 2010/40/EU on the deployment of intelligent transport systems – Provisional agreement reached by the Council and European Parliament on 8 June 2023, and approved by the European Parliament's Committee on Transport and Tourism on 26 June 2023.[173]
- Revised Delegated Regulation (EU) No 2022/670 with regard to the provision of EU-wide on Real-Time Traffic Information services (RTTI) repealing and replacing Delegated Regulation (EU) 2015/962 as from 1 January 2025.[174]
- Ongoing revision of Delegated Regulation (EU) 2017/1926 with regard to the provision of EU-wide Multimodal Travel Information Services (MMTIS).[175]
- Ongoing revision of the European Directive on River Information Services (RIS).[176]
- Adoption of delegated and implementing acts for European Maritime Single Window environment Regulation.[177]
- Ongoing adoption of delegated[178] and implementing acts for eFTI Regulation, including the interface with the eIDAS 2.0 regulation.[179]
- Proposed rules on a trustworthy environment for corridor data exchange to support collaborative logistics.[180]

---

[172] European Parliamentary Research Service (2021), "Review of the Intelligent Transport Systems Directive", https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/694240/EPRS_BRI(2021)694240_EN.pdf.

[173] European Parliament (2023), "Review of the Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport", Legislative Train Schedule,https://www.europarl.europa.eu/legislative-train/theme-a-european-green-deal/file-intelligent-transport-systems-directive-review.

[174] Commission Delegated Regulation (EU) 2022/670 of 2 February 2022 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services.

[175] Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services.

[176] European Parliament (2023), "Revision of the directive on harmonised river information services", Legislative Trains Schedule, https://www.europarl.europa.eu/legislative-train/theme-a-european-green-deal/file-karin.

[177] Commission Implementing Regulation (EU) 2023/204 of 28 October 2022 laying down technical specifications, standards and procedures for the European Maritime Single Window environment pursuant to Regulation (EU) 2019/1239 (Text with EEA relevance), C/2022/7649.

[178] Commission Delegated Regulation (EU) 2023/205 of 7 November 2022 supplementing Regulation (EU) 2019/1239 as regards the establishment of the European Maritime Single Window environment data set and amending its Annex (Text with EEA relevance), C/2022/7842.

[179] European Parliament (2023), "Regulation on electronic freight transport information", Legislative Train Schedule, https://www.europarl.europa.eu/legislative-train/package-eu-mobility-package/file-electronic-freight-transport-information.

[180] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Sustainable and Smart Mobility Strategy (2020), "Putting European transport on track for the future", COM/2020/789 final.

- Consideration of further regulation on access to in-vehicle data - The Commission published a call for evidence, accompanied by an open public consultation on a proposal on access to vehicle data, functions and resources, which would complement the DA Proposal published in February 2022.[181]
- Ongoing work on the Multimodal Digital Mobility Services (MDMS) initiative – The Commission held a public consultation in 2022[182] and stakeholder workshop in February 2023.[183]
- Adoption by the Commission of a Delegated Regulation on common EU specifications for Cooperative Intelligent Transport Systems (C-ITS) to improve road safety by enabling vehicles to communicate with each other and the infrastructure. However, the Delegated Regulation did not enter into force following an objection by the Council of the EU.[184]

Taking a closer look at the initiatives most relevant for the EMDS, Directive 2010/40/EU, known as the **ITS Directive**, was established to facilitate the coordinated and coherent deployment and use of Intelligent Transport Systems (ITS) in road transport and its connections to other modes of transportation. The ITS Directive is a fundamental legal instrument for the EMDS, as "it provides for the availability and accessibility of multimodal traffic and travel data on National Access Points (NAPs)".[185] Although the European transport sector has witnessed a significant increase in the deployment and utilisation of technologies and ITS services since its adoption, a review by the Commission indicated that further action was required.[186] For example, this includes a stronger coordination mechanism between the NAPs.[187]

The ITS Directive was introduced to establish the necessary mechanisms to support the deployment of ITS services and applications for road transport, as well as their interconnection with other transport modes.[188] In its efforts to update mobility legislation, the EC introduced a proposal on 15 December 2021 to revise the directive. This proposal is one component of a broader legislative package aimed at supporting decarbonisation, digital transformation, and enhanced resilience in transport infrastructure. On 8 June 2023, it was announced that the EU Parliament and the Council have reached a political agreement on the revised ITS Directive.[189] The updated Directive seeks to incorporate

[181] European Commission (2022, March 30), "Commission seeks views on possible measures on access to in-vehicle data", News article, https://single-market-economy.ec.europa.eu/news/commission-seeks-views-possible-measures-access-vehicle-data-2022-03-30_en.

[182] For an overview of the initiative, see European Commission (2021), "Multimodal digital mobility services", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13133-Multimodal-digital-mobility-services_en and for details on the public workshop impact assessment in 2022, see European Commission (2022), "1st Public workshop impact assessment for the initiative on Multimodal Digital Mobility Services", News article, https://transport.ec.europa.eu/news-events/news/1st-public-workshop-impact-assessment-initiative-multimodal-digital-mobility-services-2022-03-17_en.

[183] European Commission (2023, February 15), "Public workshop on the Multimodal Digital Mobility Services initiative", https://transport.ec.europa.eu/news-events/news/public-workshop-multimodal-digital-mobility-services-initiative-2023-02-15_en.

[184] European Commission (2021), "Cooperative, connected and automated mobility (CCAM)", https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/cooperative-connected-and-automated-mobility-ccam_en.

[185] European Commission (2021), "Proposal for a Directive amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (Text with EEA relevance)", (COM(2021) 813 final), p. 4.

[186] See European Commission (2019), "Commission Staff Working Document. Ex post Evaluation of the Intelligent Transport Systems Directive 2010/40/EU", https://transport.ec.europa.eu/system/files/2019-11/swd20190368-evaluation-report.pdf.

[187] For more information on harmonisation efforts for National Access Points (NAPs), see European ITS Platforms (n.d.), "Monitoring and Harmonisation of National Access Points", https://www.its-platform.eu/achievement/monitoring-harmonisation-of-naps.

[188] European Commission (2019), "Support study for the ex-post evaluation of the ITS Directive 2010/40/EU", Final report, https://op.europa.eu/en/publication-detail/-/publication/61597d8c-e99e-11e9-9c4e- 01aa75ed71a1, p. 11.

[189] European Council (2023, June 8), "Council and Parliament strike a deal on the roll-out of intelligent transport systems", https://www.consilium.europa.eu/en/press/press-releases/2023/06/08/council-and-parliament-strike-a-deal-on-the-roll-out-of-intelligent-transport-systems.

technological advancements such as connected and automated mobility, on-demand mobility apps, and multimodal transportation. Its goal is to expedite the availability and improve the compatibility of digital data that fuels these services. As a result, the proposal plays a crucial role in establishing the EMDS.

A number of Delegated Regulations were adopted under the ITS Directive. The revised **RTTI** Delegated Regulation was adopted in 2022. The RTTI Delegated Regulation outlines the requirement for road authorities, road operators, and real-time traffic information service providers to share road and traffic data, including updates and corresponding metadata, through national or common access points.[190]

The revised RTTI includes a number of changes that could increase data sharing and support the functioning of the EMDS, namely:

- **New Data Categories**
  Renaming and refining data categories (static data, dynamic road status data, traffic data) to better match data characteristics and requirements. Adding new categories such as infrastructure data (recharge/refuel points), regulations/restrictions (weight/size limits), and real-time network usage (availability of refuelling points).
- **Extended Geographical Scope**
  Expanding coverage to the entire road network (excluding private roads), with a gradual approach.
- **Greater Data Reuse**
  Strengthening provisions for reusing specific data types e.g. enhanced reuse of in-vehicle generated data by allowing public authorities to request sharing under FRAND conditions. This data access extends beyond real-time traffic information and is illustrative of the spirit of broader cooperation between partners in the public-private chain in the revised RTTI.

The additions noted above aim to improve the accessibility, exchange, re-use and update of data required to provide high quality and continuous real-time traffic information services. It is crucial to understand that the revised RTTI Delegated Regulation does not mandate the collection of new data or digitalisation. Sharing data is only obligatory when it is in a machine-readable format.

During the TN-ITS webinar[191] and NAPCORE workshop,[192] a business manager at the National Road Traffic Data Portal in the Netherlands emphasised several key takeaways, particularly the following needs:

- a quality framework between private service providers and road authorities that emphasises the stronger public-private collaboration within the sector;
- feedback loops, involving end-user input, to enhance data quality;
- low latencies for provisions/updating for the reliable and effective use of the data (including agreement between road authorities and private service providers on the definition of timely data will need to be further considered), given the emphasis on timeframe.

The revised RTTI assigns responsibilities to both road authorities and service providers. These responsibilities include data sharing and the integration of accessible traffic plans. Public authorities

[190] For a useful summary guide, see CROW (2022), "Real Time Traffic Information. A clarification of the new RTTI Delegated Regulation for road operators", https://www.crow.nl/downloads/pdf/verkeer-en-vervoer/verkeersmanagement/d397_real-time-traffic-information_en.aspx.
[191] TN-ITS (2022), "Unveiling the Latest RTTI Delegated Regulation Updates", https://tn-its.eu/unveiling-the-latest-rtti-delegated-regulation-updates/#:~:text=In%202022%2C%20the%20Real-Time%20Traffic%20Information%20%28RTTI%29%20Delegated,of%20high-quality%20and%20continuous%20real-time%20traffic%20information%20services.
[192] NAPCORE (2023), "FOLLOW UP of the workshop on the implementation of the revised RTTI DR", https://napcore.eu/video-of-the-workshop-on-the-implementation-of-the-revised-rtti-dr.

bear significant data provision duties, with deadlines as early as January 2025. Service providers, on the other hand, must adhere to multiple requirements. Many of these requirements call for a collaborative effort between the public and private sectors. NAPCORE has taken proactive steps by establishing an RTTI implementation action plan. This plan actively promotes private-public cooperation by bringing together road authorities and private service providers. Their approach places a particular emphasis on use cases and examines the varying levels of collaboration required between them.[193] The EMDS should engage and follow these RTTI implementation activities organised by NAPCORE and adopt a similar collaborative approach to future work.

The **MMTIS** Delegated Regulation is also subject to revision. With an updated proposal shared for feedback in May 2023, the consultation closed on 28 June 2023.[194] The basic principles of the Regulation, including the requirement that data be provided to the NAP only when digitalised and exchanged based on licence agreements, remain the same. However, some changes should be highlighted:[195] There is a new data category of historic/observed data, and an obligation to share dynamic data and new data sets. The MMTIS sets forth essential requirements to guarantee accessibility, interchangeability, and regular updating of standardised travel and traffic information, facilitating the provision of comprehensive multimodal travel information services across the European Union.[196] Therefore, the revision should be closely monitored, and its application to the EMDS should be considered, especially as it falls within the scope of the upcoming deployment project under DIGITAL.

In addition to the ITS Directive, there are a number of other pieces of mobility legislation that cut across modes, such as the **Trans-European Transport Network Regulation**,[197] **eFTI Regulation**,[198] and **Combined Transport Directive**.[199] The eFTI Regulation establishes a legal framework for road, rail, maritime and air transport operations to share data with enforcement authorities.[200] The Regulation is currently in the implementation process with the adoption of delegated and implementing acts.[201] Logistics is a diverse multi-stakeholder industry that by its very nature requires data sharing.[202] The success of the eFTI systems depends on engagement and collaboration with stakeholders.[203] During

[193] For further information on the previous workshops, see ibid.
[194] European Commission (2023), "EU-wide multimodal travel – new specifications for information services", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12912-EU-wide-multimodal-travel-new-specifications-for-information-services_en.
[195] Degen, A. (2023), "The bigger picture – Latest news from the EU regarding MMTIS and MDMS", https://kollektivtrafikk.no/app/uploads/2023/03/2023-03-23_EU-data-and-ticketing-initiatives_UITP.pdf.
[196] Antoniola, M. (2023), "The Future of Mobility Data Spaces. The role of local governments", Network Industries Quarterly, 25(2), https://cadmus.eui.eu/bitstream/handle/1814/75776/NIQ-Vol-25-Issue-2-june-2023.pdf?sequence=1.
[197] Regulation (EU) No 1315/2013 of 11 December 2013 on union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU Text with EEA relevance.
[198] Regulation (EU) 2020/1056 of 15 July 2020 on electronic freight transport information (text with EEA relevance), PE/27/2020/INIT.
[199] Council Directive 92/106/EEC of 7 December 1992 on the establishment of common rules for certain types of combined transport of goods between Member States.
[200] European Commission (2018), "Commission Staff Working Document. Executive Summary of the Impact Assessment", SWD 184 final.
[201] For an overview of the timeline, see TRAN Committee Meeting, EU Regulation (No) 2020/1056 on electronic freight transport information (eFTI), 2023, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/TRAN/DV/2023/03-01/DelegatedActsinRegulation20201056_EN.pdf.
[202] For more information on the logistics sector, see Bastiaansen, H. J. M., Nieuwenhuis, C. H. M., Zomer, G., Piest, J. P. S., van Sinderen, M., Dalmolen, S., and Hofman, W. J. (2020), "The logistics data sharing infrastructure: whitepaper", August 2020. TKI Dinalog, https://www.researchgate.net/publication/344068649_The_Logistics_Data_Sharing_Infrastructure.
[203] For more information on the Electronic Freight Transport Information (eFTI) System, see Hofman, W., Bouter, C., Burghoorn, M., Boertjes, E., Graaf, E., and d'Auria, A. (2022), "Towards a Mobility Data Space: Data sharing via linked semantic data, an example for eFTI", https://efti.gr/wp-content/uploads/2023/01/RA_Lisbon_2022_-

the interviews, an expert from the DTLF shared that they are currently researching the interface between the eFTI Regulation and the eIDAS 2.0 Regulation and that the potential of the eIDAS 2.0 Regulation with the Digital (Identity) Wallet could support the eFTI technical approach in the EU.

It is also important to mention the **MDMS** Regulation that is currently being prepared by DG MOVE.[204] Multimodal digital mobility services can be defined as "systems providing information about, inter alia, the location of transport facilities, schedules, availability and fares, of more than one transport provider, with or without facilities to make reservations, payments or issue tickets (e.g. route-planners, MaaS, online ticket vendors, ticket intermediaries)".[205] The initiative aims to improve the integration and coordination of all types of transport services, from long-distance to urban mobility. It also aims to better understand the challenges and barriers to the development of digital multimodal mobility services, including planning, booking, payment and ticketing functionalities. These elements serve as fundamental components of MaaS.[206] These services, allow comparison of different travel options, both public and private, on a single platform. Currently, MaaS applications and, more specifically MDMS applications are deployed in a fragmented manner, which impacts the offers across Europe. The current challenges are related to collaboration between mobility operators and digital multimodal transportation services; intricate processes for obtaining licenses and distribution arrangements; absence of universal standards and interfaces.[207]

Within the automotive sector**, type-approval legislation** for vehicles outlines the conditions under which third parties can access information related to repair and maintenance.[208] In this regard, the EC has issued an Implementing Regulation that lays down uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles.[209]

The Commission is also currently working to address broader **access to in-vehicle data** and considering revisions to the type-approval legislation to complement access to data as proposed in the DA.[210] The findings from the impact assessment on access to vehicle data indicate that the rise of connected vehicles and electric vehicles necessitates a more specific approach to ensure fair competition, innovation, and meet environmental goals.[211] Therefore, the initiative aims to address the limited and

_mobility_data_space_linked_data_and_eFTI_TNO_contribution.pdf and Chountalas, P., Dasaklis, T.K., Giannakis, K. D., Kopanaki, E., Rachaniotis, N.P., Voutsinas, T. G. (2023), "Electronic Freight Transport Information (eFTI): White Paper", https://efti.gr/wp-content/uploads/2023/03/eFTI-White-Paper_en.pdf.

[204] Antoniola, M., (2023), "The Future of Mobility Data Spaces. The role of local governments", Network Industries Quarterly, 25(2), https://cadmus.eui.eu/bitstream/handle/1814/75776/NIQ-Vol-25-Issue-2-june-2023.pdf?sequence=1.

[205] European Commission, "Multimodal digital mobility services", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13133-Multimodal-digital-mobility-services_en.

[206] Antoniola, M. (2023), "The Future of Mobility Data Spaces. The role of local governments", Network Industries Quarterly, 25(2), https://cadmus.eui.eu/bitstream/handle/1814/75776/NIQ-Vol-25-Issue-2-june-2023.pdf?sequence=1.

[207] European Commission (n.d.), "Multimodal digital mobility services", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13133-Multimodal-digital-mobility-services_en.

[208] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166.

[209] Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving systems (ADS) of fully automated vehicles.

[210] For more information on the public consultation see European Commission (2022, March 30), "Commission seeks views on possible measures on access to in-vehicle data", https://single-market-economy.ec.europa.eu/news/commission-seeks-views-possible-measures-access-vehicle-data-2022-03-30_en.

[211] European Commission (n.d.), "Access to vehicle data, functions and resources", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en.

non-standardised access to vehicle data, functions, and resources. While the DA addresses data access rights, it may not provide sufficient detail on access to functions and resources, specifically differences in data availability between vehicle brands.

The importance of cybersecurity, safety and fair competition in mobility, as remarked earlier, may also demand sector-specific measures.[212] This has sparked much discussion particularly in the automotive sector.[213] Consumers are also interested and engaged in this discussion. Consumer protection associations such as the Bureau Européen des Unions de Consommateurs, expressed their wish for sector-specific legislation on access to in-vehicle data back in 2021.[214] However, it is important to note that there are various tensions at play. Consumers want greater data transparency, specifically knowledge on what data is being generated, stored and shared by their vehicle. Data sovereignty is also crucial: consumers want to be able to exercise freedom of choice, to easily disable data processing and sharing, and to determine who has access to said data. Ensuring data security throughout the life of the vehicle is also paramount to protecting consumer safety. It is important to strike a balance between these considerations, as well as the views of other stakeholders.

Similar to the patchwork of legal regimes relevant to data, EU mobility legislation is also complex. The mobility sector encompasses various modes of transport, each with its unique characteristics and governance models. These different transport modes often require distinct governance approaches due to their specific operational requirements and market dynamics. In addition, there is a significant interplay between the public and private sectors in transportation, with varying degrees of involvement and collaboration. The history of liberalisation in modes such as aviation and railways has shaped the governance landscape, introducing market-oriented policies while balancing public service obligations. Multiple governance authorities, especially prominent in the European Union, further complicate the governance framework, as decisions and regulations are made at different levels, including supranational, national, and local. This structure of multiple governance authorities also impacts the distinction between public services obligations and market regulations, creating a complex regulatory environment. Furthermore, distinctions must be made between long-distance and urban transport, given the substantial differences in the governance models and challenges within these two contexts.

5.4. Recommendations

Conclusions

This chapter explored the legal perspective of the EMDS and its connection to governance. It stressed the importance of considering legal aspects in the development and functioning of data spaces, with a focus on how horizontal legal frameworks might apply to the EMDS and the identification of relevant mobility specific legislation. It highlights the complexity of the applicable legal framework, together with the recognition that common European data spaces are still an emerging concept and that in some cases the legislative review process is still ongoing. Finally, the chapter outlined the role of the DSSC in providing more clarity by defining generic building blocks and developing tools to support legal interoperability and contractual aspects.

---

[212] Ibid.

[213] DIGITALEUROPE (2021), "DIGTALEUROPE Access to In-Vehicle Data Position Paper", https://cdn.digitaleurope.org/uploads/2023/08/DIGITALEUROPE-Access-to-Vehicle-Data-Position-Paper_10.08.2023-FINAL_V4.4.pdf.

[214] BEUC (2021), "Urgent need for a legislative proposal on access to in-vehicle data and functions", https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-062_beuc_and_fia_joint_letter_on_urgent_need_for_a_legislative_proposal_on_access_to_in-vehicle_data_and_functions.pdf.

Recommendations

Set privacy and data protection as a priority in the EMDS

It is imperative to prioritise privacy and data protection as fundamental pillars of the EMDS. This is especially true of principles of purpose limitation and data minimisation. In this way, the EMDS fosters trust, ensures legal compliance and upholds the EU values, while improving data quality and user empowerment. Integrating these measures into the EMDS governance framework encourages responsible data sharing practices and will help the EMDS to gain public support.

Respect intellectual property rights and trade secrets

EMDS participants must respect intellectual property rights, particularly copyright and the *sui generis* database right, when sharing data. Participants should conduct comprehensive assessments of data's commercial value, secrecy, and protective measures before data sharing to consider the application of trade secret protection. The data space could implement access control mechanisms and confidentiality agreements to safeguard privately held data such as IP and trade secrets.

Consider competition law implications

EMDS participants should carefully consider competition law implications when sharing data, ensuring it serves legitimate purposes. The EMDS should stay informed about developments in competition law, especially in the context of data spaces and the mobility sector, by monitoring guidance provided by national competition authorities. It is also essential to analyse the relationship between these requirements and those laid down by the DMA. For example, if recognised gatekeepers express interest in joining the EMDS, a thorough legal analysis should be carried out to understand all implications and obligations this can entail to the data space governance.

Prioritise robust cyber resilience measures

The EMDS should prioritise robust cyber resilience measures, including verifiable credentials and digital identity, to enhance security and trust. It should also stay updated on cybersecurity legislation, especially NIS 2 and eIDAS revisions, and ensure full compliance to protect critical transport operations and maintain public confidence in data spaces like EMDS.

Assess the applicability of the Data Act (DA) to the EMDS

The proposed DA is poised to have a significant impact on data spaces like the EMDS. Given its ongoing legislative process, it is imperative to assess its applicability to the EMDS once the final text becomes available. Such an assessment ensures the EMDS remains in alignment with evolving legal requirements and can adapt its governance structure to accommodate new obligations introduced by the DA.

Monitor developments within mobility specific legislation

Given the ongoing legislative revisions and data-sharing initiatives within the mobility sector, a task force or working group within the EMDS should closely monitor developments within mobility specific legislation, such as the implementation of the revised RTTI Delegated Regulation and revision of the MMTIS Delegated Regulations. The EMDS should consider the practical application of these developments to specific sub-sectors within the mobility sector through use cases to ensure adaptability and alignment with evolving regulations.

Clarify the roles and responsibilities for participants in the EMDS

In the development and governance of the EMDS it is crucial to underscore the significance of incorporating legal definitions and delineating roles and responsibilities for participants. The DGA and the DA Proposal introduce specific legal definitions pertinent to data sharing. Terms like "data holder,"

"data user," and "data intermediation service" are defined within these legislations. The integration of these legally recognised definitions into the EMDS governance framework ensures that participants are well-informed about their rights and responsibilities, fostering a consistent and legally sound operating environment.

Explore the potential of data intermediation service providers to act as neutral facilitators for data sharing

A focused exploration of the potential role that data intermediation service providers can play as neutral facilitators of data sharing is advisable. The DGA recognises the significance of data intermediaries as trust-building entities in the data space. Knowledge sharing and cooperation between common European data spaces can ensure a consistent and harmonised approach to the use of data intermediaries across different sectors. The EMDS should closely follow research in this area and could contribute by examining data intermediaries operating in the mobility sector. For example, on the basis of the inventory, the EMDS could organise workshops on this topic, involving relevant stakeholders in the discussions. It is recommended that the DSSC develops clear and comprehensive guidance documents that outline the legal requirements, rights, and responsibilities of data intermediaries, data space operators, and participants within the data space. These guidelines should then be adapted to address specific EMDS needs and concerns.

Bridge the gap between legal and technical aspects

The EMDS should establish cross-disciplinary working groups to bridge the gap between legal and technical aspects of the EMDS and ensure interoperability at all levels. Develop standardised protocols and frameworks that align legal obligations with technical capabilities to ensure that data governance solutions are legally compliant by design.

Promote dialogue between other preparatory actions and initiatives to inform the EMDS

The EMDS should establish a formal process, possibly through the DSSC, to review and leverage the results and lessons learned from other preparatory actions and initiatives to inform the EMDS. Actions should promote the alignment and active exchange of best practices and compare sector specificities in order to effectively address upcoming horizontal legislation related to data governance, in particular with relevant sectors such as Smart Cities, Green Deal and Tourism.

5.5. Building blocks

Figure 19 shows the individual building blocks recommended for the legal aspects of the EMDS.

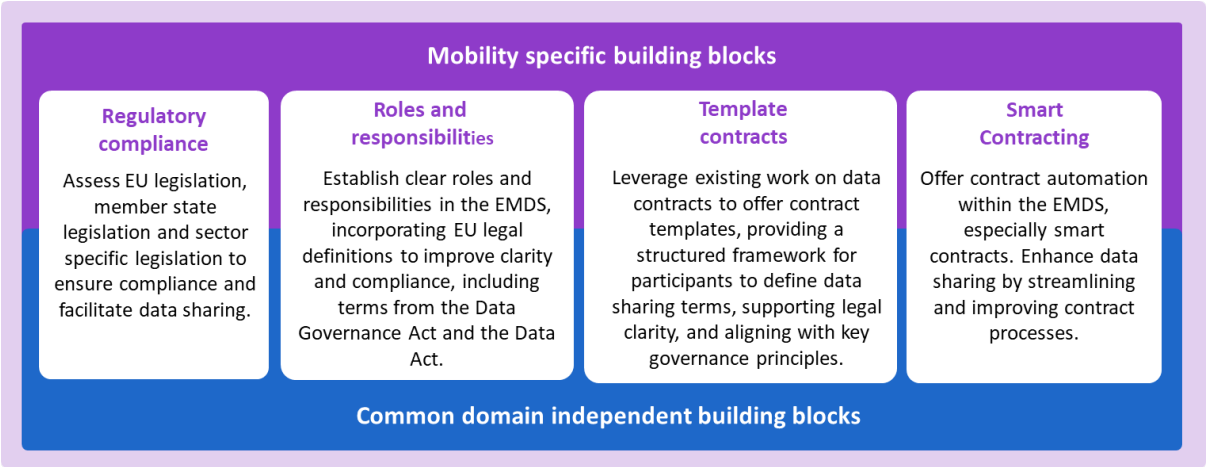


Figure 19: Building blocks covering the legal aspects of the EMDS.

IV. Technical building blocks

The work on the common building blocks for the EMDS is conducted from the perspective that the EU initiatives on developing and deploying the common European data spaces will define an aligned (organisational and technical) basis for developing interoperable sectoral data spaces.

The technical grounding for embedding sectoral data spaces within the overarching common European data spaces is expected to be developed within the upcoming DSSC blueprint initiative and the SIMPL procurement initiative. It refers to foundational technical developments required for smooth interoperability, functionality, and integration of sector-specific data spaces into the larger European data landscape. The technical grounding is addressed in Chapter 6.

The subsequent chapters in this part analyse the specificities of the EMDS building blocks, building upon and within the context of the expected development of the common European data spaces environment.

Chapters 7, 8, and 9 address the three pillars of the “Technical building blocks” from the DSSC taxonomy, i.e. “Data interoperability”, “Data sovereignty and trust” and “Data value creation”, respectively.

6. Technical grounding

6.1. Introduction

This chapter addresses the technical grounding for common building blocks. The DSSC blueprint is currently in development, however, this chapter provides a preliminary account of the current expectations regarding the potential development of the technical grounding which will serve as a basis for addressing the sectoral specificities of building blocks for the EMDS.

The DSSC technical grounding is part of the DSSC taxonomy of building blocks (Figure 2). It stems from the preparatory and ongoing work on reference architectures for federated data sharing that has evolved over the last years. Key contributions to this evolution include the IDSA Reference Architecture Model[215], the Gaia-X Federation Services[216], the iSHARE components[217], the DSBA Technical Convergence document[218], the DSSC blueprint (under development), and the preparatory works in the context of the SIMPL procurement initiative[219].

Based on the ongoing results of these initiatives, Section 6.2 addresses the importance for the EMDS to adhere (where possible) to the blueprint that is being developed by the DSSC to enable interoperability between data spaces, especially in terms of data sovereignty, trust, and discoverability capabilities.

The following sections in this chapter address the technical grounding for data spaces, specifically software and services implementations for data spaces, as identified in the DSSC taxonomy (Figure 2):

- Data space registries (Section 6.3);
- federated services (Section 6.4);
- data space connectors (Section 6.5).

The final Section 6.6 provides the conclusion, recommendations and building blocks for the technical grounding.

6.2. A common blueprint on data sovereignty, trust and discoverability

Mobility and logistics are cross-border and cross-sector by nature. Therefore, mobility data spaces need to be interoperable, both between various mobility and logistics data space initiatives and with other sectoral data space initiatives. As described in Chapter 4, **interoperability and federation of data spaces** extend the reach and scope of data accessibility enabling the development of new business models and services across sectors and regions. Consequently, managing an ecosystem of sovereign actors and data spaces poses a key challenge for the EMDS. Data space interoperability will allow data space participants to access the resources of the interconnected data spaces when connected to a single data space, eliminating the need of subscribing to multiple data spaces. This fosters the development of new cross sector use cases and business models.

---

[215] International Data Spaces Association (2022), "International Data Spaces: Reference Architecture Model Version 4", GitHub: https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0.
[216] Gaia-X Federation Services (n.d.), "Specifications", https://www.gxfs.eu/specifications.
[217] iSHARE Foundation (n.d.), "iSHARE – Trust Framework for Data Spaces", https://ishare.eu.
[218] Data Space Business Alliance (2023), "Technical Convergence. Discussion Document", Version 2.0, https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.
[219] European Commission (2022), "SIMPL: Preparatory work in view of the procurement of an open source cloud-to-edge middleware platform - Architecture Vision Document", Version 4.0, https://ec.europa.eu/newsroom/dae/redirection/document/86241.

With the goal of embedding the EMDS into the overarching **EU ambition of creating common European data spaces**, the EMDS must build upon the technical grounding for interoperability within and across the EU's sectoral data spaces, as defined by the DSSC and the upcoming EU SIMPL initiative. It is crucial to align and harmonise the development and deployment of the EMDS with these overarching EU initiatives. This specifically applies to enhancing the capabilities related to:

- Data sovereignty and trust;
- discoverability.

Due to the key role these two capabilities play in data space interoperability, they are identified as separate technical building blocks in the DSSC taxonomy (Figure 2) and are further elaborated upon in Chapter 8 and Chapter 9, respectively.

The alignment and harmonisation of the EMDS with the development and deployment of these two key capabilities will be part of the multi-level governance approach discussed in Chapter 4.

6.3. Data space registries

Data space registries serve the purpose of appropriately registering the participants of a data space. However, in view of the role that data space registries may play in the context of the role models for intra and inter data space interoperability (as described in Chapter 4 and elaborated in Chapter 10), a distinction needs to be made between:

- **Registries for participants within a specific data space instance**
  These registries provide internal registration capabilities for a data space instance. Although mainly used for intra data space interoperability, they can also be implemented to federate or interconnect with internal registries of other data spaces. Refer to Section 6.4 for details on the federation of building blocks across data space instances.
- **Registries for data space instances**
  In a federation comprising multiple data space instances, a registry for the capabilities of these data spaces may also be required. The registry of data space instances can also include references to each of their associated registries to improve visibility for data space participants.

The DSBA architecture[220] and the iSHARE architecture offer an additional type of registry: internal registries for participants that contain information about **policy delegation rights** to other organisations or users. These registries are not accessible to external users but are necessary for evaluating authorisation polices (access rights) to organisations, users, or machines. The relevance of policy registries with the capability to delegate rights is particularly relevant for the trust architecture in the mobility sector (especially logistics) and is further addressed in Section 8.3.

In addition, data space registries will further be addressed in Chapter 9, with a specific focus on catalogue functions, discoverability, and metadata brokering of IT resources in data spaces, as well as on data services, applications, and data models and mappings.

6.4. Federated services

The environment of federated data sharing and data spaces is still evolving (Section 1.2). Their building blocks will be defined and specified as part of the DSSC blueprint and will be developed as open source under the EU SIMPL procurement initiative. They are expected to be deployed by numerous sectoral data spaces, including the EMDS deployment initiative. Currently, it is unclear whether the process of

[220] Ibid.

development and deployment will be governed by the EDIB, and whether its role will extend beyond advisory functions.

Neither the DSSC blueprint nor the building blocks to be introduced by the SIMPL project have been fully specified. It is reasonable to expect that the DSSC blueprint and the SIMPL project will build upon **ongoing technical developments** for the interoperability of data spaces, as addressed by reference architectures such as the IDSA Reference Architecture Model, the Gaia-X Federation Services, the iSHARE components and the DSBA Technical Convergence document.

The DSSC blueprint and the building blocks of SIMPL are key in establishing the foundation for interoperability and federation of data spaces. This importance has also been addressed in Chapter 4, highlighting the significance of managing an ecosystem of sovereign data spaces and its associated multi-level governance model.

The following paragraphs address the expected direction of architectural development.

Developments in data space architectures

Two main aspects regarding the expected direction of architectural development for federated data sharing and data spaces are (1) decentralisation and federation of data spaces and (2) separation between the control plane and data plane for the data space connectors.

Decentralisation and federation: the Dataspace Protocol

Decentralisation and federation form the basis of the developmental direction for the future environment of federated data sharing and data spaces. Key European initiatives focused on federated data sharing and data spaces (IDSA, Gaia-X, etc.) are indeed evolving towards becoming fully decentralised architectures, allowing the various data space building capabilities to be implemented in a highly decentralised manner. This decentralised approach involves the use of **data space connectors** (Section 6.5), which can be deployed closer to the "edges" of the infrastructure, in **proximity to the actual data sources.** For example, they may be integrated within IT infrastructures of individual participating organisations or even within systems and devices such as cities' IoT systems or traffic sensors. In such a highly decentralised infrastructure, it is essential that the data space connectors are interconnected in a federated manner.

An architectural approach based on data sharing between autonomous entities (participants, data space connectors) requires **extensive exchange of metadata between the data space connectors through a well-defined protocol**. The emerging Dataspace Protocol[225] defines how this metadata is provisioned. It comprises a set of specifications designed to facilitate interoperable data sharing between entities governed by usage control and based on web technologies. These specifications define the schemas and protocols required for entities to publish data, negotiate usage agreements and exchange data as part of a federated data sharing architecture or data space (Figure 20).

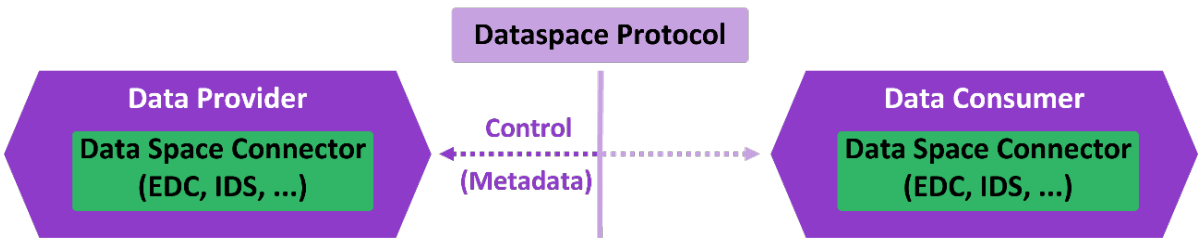


Figure 20: The Dataspace Protocol defining the control interface.

The Dataspace Protocol defines how data assets are deployed (as DCAT catalogues), how usage control policies are expressed (as ODRL policies), and how contract agreements that govern data usage

are syntactically expressed and electronically negotiated. The Dataspace Protocol specification does not cover the data transfer process itself. Instead, data transfer is controlled by the Transfer Process Protocol, while the data transfer itself (and especially the handling of technical exceptions) falls under the responsibility of the transport protocol employed.

This separation aligns with the basic design assumption that the **control plane** (involving metadata exchange to enable data sharing) and the **data plane** (with the actual transfer of the (potentially sensitive) primary data) will be separated. Further details on this separation are addressed below.

Separation between control plane and data plane

From the outset, IDSA has adopted an architectural approach for the IDS connector in which the exchange of control information (metadata) is integrated into the data sharing protocol that also contains the primary data to be transferred. This approach is referred to as in-band control. In-band control within the IDS connector, as well as its associated IDS protocol and the IDS Communication Protocol (IDSCP), is depicted in Figure 21.

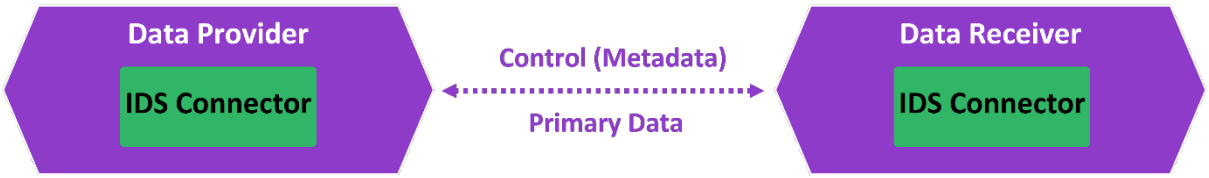


Figure 21: The IDS-connector with in-band control through the IDSCP protocol.

Currently, an architectural approach is being developed and rapidly adopted based on the separation of the control plane and data plane. This separation, illustrated in Figure 22, is also referred to as out-band control for federated data sharing. The out-band control mechanism is currently adopted by several of the main EU data space initiatives using the EDC, such as MDS, Catena-X and EONA-X.

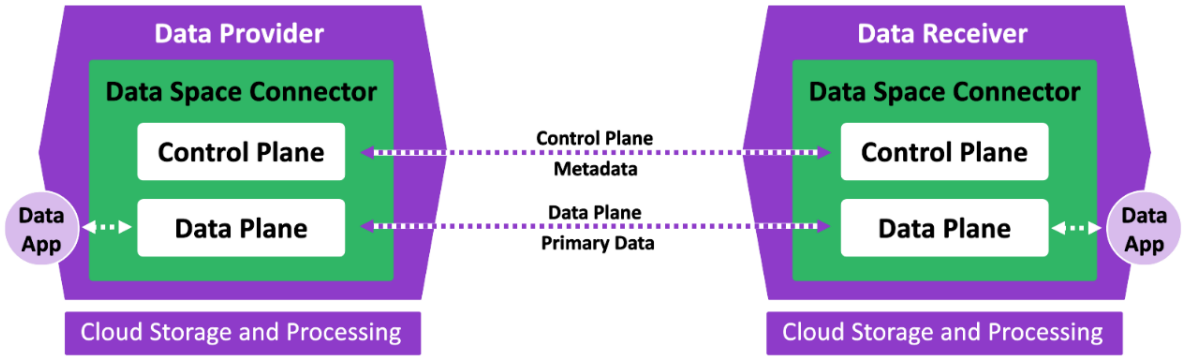


Figure 22: Out-band control for federated data sharing: separating the control and data plane.

The **control plane** handles the discovery of the Information Communications Technology (ICT) assets offered by connectors and their associated policies as well as contract negotiations. To achieve this, the control plane exchanges metadata with the control plane of other data space connectors.

The **data plane** handles the actual transfer of the shared data with the data plane of other data space connectors. This is referred to as the primary data, which may contain sensitive information.

There are several advantages of using an out-band control mechanism with separation of the control plane and the data plane (Figure 22) compared to an in-band control mechanism (Figure 21):

- It offers more flexibility in allowing multiple connectivity protocols at the data plane. These can be enabled simultaneously, for example to support multiple types of data sharing such as

data streaming, and to serve different connectivity needs within a single data space, even when control metadata exchange differs from the primary data transfer.

- It allows for a flexible and gradual evolution trajectory in which control and data plane protocols are added when there is a demand for them. Not all control and data plane options need to be supported from the start but may be added as needed.

The separation of the control plane and the data plane may, on the one hand, lead to new interoperability challenges as it allows for differentiation or variation in the choices for (connectivity) protocols to be supported at the data plane. On the other hand, it is expected that only a limited set of (connectivity) protocols at the data plane will be needed and adopted to serve the majority of the connectivity requirements to support the various types of data sharing. These may include the HTTP, MQTT, Kafka and (Amazon) S3 protocols.

Approaches for harmonisation of data spaces

Interoperability between data spaces is a key aspect of the EU Data Strategy and the EU's ambition to create common European data spaces. The Data Sharing Coalition addresses interoperability between multiple data spaces through its Data Sharing Canvas[221]. It introduces the concept of "harmonisation", defined as "the establishment of agreements, standards, and requirements between participants to enable data sharing".

According to the Data Sharing Canvas, interoperability between multiple data spaces can be achieved via full or partial harmonisation. In case of full harmonisation, individual data spaces adhere to the same harmonised requirements and principles. **Full harmonisation between data spaces offers major advantages** for inter data space interoperability, both in terms of functionally and for greater ease and efficiency.

Nevertheless, achieving full harmonisation between data spaces is often not feasible in practice and might even be unattainable for all newly formed data spaces. For existing data spaces, opting for full harmonisation with other data spaces can have a significant impact in terms of alignment and migration efforts and costs. The Data Sharing Canvas therefore introduces **partial harmonisation** through a new component, the "**data space proxy"**, that absorbs the complexity of harmonisation of data spaces. Proxies allow data consumers and providers within a data space to simply connect to other data spaces via their proxy. Proxies have the main functionality of translating data space specific transactions to their harmonised equivalents, thereby facilitating interoperable transactions and creating an understanding of concepts such as trust and security across data spaces. The definition of the harmonised equivalents and the transformation to these equivalents can be a complex exercise, as described in a Use Case Implementation Guide by the Data Sharing Coalition[222].

The concepts of full and partial harmonisation are illustrated in Figure 23. Both full and partial harmonisation are applicable to each of the **four interoperability levels** of the European Interoperability Framework: technical interoperability, semantic interoperability, organisational interoperability, and legal interoperability under an overarching integrated governance approach[223].

[221] Data Sharing Coalition (2021), "Data Sharing Canvas. A stepping stone towards cross-domain data sharing at scale", https://datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf.
[222] Data Sharing Coalition (2022), "Use Case Implementation Guide", https://datasharingcoalition.eu/app/uploads/2022/03/data-sharing-coalition-use-case-implementation-guide-ucig.pdf.
[223] European Union (2017), "New European Interoperability Framework (EIF). Promoting seamless services and data flows for European public administrations", https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

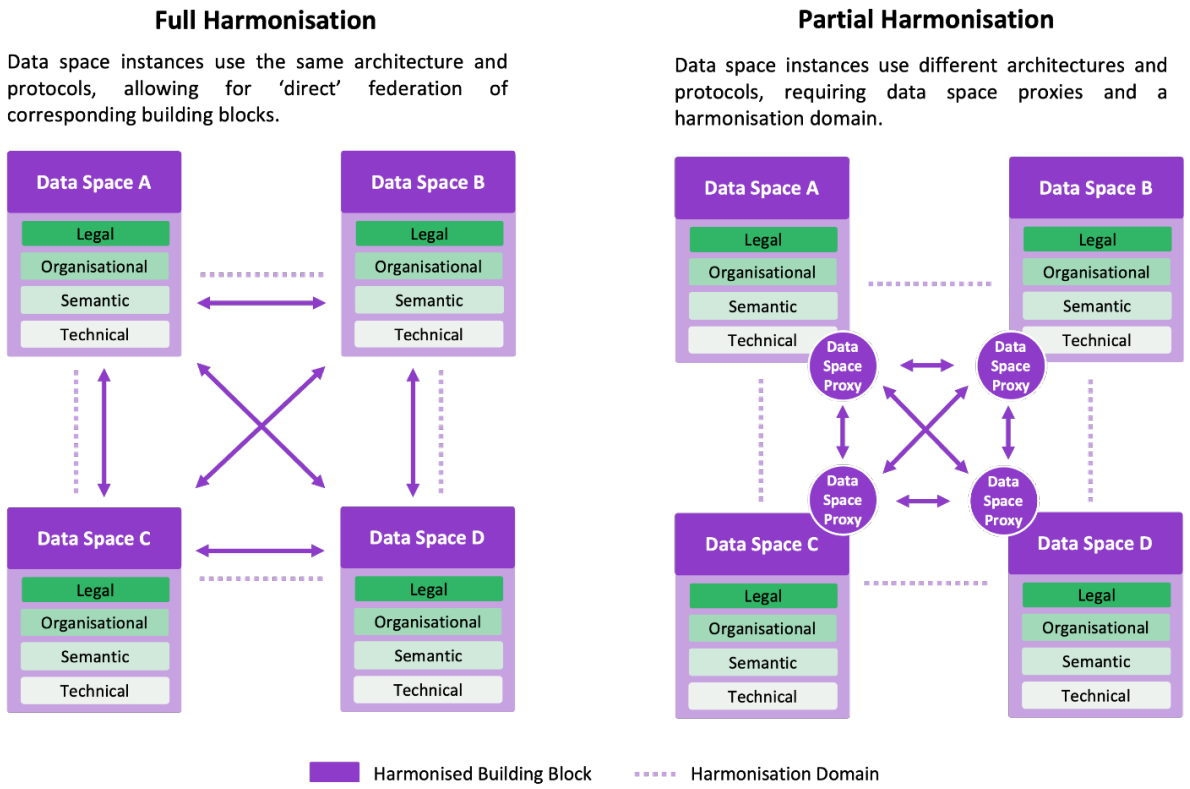


Figure 23: Full (l) and partial (r) harmonisation for inter data space interoperability.

Full harmonisation: federated building blocks and the Dataspace Protocol

According to the Data Sharing Canvas[221], full harmonisation between data sharing domains exists when the domains use or follow a shared cross-domain design, i.e. following the same technical protocols and speaking the same language.

Full harmonisation has implications for the interactions between associated instances of a building block in the various data spaces. These various instances of a building block in different data spaces must interact in a way that they jointly act as **a seemingly single instance** towards their users. The building blocks capable of acting as a single instance are referred to as "federated building blocks". Federation can be applied to various capabilities in the data space architecture.

Various interaction scenarios for federation between building blocks can be distinguished as follows[224]:

- **Building block initiated federation** further distinguished between federation at publish-time and federation at query-time;
- **Connector initiated federation** further distinguished between service consumer-initiated federation and service provider initiated federation.

The emerging Dataspace Protocol[225] has a specific role to fulfil in the creation of federated building blocks. Sharing data between autonomous entities (participants, data space connectors) requires the provision of metadata to facilitate the transfer of assets by making use of a data transfer protocol. The

[224] The Netherlands AI Coalition Working Group Data Sharing (2022), "Reference guide for inter AI data space interoperability", https://nlaic.com/wp-content/uploads/2023/04/NL-AIC-inter-AI-Data-Space-Interoperability-v3.2.pdf.
[225] International Data Spaces Association (2023), "Dataspace Protocol", Version 0.8, https://github.com/International-Data-Spaces-Association/ids-specification/tree/main.

Dataspace Protocol defines how this metadata is provisioned. It defines the interoperability specifications for data space connectors to publish data, negotiate usage agreements and access data.

Partial harmonisation: data space proxies

The second mode of harmonisation between data spaces is partial harmonisation, which includes the use of proxies absorbing the complexity of the endeavour. It allows data consumers and providers to simply connect to other data spaces via their proxy. The main functionality of **data space proxies** (as introduced at the beginning of this section) is to translate data space specific transactions into their harmonised equivalents:

- Proxies **translate data space specific language** into a harmonised language in the Harmonisation Domain to enable multilateral end-to-end interoperability;
- Proxies facilitate trust across data spaces by conforming to the rules and agreements of the Trust Framework;
- Proxies enable the discovery of data providers across data spaces.

The proxies implemented by all data spaces form a network, known as the Harmonisation Domain, which enables each data space to share data effortlessly with other data spaces[226]. The eIDAS nodes, formerly known as the "Pan European Proxy Server" (PEPS) are an implementation of proxies used to enable interoperability of digital identities across EU Member States that could become relevant for personal cross-border mobility services[226].

6.5. Data space connectors

Data space connectors are important components for implementing a data space with all its features, capabilities and building blocks. They serve as the interconnection between an organisation or system and a data space.

The following paragraphs address the functionalities of a data space connector and the EDC as state-of-the-art. It is important to note that other data space connectors are also under active development, as described in the DSBA Technical Convergence document.

Functionalities of a data space connector

To provide the interconnection between an organisation or system and a data space, the main functionalities and roles of a data space connector should include (Figure 24)[227]:

- Providing knowledge about the ICT assets a company or organisation wants to share and the associated usage policies;
- Handling contract negotiations and storing contract agreements;
- Facilitating the transfer of data;
- Offering an API to the internal IT backend of a connected organisation (which may be connector-specific and implemented by means of a "data app");
- Communicating to the data space using well defined protocols.

[226] Data Sharing Coalition (2021), "Data Sharing Canvas. A stepping stone towards cross-domain data sharing at scale", https://datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf.
[227] See, for example, International Data Spaces Association (2022), "Data Connector Report", https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/International-Data-Spaces-Data-Connector-Report-November-2022.pdf and NTT DATA (2022), "Dataspace Connector Survey Report - Overview of IDS-RAM and Eclipse Dataspace Connector", https://www.nttdata.com/global/en/-/media/nttdataglobal/1_files/technology/dataspaceconnectorsurvery_sep2022.pdf.

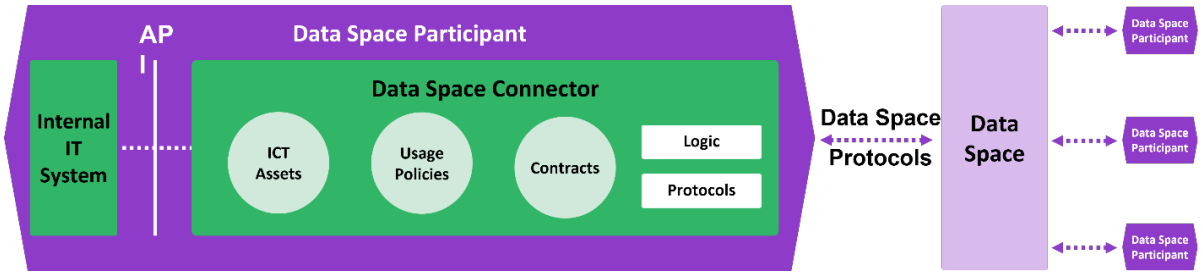


Figure 24: Data space connector: high-level functionality.

A **data space connector serves as secure gateway** for systems and organisations to a data space. As depicted in Figure 2, its functions relate to and overlap with all technical building blocks in the DSSC taxonomy. Specifically, it needs to implement capabilities to support the technical building blocks within each of the three categories: “Data interoperability”, “Data sovereignty and trust” and “Data value creation”.

The Eclipse Data Space Components (EDC)

Currently, the EDC connector receives significant attention for implementing the data space connector following the separation of the control plane and the data plane, as well as for enabling the Dataspace Protocol for interoperability.

However, it is important to note that the EDC is more a software framework for developing data space connectors rather than specifying the architecture and protocols of the data space connector itself. Consequently, the EDC allows for several design choices to be made at the protocol and data space connector level. This implies that adopting the **EDC does not automatically guarantee interoperability** with other data spaces that adopt the EDC.

Nevertheless, the EDC enjoys support from major organisations and companies (such as Amadeus, BMW, Fraunhofer, Microsoft and T-Systems, among others). It is already used in several major European data space initiatives.

6.6. Recommendations

Conclusions

The DSSC blueprint is currently in development. While it is expected to follow the technical grounding described in this chapter, the specific protocols and implementation details have to be agreed upon and formalised.

Nevertheless, the next steps in developing the architecture and building blocks for the EMDS in a future proof manner should take into account:

- The architecture and building blocks for the generic infrastructure underlying the common European data space, developed by the DSSC and SIMPL initiatives;
- The inclusion of additional building blocks in the EMDS, especially to support the four types of data sharing described in Section 2.2 and the mobility and logistics specific building blocks as identified in the following chapters.

Recommendations

Align and harmonise the development and deployment of the EMDS with the overarching approach of the common European data spaces

Data sources in mobility and adjacent data space instances should be made mutually accessible, with data space interoperability being a key aspect in realising the ambition of the common European data spaces. Hence, to embed the EMDS into the overarching EU ambition of the common European data spaces, it needs to build upon the technical grounding for interoperability within and across the EU's sectoral data spaces as developed by the EU DSSC's blueprint initiative and the upcoming EU SIMPL procurement initiative. Alignment and harmonisation of the EMDS development and deployment approach is needed with these overarching EU initiatives, both with respect to the "organisational and business" building blocks and with the "technical" building blocks.

Develop Minimal Interoperability Mechanisms (MIMs) for the EMDS and across the EU sectoral data spaces for the building blocks on data sovereignty, trust and discoverability

Data sovereignty, trust and discoverability are key capabilities for making data space interoperable. These capabilities are broadly defined and may have many implementation variants. Hence, concrete agreements and guidelines on how to design and implement them are required. One approach to achieve this is to define MIMs across mobility and other sectoral data spaces. MIMs are a practical set of capabilities built on open technical specifications that allow data spaces to replicate and scale solutions on a global scale. The Open & Agile Smart Cities[228] (OASC) manages MIMs with focus on mobility and smart cities. In collaboration with the DSSC, a similar approach may be considered for a cross-sectoral approach to address data sovereignty, trust, and discoverability capabilities.

Develop interconnection scenarios and tooling to stimulate adoption of the EMDS

The EMDS will need to be developed, deployed and embedded in the European mobility and data sharing landscape. To stimulate adoption of the EMDS by existing data sharing initiatives in the mobility sector, the barriers for interconnection should be made as low as possible. This can be enabled by defining both representative scenarios for interconnection and develop the supporting tooling. The EMDS deployment initiative should take the lead, e.g. for scenarios and tooling (data space connectors) for IDSA, FIWARE, Gaia-x or iSHARE based data sharing environments.

6.7. Building blocks

Figure 25 shows the individual building blocks recommended for the technical grounding of the EMDS.

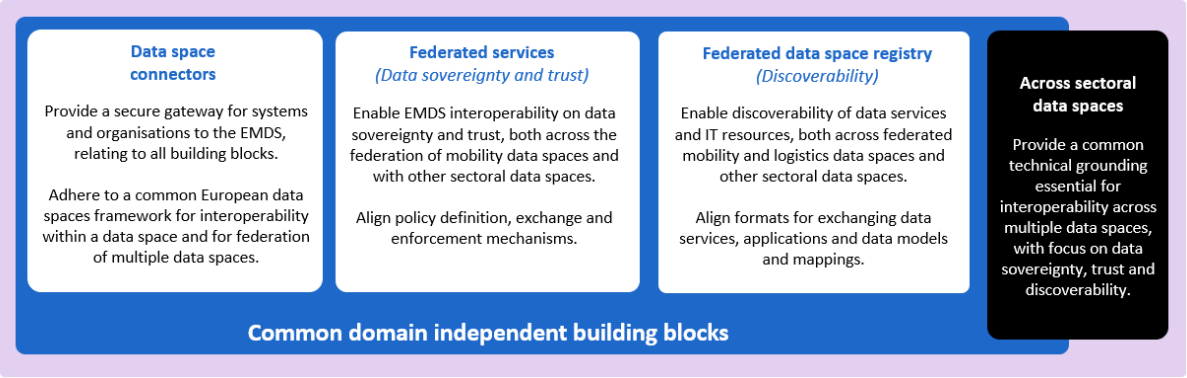


Figure 25: Building blocks for the technical grounding.

[228] Open & Agile Smart Cities (n.d.), "Welcome to Open & Agile Smart Cities, or OASC for short", https://oascities.org.

7. Data interoperability

7.1. Introduction

In a data space, participants need to be able to share and exchange data in a standardised way, both within a specific area (e.g. between different stakeholders in traffic management), as well as across domains (e.g. mobility and tourism to improve traffic management in touristic areas). As such, data interoperability is essential. It allows participants to maximise the value of their data and overcome the significant challenges posed by proprietary data assets (in company- or sector-specific formats). Data interoperability requires capabilities to enable semantic interoperability, which is the ability to exchange data with unambiguous, commonly agreed meaning between participants in a data space. In practice, this means enabling participants to specify their (both domain-specific and cross-domain) semantics, link them to (common) technical interfaces, and record which data was exchanged with whom.

Data interoperability is important for organisations as it enables data to be accessible across different formats and platforms. This capability allows organisations to make data-driven decisions, leading to reduced costs, increased operational efficiency and improved business cases. Achieving data interoperability allows an organisation to maximise value from its data and overcome the significant challenges posed by proprietary data assets. In a data space, participating organisations must share and exchange data in a standardised way. Data interoperability is essential for this purpose because it ensures that data can be utilised between different systems and applications. This means that participating organisations can use their own systems and applications to access and use data from other participants in the data space.

Section 7.2 in this chapter defines the scope and methodology of the interoperability analysis, followed by the findings of the analysis (Section 7.3), especially regarding the identified data models and data exchange standards in different mobility and logistics domains. Section 7.4 presents the main observations, followed by a conclusion, a comprehensive set of recommendations and the building blocks for data interoperability.

7.2. Scope

Functional Scope

To approach the topic of data interoperability within a data space, this chapter follows the DSSC and (and former OpenDEI) taxonomy, which is a functional description of a set of reusable and specifiable building blocks that can be used to develop a data space. According to the DSSC taxonomy, “[interoperability building blocks] should be deployed by all data providers and data consumers participating in a data space. This approach ensures that each data provider can be certain that any data published can be technically consumed by any data consumer entitled to do so, while each data consumer can be certain they are able to technically access and use any data made available by any data provider selected. The following building blocks belong to this category:

- **Data models and formats**
  This building block establishes a common format for data model specifications and representation of data in data exchange payloads. Combined with the “Data exchange” building block, this ensures full interoperability among participants.
- **Data exchange**
  This building block facilitates the sharing and exchange of data (i.e. data provision and data consumption/use) between data space participants. An example of a data interoperability building block providing a common data exchange API is the “Context Broker” of the CEF,

which is recommended by the European Commission for sharing right-time data among multiple organisations.

- **Data provenance and traceability**
  This building block provides the means to trace and track the process of data provision and data consumption/use. It forms the basis for a number of important functions, including identification of the lineage of data to audit proof logging of transactions. It also enables implementation of a wide range of tracking use cases at application level, such as tracking of products or material flows in a supply chain."[229]

The **functional scope** of this chapter is based on the "data interoperability" pillar of the DSSC taxonomy of building blocks.

This chapter covers "Data models and formats" and "Data exchange". "Provenance and traceability" has close ties to trust topics and is therefore analysed in Chapter 8 on data sovereignty and trust. The analysis focuses mostly on **domain-specific** building blocks, such as data models and formats, data exchange protocols and APIs, as well as on models for metadata that are used to describe these building blocks in a machine-readable way. Cross-data space interoperability between technical (and organisational) building blocks is not included here, as it is primarily addressed by the DSSC.

Thematic Scope

The mobility sector is categorised into 18 individual application domains that represent use case clusters. These thematic clusters are described in Table 3, Section 1.4.

7.3. Data models and data exchange

Table 13 presents the preliminary results of the collection of interoperability building blocks related to data models and Data exchange (APIs and protocols), which have been mapped to the individual thematic categories (i.e., the mobility domains), which have been defined in Table 3.

Table 13: Mapping the identified Interoperability building blocks to thematic categories.

Thematic Category (Mobility Domain)	Payload Data Models	Data Exchange API/Protocols
Public transport	• Transmodel (infrastructure) • NeTEx (timetables) • GTFS • SIRI (real-time) • OJP • NaPTan • TAP TSI (for rail) • OSDM	• SIRI • OJP • TRIAS • TOMP-API
Individual transport	• DATEX II • C-ITS (ETSI ITS)	• DATEX II • OJP • C-ROADS IP based interface

[229]EU Open DEI project (2021), "(2021), "Design Principles for Data Spaces. Position Paper", https://design-principles-for-data-spaces.org.

Thematic Category (Mobility Domain)	Payload Data Models	Data Exchange API/Protocols
Shared mobility	• MDS (mobility data specification) • GBFS • CDS (Curb Data Specification) • SIRI • NeTEx	• GBFS • TOMP-API • SIRI
Electric vehicles and charging	• DATEX (for parking and energy) • APDS • Transmodel	• OCPP (Open Charge Point Protocol) • OCPI (Open Charge Point Interface) • ISO 15118 (vehicle-to-grid communication) • ITxPT • TOMP-API
Multimodal mobility in smart cities including smart parking	• OGC CityGML • ETSI NGSI-LD with Smart Data Models • CityJSON • ISO 37120 • MIMs • ISO/IEC 30145 (Information technology - Smart City ICT reference framework) • ISO standard ISO/IEC 30182:2017 (Smart city concept model) • APDS • DATEX II (parking) • Transmodel • DIN SPEC 91367 (Urban mobility data collection for real-time applications) • DIN SPEC 91607 (Digital Twin for cities and communities) • In progress: DIN SPEC 91377 (Data models and protocols in open urban platforms)	• MQTT • CDS (curb data specification) • MDS • DIN SPEC 91394 (Digitalisation of parking processes – Data interfaces) • OJP
On-demand mobility	• TOMP API	• TOMP API
MaaS	• TOMP API • GTFS • GBFS • Transmodel	• TOMP API • GTFS • GBFS • OJP

Thematic Category (Mobility Domain)	Payload Data Models	Data Exchange API/Protocols
Vehicle data	Subcategory vehicle and sensor data: • SENSORIS, • ExVe (Extended Vehicle) • SAREF4AUTO • ETSI NGSI-LD with Smart Data Models Subcategory automated driving, simulation: • ASAM OpenDRIVE, • OpenSCENARIO, • OpenODD Subcategory testing and diagnostics: • ODX • OTX	
CCAM	• C-ITS/ C-Roads profiles • SENSORIS • ExVe • DATEX II • SAREF4AUTO	• ITS-G5 (short range) • C-ROADS IP based Interface • AMQP • DATEX II (REST/SOAP)
Road transport	• DATEX II • IDF • OpenStreetMap Data Model • Lanelet2 • INSPIRE • ETSI NGSI-LD with Smart Data Models	• DATEX II • INSPIRE
Road operator information: static and dynamic	• DATEX II • TN-ITS • HERE • OSI prime 2 • C-ITS • ETSI NGSI-LD with Smart Data Models	• DATEX II • C-Roads IP-based interface
Rail transport	• NeTEx (timetables) • SIRI (real-time) • RailML (railway applications) • TAF/TAP TSI	• SIRI (REST/SOAP) • RailML (railway applications) • OJP
Air transport	• IATA OneRecord	• IATA OneRecord
Inland waterway freight transport	• INSPIRE • RIS Standards • EuRIS	• TAF-TSI Technical Document B14 (railway freight) • TOMP-API (for ferries booking)

Thematic Category (Mobility Domain)	Payload Data Models	Data Exchange API/Protocols
		• EuRIS
Maritime freight transport	• Digital Container Shipping Association data model standards on bill of Lading etc. • UN/CEFACT MMT • IMO (International Maritime Organisation)	• Track & Trace 2.2(/1.2)
Logistics	• FEDeRATED Semantic Model (DGMove DTLF) • OpenTripModel (OTM) • Port Communication System (Portbase) • BlauweGolfVerbindend (open bridges and harbouring information) • DIUM (Uniform Distance Table for International Freight Traffic)	• FEDeRATED APIs for Event Driven Data Exchange/Flow Control (DG MOVE/DTLF) • TAF-TSI (railway freight) • TAP-TSI • RailML (railway applications) • OTM (v5) • Portbase: multiple APIs • BlauweGolfVerbindend: (API available on request) • sFTP (within freight railway) • Peppol
Sustainable Urban Mobility Indicators (SUMI)	No building blocks identified. Under development.	
Geospatial data	• INSPIRE • GeoJSON • OGC Standards • ETSI NGSI-LD with Smart Data Models	

In addition, the following interoperability building blocks have been identified for describing and transmitting metadata, which includes information about resources such as data sets, APIs, protocols, and more:

- DCAT-AP
- DCAT-NAP-AP
- CMD (Coordinated Metadata Catalogue)
- mobilityDCAT-AP

Table 14 presents and describes the individual data interoperability building blocks that have been identified by the project. They are employed to support interoperability between stakeholders either on a European level, on a national level or within a specific stakeholder ecosystem:

Table 14: Description of the identified Interoperability building blocks.

Data Models	Description
Transmodel	Transmodel is a European standard for public transport information systems. It defines a common data model that covers various aspects of public transport, such as timetabling, fares, operations, real-time data and journey planning. It aims to facilitate interoperability and data exchange among different public transport systems and services. Transmodel covers both conventional and alternative modes of transport, such as bus, tram, metro, rail, taxi, vehicle sharing and pooling. Transmodel is based on an abstract model that is independent of any specific technology or implementation. Website: https://transmodel-cen.eu/
NeTEx	NeTEx is a CEN Technical Specification for exchanging public transport schedules and related data. It is based on Transmodel and supports the exchange of complex multimodal networks, stop places, timetables, vehicle schedules, passenger information and fares. It uses XML schema to define a common syntax and structure for the data. It is designed to be used in conjunction with other standards such as SIRI and IFOPT. Website: https://www.netex-cen.eu/
SIRI	SIRI (Service interface for real-time information) is a CEN Technical Specification for exchanging real-time information about public transport services. It is based on Transmodel and defines a set of functional services for different aspects of real-time information, such as estimated times of arrival/departure, vehicle monitoring, situation exchange, and connection protection. It uses the XML schema and SOAP web services to define a common syntax and protocol for the data. It is designed to be used in conjunction with other standards such as NeTEx and IFOPT. Website: https://www.siri-cen.eu/
GTFS	GTFS (General Transit Feed Specification) is a common format for public transit schedules and associated geographic information. It was originally developed by Google in 2005 to power Google Maps transit trip planner. It defines a set of text files that contain information about stops, routes, trips, stop times, calendar, fares and shapes. It uses CSV format to define a common syntax for the data. It is widely used by transit agencies and third party developers around the world. Website: https://gtfs.org/
OJP (Open Journey Planner)	OJP (Open Journey Planner) is a CEN Technical Specification for requesting and providing multimodal journey planning information. It is based on Transmodel and defines a set of functional services for different aspects of journey planning, such as trip request, trip response, trip update request and trip update response. It uses XML schema and SOAP web services to define a common syntax and protocol for the data. It is designed to be used in conjunction with other standards, such as NeTEx, SIRI and IFOPT. Website: https://www.transmodel-cen.eu/ojp-standard/
NaPTan	NaPTan (National Public Transport Access Nodes) is a UK national system for identifying and naming all the points of access to public transport in Great Britain. It provides a unique identifier and a common name for every bus stop, railway station, airport, ferry terminal etc. in the country. It also provides additional information such as location coordinates, accessibility features and local authority codes. It uses XML schema to define a common syntax for the data. It is used by various public transport information systems and standards in the UK, such as Traveline and TransXChange.

Data Models	Description
	Website: https://beta-naptan.dft.gov.uk/
ZHV	The "central stop registry" (ZHV) is the single and most current data set holding all information regarding stops in Germany. The data model is proprietary and the data format is XML. Website: https://zhv.wvigmbh.de/
TRIAS	VDV 431 TRIAS (Travellers' Realtime Information Advisory Standard) is defined as API for information platforms for public transport. TRIAS is modular and service-based and used as communication interface for different software system for timetable and real-time information. Website: https://www.vdv.de/vdv-431-2-ekap-schnittstellenbeschreibung.pdfx
ITxPT	ITxPT is focussed mainly on the standardisation of public transport vehicle equipment such as displays or ticketing machines, and the in-vehicle data exchange between these systems. Data from these systems, relevant to fleet operation or passenger information, is provided from the vehicles towards the fleet operator, and from the fleet operator to other relevant stakeholders. Websites: • https://itxpt.org/specifications/ • https://itxpt.org/catalogue/
DATEX II	DATEX II is a European standard for the exchange of traffic-related data between different actors in the traffic and travel information sector. DATEX II defines a common data model that supports a seamless and interoperable transmission of traffic and traveller information across borders. The data model covers various aspects such as location referencing, situations, variable message signs, measured and elaborated data, parking, traffic management and traffic signal management. DATEX II is a multi-part specification, maintained by CEN Technical Committee 278 (Road Transport and Traffic Telematics). Website: https://datex2.eu/
MDS (Mobility Data Specification)	MDS (mobility data specification) is a data standard that helps cities better manage transportation in the public right of way, standardising communication and data-sharing between cities and mobility providers, such as e-scooter and bike share companies. It consists of six APIs that allow cities to share and validate policy, monitor vehicle status and location, and collect trip data. Website: https://github.com/openmobilityfoundation/mobility-data-specification
GBFS (General Bikeshare Feed Specification)	GBFS (General Bikeshare Feed Specification) is a common data model for shared mobility operators to share information about services available to travellers. It includes information about vehicles (bicycles, scooters, mopeds, and cars), stations, pricing, and more. It is a real-time data specification that describes the current status of a mobility system. Website: https://gbfs.mobilitydata.org/
CDS (Curb Data Specification)	CDS (Curb Data Specification) is a data model that helps cities and companies pilot and scale dynamic curb zones that optimise commercial loading activities. It provides a mechanism for cities to express curb regulations, measure activity, and develop policies that create more accessible, and useful curbs. It consists of three APIs that allow cities to digitally publish curb

Data Models	Description
	locations and regulations, transmit real-time and historic commercial events happening at the curb, and track curb usage metrics. Website: https://github.com/openmobilityfoundation/curb-data-specification
OGC CityGML	OGC CityGML is a standard for representation, storage and exchange of virtual 3D city models. It defines a common semantic information model to for the description of urban objects and their geometry, attributes and relationships. It supports various applications for smart cities and urban digital twins, such as planning, simulation, navigation and disaster management. It can be encoded in different formats, such as GML/XML or JSON. Website: https://www.ogc.org/standard/CityGML/
ETSI NGSI-LD with Smart Data Models	ETSI NGSI-LD is an information model and API for publishing, querying and subscribing to context information. It facilitates the open exchange and sharing of structured information between different stakeholders. It is used across application domains such as smart cities, smart industry, smart agriculture and more generally for the Internet of things, systems of systems and digital twins. The Smart Data Models initiative aims to enable actual data interoperability between diverse systems based on open-licensed data models. Websites: • https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.07.01_60/gs_CIM009v010701p.pdf • https://smartdatamodels.org/ • https://github.com/smart-data-models
CityJSON	CityJSON is a community standard for encoding 3D city models using JSON. It is based on CityGML and aims to be more compact, easy to read and write, and suitable for web and mobile applications. It supports different levels of detail, thematic extensions and metadata, and it can be validated using JSON Schema. Website: https://www.cityjson.org/
ISO 37120	ISO 37120 is a standard for defining and measuring indicators for city services and quality of life across various domains, such as economy, education, environment, health, safety and transport. It provides a framework for collecting, reporting and comparing data across cities. It helps cities to monitor their performance, identify gaps and improve their sustainability. Website: https://www.iso.org/standard/62436.html
MIM	MIMs, or minimal interoperability mechanisms, enable data exchange and service integration among smart city stakeholders. They are based on open standards, specifications and best practices that are widely adopted and supported by the market. They include common data models, APIs, protocols and platforms. MIMs reduce complexity, costs and risks for smart city solutions. Website: https://oascities.org/mims/
ISO/IEC 30145	ISO/IEC 30145 is a standard for developing a smart city ICT reference framework. It defines the concepts, principles, components and relationships of a smart city ICT system. It provides guidance for the design, implementation and evaluation of smart city ICT solutions, and supports interoperability, scalability and security of smart city ICT systems.

Data Models	Description
	Website: https://www.iso.org/standard/76371.html
DIN SPEC 91367	DIN SPEC 91367 is a data model for urban mobility data collection for real-time applications. It defines the data elements and formats for collecting and exchanging mobility data from various sources, such as vehicles, infrastructure, and users. It aims to enable interoperability and innovation in urban mobility services. Website: https://www.din.de/de/forschung-und-innovation/din-spec/alle-geschaeftsplaene/wdc-beuth:din21:3023173
DIN SPEC 91607	DIN SPEC 91607 is a data model for digital twins for cities and communities. It provides a guideline for planning, designing and implementing a digital twin for urban areas, using available standards and avoiding duplication or fragmentation. It addresses various aspects such as use cases, data access and visualisation methods, sustainability goals, citizen participation, and business models. Website: https://www.din.de/de/forschung-und-innovation/themen/smart-cities/aktuelles/der-digitale-zwilling-fuer-staedte-und-kommunen-kommt--859000
DIN SPEC 91377	DIN SPEC 91377 is a data model for data models and protocols in open urban platforms. It is a work in progress and aims to define data models and interfaces for an open urban data platform that can integrate data from various sources and domains, such as energy, mobility, environment, and social services. It goal is to facilitate data sharing and collaboration among different stakeholders in smart cities. Website: https://smart-city-forum.de/?view=article&id=147&catid=22
DIN SPEC 91394	DIN SPEC 91394 is a data model for digitalisation of parking processes, specifically focussing on Data Interfaces. It describes the processes for digital parking management, recording and parking procedures. It additionally offers interfaces for the exchange of data between all parties involved, such as parking operators, service providers, users, and authorities. It also specifies the requirements for the data format. Website: https://www.beuth.de/de/technische-regel/din-spec-91394/299134258
TOMP API	The Transport Operator to Mobility Provider (TOMP) API is a standardised interface for data exchange between transport operators and MaaS providers. It encompasses the entire user trip, from planning to booking, execution, and payment. It is developed and maintained by the TOMP working group, which aims to create an interoperable open standard for technical communication in the MaaS domain. Website: https://github.com/TOMP-WG/TOMP-API
SENSORIS	SENSORIS is a global standardised interface to exchange information between in-vehicle sensors and a dedicated cloud, as well as between clouds. It enables real-time, cloud-based information services that support mobility and automated driving. It is managed by ERTICO – ITS Europe and represents a group of key players from the automotive ecosystem. Website: https://sensoris.org/
ExVe	ExVe (Extended Vehicle) is a concept that allows external service providers to access vehicle data and functions via a standardised interface. It is based on the ISO 20078 standard and aims to ensure fair and secure data access for all stakeholders. It is supported by the European Automobile Manufacturers Association (ACEA) and several vehicle manufacturers. Website: https://www.iso.org/standard/66978.html

Data Models	Description
SAREF4AUTO	SAREF4AUTO is an extension to the ETSI SAREF ontology, which aims at data interoperability in the IoT domain by linking concepts regarding the description of devices. SAREF4AUTO extends this ontology to include the automotive domain and addresses use cases like “platooning”, “Automated Valet Parking (AVP)”, and “Vehicle environment with Vulnerable Road Users (VRU)”. Website: https://saref.etsi.org/saref4auto/
OpenDRIVE	ASAM OpenDRIVE is a standard that defines a common road network description format for driving simulators and testing applications. It describes the logical and geometrical representation of roads, lanes, intersections, traffic signs, signals, and other road features. It is developed and maintained by the Association for Standardisation of Automation and Measuring Systems (ASAM). Website: https://www.asam.net/standards/detail/opendrive/
OpenSCENARIO	ASAM OpenSCENARIO is a standard that defines a common scenario description format for driving simulators and testing applications. It describes the dynamic behaviour of traffic participants, environmental conditions, events, actions, and manoeuvres in a simulation. It is developed and maintained by ASAM and complements ASAM OpenDRIVE. Website: https://www.asam.net/standards/detail/openscenario/
OpenODD	ASAM OpenODD (Open Operational Design Domain) is a standard that defines a common description format for operational design domains (ODDs) of automated driving systems. It describes the conditions and limitations under which an automated driving system can operate safely and reliably. It is developed and maintained by ASAM and complements ASAM OpenDRIVE and ASAM OpenSCENARIO. Website: https://www.asam.net/standards/detail/openodd/
ODX (Open Diagnostic Data Exchange)	Open Diagnostic Data Exchange (ODX) is a standard that defines a common data format for exchanging diagnostic data between vehicle manufacturers, suppliers, and service providers. It covers the specification of diagnostic communication, data identification, service parameters, error memory entries, flash processes, and variant coding. It is based on the ISO 22901 standard and supported by several industry associations and organisations. Website: https://www.asam.net/standards/detail/odx/
OTX (Open Test sequence eXchange)	Open Test sequence eXchange (OTX) is a standard that defines a common scripting language for exchanging test sequences between different test systems and tools. It covers the specification of test procedures, test steps, test parameters, test results, test reports, and test diagnostics. It is based on the ISO 13209 standard and supported by several industry associations and organisations. Website: https://www.asam.net/standards/detail/otx/
C-ITS and C.Roads	C-ITS means intelligent transport systems that enable ITS users to cooperate by exchanging secured and trusted messages. Messages exchange include, among others, hazardous event warnings, traffic light information, dynamic traffic signs, etc. Messages are standardised by ETSI ITS, and C-Roads has developed profiles for infrastructure and vehicle communication (V2X), as well as for vehicle-to-vehicle communications (V2V). Messages are distributed either over short range over ITS-G5 or over long range between backends. C-Roads has developed protocols for both control and data plane communications.

Data Models	Description
	The EU has developed a C-ITS trust model (C-ITS Credential Management System) based on a Public Key Infrastructure (PKI) with federated certificate authorities.
OSI prime 2	OSI prime 2 is a seamless digital database for the entire country of Ireland that provides a standardised and authoritative spatial data infrastructure for the consistent and accurate referencing and integration of national data related to location. It does not use individual map sheets, but treats all mapping features as continuous objects. It is aligned with the Public Service ICT Strategy and enables the amalgamation of multiple national data sets for better analysis and decision making. Website: https://osi.ie/
INSPIRE	INSPIRE is a directive that aims to establish an infrastructure for spatial information in Europe to support environmental policies and activities that may impact the environment. It specifies common data models, code lists, map layers and metadata for 34 spatial data themes across three annexes. It also defines a set of implementing rules and technical guidelines to ensure the interoperability and accessibility of spatial data sets and services. Website: https://inspire.ec.europa.eu/
TN-ITS	TN-ITS is a European platform for the exchange of information on changes in static road attributes, such as road signs and speed limits. It aims to provide fresh, accurate and trusted digital maps for intelligent transport services and applications. It involves public and private stakeholders in the data chain mechanism. Website: https://tn-its.eu/
RailML	RailML is a common data format for railway applications. It is based on XML and enables interoperability and data exchange between different railway systems and software tools. It covers various aspects of railway operations, such as infrastructure, timetabling, rolling stock, and signalling. Website: https://www.railml.org/en/
TAF/TAP TSI	TAF/TAP TSI, which stands for Telematic Applications for Freight and Telematic Applications for Passengers, are technical specifications for interoperability. They define common data formats and processes for railway traffic management and passenger information in Europe. They aim to improve the efficiency, quality and reliability of rail transport services. Website: https://taf-tsi.uic.org/
OSDM (Open Sales and Distribution Model)	OSDM (Open Sales and Distribution Model) is a new standard for ticket sales and distribution in the rail industry. It is based on RESTful APIs and JSON data structures and enables seamless integration of different sales channels and systems. It supports various features, such as fares, reservations, ticketing, after-sales and reporting. Website: https://osdm.uic.org/
IATA CargoXML	IATA CargoXML is a standard for electronic communication between airlines and other air cargo stakeholders, such as shippers, freight forwarders, ground-handling agents, and regulators, as well as customs and security agencies. It is based on multimodal and cross-border messaging and aims to facilitate cargo business processes, fulfil customs requirements, and comply with security regulations. Website: https://www.iata.org/en/programs/cargo/e/cargo-xml/

Data Models	Description
IATA Cargo IMP	IATA Cargo IMP is a standard for electronic communication between airlines and other air cargo stakeholders using legacy EDIFACT messages. It defines the structure, format, and content of messages such as air waybill, flight manifest, house waybill, etc. It is widely used in the air cargo industry but is gradually being replaced by CargoXML. Website: https://www.iata.org/en/programs/cargo/e/cargo-xml/
IATA ONE Record	IATA ONE Record is a standard for creating and sharing data about air cargo shipments using a common data model and an API-based platform. It enables end-to-end visibility and traceability of air cargo shipments by allowing stakeholders to access and update data in real time. It also supports data quality and security by using digital identity and consent management. Website: https://www.iata.org/en/programs/cargo/e/one-record/
eFreight	eFreight is an initiative to replace paper documents with electronic data and messages throughout the air cargo supply chain. It aims to improve the efficiency, accuracy, security, and environmental sustainability of air cargo operations. The initiative mandates the use of CargoXML or CargoIMP standards for data exchange. Website: https://www.iata.org/en/programs/cargo/e/efreight/
eAWB360	eAWB360 is an initiative to accelerate the adoption of the electronic air waybill (e-AWB) in the air cargo industry. It is a collaborative approach that involves airlines, freight forwarders, ground handlers, and IT providers to implement e-AWB at selected airports. It aims to reduce the costs, errors, delays, and carbon footprint of air cargo shipments. Website: https://www-intfx.iata.org/en/programs/cargo/e/eawb/eawb360/
DCSA data model	Digital Container Shipping Association is an organisation established by container shipping companies with the goal of establishing de facto standards for interoperability of IT solutions. It provides standards for special use cases such as the booking process, cyber security, electronic bill landing, and more. Website: https://dcsa.org/standards/
UN/CEFACT MMT	The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) provides recommendations and standards for multiple trade topics. One of these standards is MMT-RDM (Multimodal Transport Reference Data Model), which deals with commercial transactions (BUY), transport control (SHIP) and financial transactions (PAY). Website: https://unece.org/trade/uncefact/mainstandards

7.4. Findings and observations

During the analysis for state-of-the-art interoperability building blocks, several key findings and examples emerged. These findings are presented based on the DSSC building block taxonomy.

Observations for “Data models and formats”:

- In the research on interoperability, 18 individual thematic categories were identified, as presented in Section 1.4. These different mobility domains partly use different data exchange standards and data formats. For example, road traffic information is often provided via DATEX II, while rail transport employs different standards (RailML, OJP, SIRI, TAF/TAP, etc.).

- The listed standards are widely accepted and commonly used in the respective domains. However, within domains, data is often available in different data model formats including different standards, profiles and versions, proprietary solutions. For example, while NeTEx and GTFS both cover public transport schedules, GTFS can be considered a subset of NeTEx and therefore less comprehensive. Nevertheless, it has been observed that data customers prefer more lightweight data models like GTFS over complex data models such as NeTEx or OJP because they are easier to use and implement.
- Other examples are NaPTan (UK) and ZHV (Germany). Both serve the purpose of proving stop information on a national level and can be considered as building blocks for interoperability within their respective countries. However, they lack alignment on a European level, rendering them non-interoperable. This might be due to the absence of suitable European standard at the time, or the standards were not user-friendly enough. The EMDS should explore methods to support its participants to map or convert such different data models to enable utilisation in a unified way.
- European Standards with national Profiles: European Standards like DATEX II or NeTEx[230] are used by individual countries by applying their own "profiles" tailored to their specific needs. There are some efforts within the EU to harmonise local NeTEx profiles and to develop EU profiles.
    - In the public transport domain, efforts to harmonise the collection and exchange of mobility data (e.g. stop place information, timetable data, real-time data, flex and also relatable on-demand mobility) stem from a need to address identified gaps in the variety of data languages and semantics. For example, the reference standard Transmodel[231] makes data available in standard formats such as NeTEx and SIRI. As such, it serves as an example of a reference standard which plays an important strategic role in European Public Transport Data under the ITS Directive (Priority Action A).
    - In contrast, NeTEx is a comprehensive data format designed to describe different concepts for public transport data in various ways. In some cases, local or national specificities related to public transport systems may require adaptation as they exceed requirements in the actual implementation. Therefore, some countries use "profiles" by offering a predefined set of choices (i.e. guidelines) for use in a specific context or use case. This defines additional explicit rules to help in the implementation. These profiles remain compliant with the standard (e.g. NeTEx) and merely represent a subset to simplify and address the needs of a particular application, with the potential to be subsequently used for any similar initiatives.
    - In the EU, several different "profiles" exist to specify the needs of a particular application. One example is the European Passenger Information Profile[232], which serves as a reference profile for EU Member States by focusing on a set of minimal requirements for information that is for passenger information services. This means that for a given use case or context it is expected to exchange data only on specified parts of the NetEx format. Another example is the Nordic NeTEx[233], which focuses on a set of features (frames, files, values and how data should be interpreted) and outlines the scope for usage in Norway.[234] There are plans for a joint interpretation,

[230] NeTEx (n.d.), "Network Timetable Exchange", https://www.netex-cen.eu.
[231] Transmodel (n.d.), "Transmodel is the CEN European Reference Data Model for Public Transport", https://www.transmodel-cen.eu.
[232] Data4PT (2021), "NeTEx-CEN/NeTEx-Profile-EPIP", https://github.com/NeTEx-CEN/NeTEx-Profile-EPIP.
[233] Nordic NeTEx Profile (n.d.), https://enturas.atlassian.net/wiki/spaces/PUBLIC/pages/728891481/Nordic+NeTEx+Profile.
[234] ODIN (n.d.), "Open Mobility Data in the Nordics", nordicopenmobilitydata.eu.

design and implementation of the Nordic NeTEx, thereby enabling more opportunities for cross-border mobility services.
    - Harmonising these profiles could strengthen the implementation of standard reference data models, helping data exchange of public transport information. This harmonisation is essential in the EU for travellers, public transport operators, and third party service providers to present relevant and high-quality data (e.g. for journey suggestions). Furthermore, harmonised profiles will minimise the costs of supporting multiple different exchange formats by reusing data to develop relevant services, thus enabling continuous growth through the standardisation of public transport data exchange.
- Semantic interoperability faces additional challenges due to the variety of the languages used in recording data. Translating and aligning data across Member States for consistent meaning and interpretations is complex and time-consuming. While guidelines and principles exist for some data models, newer sources may lack explicit standards or still use outdated formats due to legacy systems.
    - A good example can be found in the logistics sector. This domain faces hurdles with outdated systems and data quality issues, resulting in duplication and inefficiency. A lack of investment in modernising these systems further compounds the problem. Aligning customs regulations and national implementations in logistics is a complex and time-consuming endeavour. Especially when the data quality differs and varies among national/international data sources, which makes interoperability a challenge (identified data might be available but not always in the correct format to allow easy integration or fusion). These challenges underscore the critical importance of fostering trust and security in data spaces to encourage collaboration and innovation in the mobility sector.
    - Another example is the relatively new shared mobility domain. It is observed that existing standards are being extended to cover this domain, like NeTEx or SIRI. In parallel, new data models are emerging in these domains, such as MDS and GBFS.
- Providing data models in an open environment (like the Smart Data Models on Github) enables active contributions from domain experts. This approach ensures that decisions, issues and change processes can then be handled in a transparent way.

Observations for “Data exchange”:

- In the analysis of the mobility ecosystems, different approaches for data exchange have been identified. They range from:
    - Centralised approaches, where all data is stored on the platform. This type is of often found in open data platforms, where the data does not change frequently.
    - Platforms that transmit the current data set from the provider to the consumer acting like a message broker, or platforms that only provide links to data provider’s own systems. This type of platform is used where real-time information, such as road conditions, public transport or supply chain events, needs to be instantly provided to support information services and applications.
- Some platforms collect the data from sources/providers and invest additional effort into normalisation and harmonisation of the data to create a new harmonised data set. This approach ensures standardised data exchange for consumers. There is a downside, however, as collecting, harmonising and providing this data requires substantial resources at the platform, and harmonisation may change the original data.
- Decentralised platforms act as intermediaries, assuming specific organisational tasks such as registration, authentication, or metadata provision.

- Exchange takes place bilaterally between the partners involved. Data sovereignty remains with the provider and data reaches the consumer unchanged, exactly as the provider makes it available. There is no adaptation of the data content or formats; the corresponding transformation work must be carried out by the consumer.
- Decentralised data sharing approaches exist within mobility data spaces (e.g. EONA-X, the MDS, Catena-X, etc.). Data owners seem more inclined to follow this path. The amount of work handled by the platform (and its software) must be adapted to provide a software solution for the participants. This could include, for example, the necessary platform or data space functionality for self-descriptions, checking identities, establishing data exchange, tracking data usage, etc. by Infrastructure-as-a-Service providers (see Section 3.2 and 4.3) and the on-premises functionality for connecting to a data space and executing data apps by "Connector-as-a-Service" providers (see Section 2.3 and 3.5).
- It is observed that many data ecosystems do not provide a technical data exchange capability, meaning that the user is expected to be a natural person, who searches for and downloads data via its browser.
- Data ecosystems with data exchange capabilities were found to be either proprietary solutions or reliant on a few open source implementations, such as CKAN or FIWARE which implements the ETSI NGSI-LD as a domain-agnostic, common language for data spaces.
- An important observation was that in the mobility sector, there has been substantial effort in standardising data models, but significantly less in terms of data exchange. Only a few standards, such as DATEX II, SIRI or OJP, also cover the data exchange layer, given the fact that these standards extend into the application layer.

Observations for "Provenance and traceability":

- Most data ecosystems investigated did not support capabilities regarding provenance and traceability. Neither the ecosystem operators nor the data providers could determine who and how often data sets had been consumed or downloaded.
- A few data platforms, like the Mobilithek (German NAP), offer monthly protocols to consumers and providers to check compliance with service-level agreements etc, but these protocols must be manually accessed and are not available via an API.
- A few data space implementations, like the MDS, have already implemented services like the IDSA clearing house to log data transactions.
- In the logistics domain, the concept of "event-driven real-time data flow control" has been developed by the EU CEF FEDeRATED project[235] and is strongly promoted by the DTLF (Section 2.2). Its architecture enables the use, storage and propagation of application-level events (in supply chains). This process triggers smart contracts that grant access to specific data within a data space. It is not yet clear if these concepts are suitable on a data space level or if their relevance is limited to the use case level where it enables secure data sharing between stakeholders.

7.5. Recommendations

Conclusion

Interoperability of data in the mobility and logistics sector is a pressing issue across all application domains identified through the consultation activities. The data collected and made available by different stakeholders are supported by diverse data formats and standards and vary in accessibility through various platforms. In addition, standards and frameworks applied within each application

[235] EU FEDeRATED project (n.d.), "EU-project for digital cooperation", http://www.federatedplatforms.eu.

domain are often optimised to facilitate data exchange for specific scopes and needs only, and often vary per geographical region. The diversity in these data formats, standards and accessibility among different stakeholders, different application domains and regions poses challenges in optimising data sharing and harmonisation processes across Europe. For instance, a transportation agency may struggle to align its data format with that of other companies or government agencies. Such a lack of interoperability hinders the effective integration and analysis of data while also restricting possibilities for advanced purposes like training machine learning or AI models. Thus, linking and combining data sets within and across sectors in a future common EMDS remains a significant hurdle.

Recommendations

In a decentralised data space, it is almost not feasible to mandate the use of or the migration towards certain data models or standards from the outset. Such an approach would likely encounter a lack of acceptance and entail high investment costs. Moreover, it would contradict the principles of data sovereignty. Instead, it is more pragmatic to embrace existing data models, which have evolved for specific reasons and serve well-justified purposes. Nevertheless, harmonisation should remain an important goal in achieving interoperability between these data models and standards by considering the following recommendations.

Promote sector specific data models and target their interoperability

Harmonisation can only be achieved incrementally. While cross-sector data exchange is desirable and important, it is prudent to initially focus on mobility and logistics when establishing a data space. A first step should be to strengthen interoperability within a sector. This should be accomplished by analysing the influence and prevalence of different **sector specific data models**, understanding the reasons for adopting proprietary solutions even when standards are available, and identifying 1-2 reference standards for the domain (including the provision of suitable profiles if the standard is not a perfect fit), and offering services to support data suppliers in aligning their data according to the selected standard(s). Although some sectors seem to use standardised models such NeTEx or DATEX II, the usage of application profiles or attributes within these standards differs by country or region.

- The usage of these standards should be harmonised on a European level, by emphasising on achieving **common usage of attributes and application profiles**.
- A further step should be to improve interoperability between sectors, for example by introducing and using **basic data models** and vocabularies such as TRANSMODEL or INSPIRE that can be included or referred to from existing data models.
- In the application domains related to freight and logistics (specifically cross-border operations), narrowing the focusing solely on EU standards will be limiting due to the global nature of shipping logistics[236].

Foster linked data concepts

In cases where the adoption of basic data models into domain specific data models is not feasible, **linked data concepts** can be employed to map information from a data model towards a harmonised taxonomy. This linking information is typically provided within the accompanying metadata or information model data (see below). As a result, several data models become interoperable by linking their attributes to a unified concept model.

[236] To address the lack of consistent identifiers across the many actors involved in the chain of logistics, a common language is necessary between trade and transport sectors. As such, UNECE UN/CEFACT has produced international standards (e.g. references data models) to streamline communication between these actors, see UNECE (n.d.), " Streamlined presentation of UN/CEFACT standards, https://unece.org/trade/uncefact/mainstandards.

Foster mapping and utilisation in data space services and data apps for data conversion

Interoperability can be enhanced by offering means to transform data sets from one data model to another. The basis of data model conversions lies in **schema mappings** from one data model to another (like NeTEx to GTFS or GBFS to NeTEx and SIRI[237]). These mappings should either be part of existing standards or established as standalone standards. These mappings serve as a basis for data model conversion or even function as a quality assurance measure. They could be provided as **data space services** or integrated into data space connectors as **data apps** to be utilised by the participants when needed.

Utilise a unified metadata model

In contrast to the various data models that are used for specific application domains, the EMDS should advocate for **one single metadata model** to provide additional information on a data set such as licence, ownership, geographic coverage, temporal validity, etc. The NAPCORE project is currently standardising the **mobilityDCAT-AP** metadata model to serve as a harmonised foundation applicable to all National Access Points. It builds upon DCAT-AP and the Coordinated Metadata Catalogue, which also formed the basis for the metadata model of the MDS. The model is flexible, extendable, and linkable to other data models, making it the current best option for ensuring interoperability of metadata.

Employ data quality frameworks from a use case perspective

Interoperability between data sets and data models can be enhanced by defining **harmonised quality metrics** that can be used to measure specific quality dimensions. It is important to approach this topic not solely from the perspective of the data set itself, but rather from the context of the use case that employs the data set. From the perspective of use cases, specific requirements can be derived and translated into measurement units. Evaluating these measurements can determine if a data set aligns with a set of specific use cases. Currently, several initiatives are focusing on the standardisation of such **data quality frameworks**, such as ITxPT, NAPCORE and EU-EIP[238]. It is recommended that the EMDS supports these quality frameworks and actively advocates for their usage.

Utilise a unified information model

Information models serve the purpose of technically describing organisations, their capabilities, technical systems, data endpoints and more. Information models on a data space level encompass a much broader range compared to metadata models. Similar to the metadata model, it is important that the EMDS adopt a single information model, for example the IDS Information Model, the Gaia-X information model (based on self-sovereign identities), or FIWARE NGSI in conjunction with the Smart Data Model initiative.

Ensure compatibility of data exchange building blocks with sector specific protocols

Leverage the benefits by implementing generic, non-domain-specific **data exchange APIs** like NGSI-LD or those data exchange protocols proposed by data space initiatives such as IDSA. These protocols also incorporate semantic web/linked data approaches, contributing to the development of the European common data spaces. This becomes increasingly important and helpful with regard to data space federation, as it facilitates connecting and interlinking of data to other related domains.

[237] MobilityData, DATA4PT (2022), "GBFS to NeTEx & Siri", Version 1.0, https://drive.google.com/file/d/1bvxr8s4tOEJigstJUt_qyA2dn29jC84O/view.

[238] European ITS Platform (2022), "C-ITS. Quality Package", Version 1.0, https://www.its-platform.eu/wp-content/uploads/ITS-Platform/AchievementsDocuments/Quality%20Frameworks/EU%20EIP%204.1_C-ITS%20Quality%20Package%20v1.0_20220121.pdf.

However, it is important that mobility specific applications layer protocols, like SIRI, are supported by the generic, non-domain-specific data exchange building blocks.

7.6. Building blocks

Figure 26 shows the individual building blocks recommended for data interoperability.

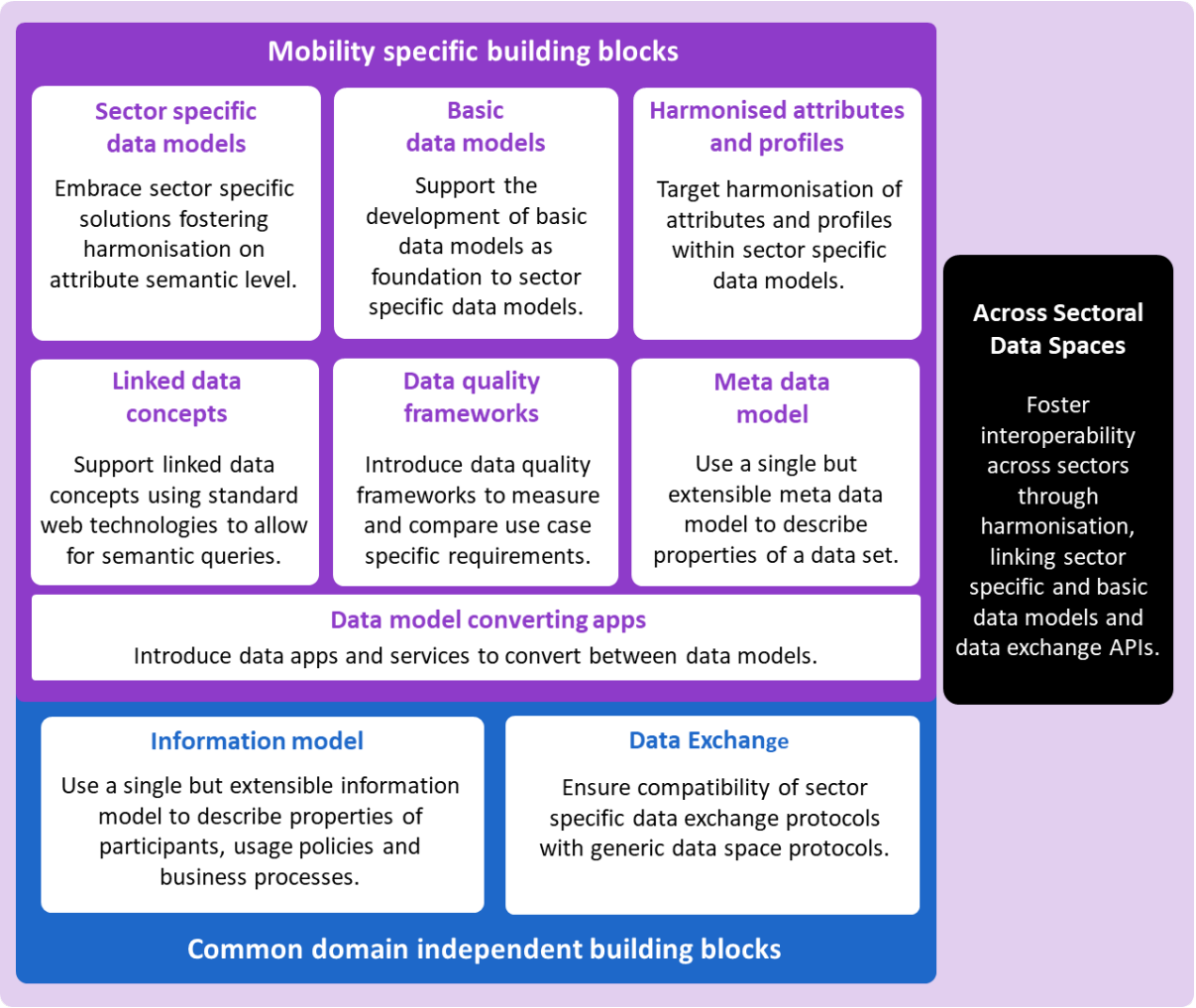


Figure 26: Building blocks for data interoperability.

8. Data sovereignty and trust

8.1. Introduction

Data sovereignty refers to the concept of retaining authority and control over one's data, empowering individuals or organisations to determine who can access their data and for what purposes. Trust also establishes confidence in shared data and includes the capabilities required for both data sovereignty and for information security, ensuring accuracy and integrity of the shared data.

Data spaces should guarantee that participants within a data space can exercise sovereignty over the data they share, for instance by defining, and legally and technically enforcing access and usage control policies. Trust between data space participants and in the data they share is essential. Data sovereignty and trust call for the adoption of common standards for managing the identity of participants and capabilities and for verifying their truthfulness. Further, they require the definition, agreement, and enforcement of data access and usage control conditions. Finally, it is worth noting that data sovereignty is a key aspect within the broader scope of **digital sovereignty**, which is defined as "control over the design and use of (business) critical digital systems, algorithms, and the data generated and processed by them"[239].

This chapter addresses data sovereignty and trust within the context of the EMDS. As explained in Chapter 4 on governance, these concepts play a fundamental role for enabling data sharing within and across data spaces. As such, they require an aligned approach to enable interoperable data spaces, implying that (by default and whenever possible) the **trust mechanisms** for a mobility data space should align with the common approach and building blocks that are **generically developed across data spaces**, such as those outlined in the DSSC blueprint. Moreover, when developing trust building blocks for the EMDS, only mobility specific aspects and features should be considered as additional input for the DSSC blueprint development or as a specific feature within the EMDS.

Section 8.2 addresses the generic data sovereignty and trust mechanisms and frameworks required for the EMDS. These mechanisms are intended to be defined and developed as generic (and therefore interoperable) building blocks for various domains and should be adopted and adhered to by the EMDS. Section 8.3 addresses the features/requirements that may be mobility specific and should be considered as additional input for the DSSC blueprint development or as a specific feature within the EMDS. Section 8.4 addresses the information security aspects. Section 8.5 presents the conclusion, recommendations and building blocks for data sovereignty and trust for the EMDS.

8.2. Generic building blocks for data sovereignty and trust

Data sovereignty, trust and the associated building blocks constitute integral elements of the data space concept. These should be developed as generic concepts and building blocks for multiple domains across data spaces to ensure interoperability and contribute to the EU's ambition of common European data spaces.

The following subsections address the data sovereignty and trust building blocks in a generic, i.e. non-mobility specific, manner. They are expected to be defined and developed by the DSSC blueprint. The EMDS should (by default) adopt and adhere to these generically developed building blocks as data sovereignty and trust are key capabilities for interoperability between data spaces.

[239] TNO (2022), "R10507. Bridging the Dutch and European Digital Sovereignty gap", https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf.

Identity management

Identity management enables the identification and authentication of "entities" within a data space, serving as a basis for granting access to IT resources such as data sets and data services. As such, identification and authentication may apply to both legal persons, natural persons, and software modules including connectors, gateways, and systems.

Moreover, identification and authentication of entities within a data space occur at two levels[240]:

- At the level of **legal identities** to identify and authenticate natural persons, organisations or software components as legal entities.
- At the level of **data space members** to manage the membership of legal entities of a data space, designating them as "participants", and ensuring adherence to legal agreements. During run-time, a data sharing transaction may include a process for verification of legal identity and status of participants, including their data space membership.

It is important to note that both levels of identification and authentication are relevant for data spaces. Identifying entities as data space members serves as a basis for verifying that these entities have been onboarded to a specific data space, certifying their compliance with and adherence to the data space agreements. Identifying entities as legal entities also allows individual verification processes for legal status and trustworthiness among participants, both within a single data space instance and across multiple data space instances.

Information provision is also an important aspect of identity management, enabling entities to define data access and usage control. This aspect will be addressed as part of the "Authorisation" trust mechanism below.

The use of unified identities allows for interoperability and trust across data spaces, enabling a standardised approach to identity management, authentication and authorisation. With unified identities, individuals, machines, organisations, or other entities are granted consistent and recognised identities, regardless of the data space they inhabit. Furthermore, unified identities enable findability of parties across data spaces.

OAuth2.0 and OpenID Connect, commonly used for authentication and authorisation in modern web applications, serve as standard trust mechanisms in data spaces. They offer improved security by using access tokens instead of traditional credentials like passwords, thereby reducing the risk of exposing sensitive information. These protocols ensure that resource owners retain control over their data. OAuth2.0 is commonly employed in machine-to-machine flows, facilitating communication between a client and resource applications. OpenID Connect serves as an authentication protocol built on top of OAuth2.0. It is designed for human-to-machine flows, where human clients request access to specific resources.

The (inter-)national environments of federated data sharing and data spaces are still in development. Leading European reference architecture initiatives on federated data sharing and data spaces (IDSA, iSHARE, Gaia-X, DSBA, etc.) are progressing **towards fully decentralised trust framework capabilities**. The same applies to identification and authentication, for which Self Sovereign Identities (SSIs), Verifiable Credentials (VCs) and Decentralised IDentifiers (DIDs) provide the means for a fully decentralised approach. While these developments are rapidly maturing, they still have to prove their technical and market viability for large-scale deployed in the near term. Nevertheless, a fully

[240] International Data Spaces Association (2021), "Position Paper: Governance for Data Space Instances – Aspects and Roles for the IDS Stakeholders". https://internationaldataspaces.org/wp-content/uploads/IDSA-Position-Paper-Governance-for-Data-Space-Instances-Aspects-and-Roles-for-IDS-Stakeholders.pdf.

decentralised approach should be considered and integrated into the design, development and deployment of the EMDS from the outset. In particular, the FEDeRATED approach for data sharing in the logistics sector asserts longer-term that each organisation applies its own identity and access management capabilities, with support from SSIs, VVCs and DIDs.

Authorisation

To establish trust and data sovereignty for the data-entitled parties, data-sharing policies need to be implemented within data spaces. These policies allow data-entitled parties to delegate precise rights to consuming participants. To ensure effective implementation and safeguard trust, it is essential to define, register, agree upon and technically enforce these policies, which may necessitate separate capabilities. As such, the following subsections address the definition, registration, agreement, and enforcement of authorisation policies, respectively. To define **authorisation (access and usage control) policies**, a policy definition and description language is required. An extensive overview of 21 policy classes for usage control, which are considered to be supported, is provided in an IDSA position paper on usage control[241]. Of the 21 policy classes for usage control as described in the IDSA position paper, most can be envisaged as relevant for use cases in the mobility and logistics sector. These include, for example, “Restrict the data usage when a specific event has occurred”, “Restrict the data usage to a specific time interval”, “Log data usage information”, “Notify a party or a specific group of users when the data is used” and “Attach policy when distributing data to a third party “.

The XACML policy language is one such standard with a general focus on access control and providing an architecture. In contrast, the ODRL standard policy language expresses and manages digital rights in a machine-readable format with a focus on the syntax and semantics of rights expression for digital content. This includes permissions, prohibitions and obligations associated with digital content and services. Based on a W3C standard, ODRL is a powerful and flexible, semantics-based standard for policy definition[242].

IDSA, iSHARE, Gaia-X, DSBA, and the emerging **Dataspace Protocol** all recommend using ODRL as a policy definition language. Therefore, it is suggested that the EMDS align with this approach and use ODRL to define usage and access control policies. A policy registry capability (building block) can be used to register, expose and query formal data sharing policies. It contains the specific access and usage conditions for IT resources to be shared. In addition, the policy registry can function as a delegation registry, allowing an entitled party to delegate access and usage rights to other data space participants. In the iSHARE trust framework, a **policy registry** is designated a distinct role, referred to as “Authorisation Registry”. It includes the functionality to support various levels of **authorisation delegation**. Three main approaches for agreement on authorisation policies may be distinguished as follows:

- **By overarching contract and unidirectional communication**
  An overarching contract governs the relationship between data space participants, setting standardised terms and conditions for data sharing. It ensures consistency, transparency and trust among participants while serving as the basis for data exchange. Sub-contracts between individual participants allow for more specific data sharing arrangements built upon the principles outlined in the overarching contract. This ensures a secure and compliant environment for data exchange while respecting data privacy and ownership rights.

[241] International Data Spaces Association (2021), “Usage Control in International Data Spaces”, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3.pdf.
[242] World Wide Web Consortium (2018), “ODRL Information Model 2.2”, W3C Recommendation, https://www.w3.org/TR/odrl-model.

An example of an overarching contract can be found in the iSHARE Trust Framework[243], where this contract is known as the "Accession Agreement". This agreement is established between a data space participant and the governing body of the data space, referred to as the "Satellite" within the iSHARE framework. All participants within the Accession Agreement are bound by the terms of use and iSHARE specifications. After signing the agreement, the participant becomes a part of the data space.

- **By authorisation licenses**
  Authorisation licenses define how services can be consumed and the conditions for data exchange. These licenses complement authorisation policies, providing more specific usage guidelines. Participants within a data space agree upon and adhere to these licenses, enabling mutual compliance. In the iSHARE trust framework, licenses are standardised; in authorisation policies they must be specified. Participants are bound to the framework rules and can request each other to follow the provided licenses.
- **By (bilateral) contract negotiation**
  The (self-)description of available data assets also includes an authorisation policy (usage control information) in the form of a contract, describing the conditions under which a data provider is willing to make its data available to a data consumer. These conditions can range from simple access restrictions to complex pre- and post-duties (usage restrictions). In a (semi-)automated negotiation process, the data consumer and the data provider need to agree on a data usage contract.
  IDSA[244], Gaia-X[245], DSBA[246], and the emerging Dataspace Protocol[247] support contract negotiation capabilities. In its Technical Convergence document, the DSBA explicitly proposes the Dataspace Protocol as the foundation for contract negotiation and control.

Various types of data sharing need to be supported within the EMDS, as described in Chapter 2. This includes, for example, the sharing of (persistent) data bilaterally between specific data space participants and the simultaneous sharing of streaming data from a single provider to a multitude of receivers. This diversity also implies that a one-size-fits-all mechanism for agreeing on authorisation policies is not feasible for all use cases. Hence, it is to be expected that each of the approaches described above needs to be supported within the EMDS.

Enforcement of authorisation policies can include both legal and technical components:

- The **legal enforcement of authorisation policies** can be achieved by establishing legally binding contracts between the data sharing participants, ensuring adherence to agreed-upon authorisation policies. Various approaches for establishing legally binding contracts for authorisation agreements may be used, as described in the previous subsection. Legal aspects of data sharing are further addressed in Chapter 5.
- For the **technical enforcement of authorisation policies**, the eXtensible Access Control Markup Language (XACML) standard [248] is commonly used to implement a Policy Enforcement

243 iSHARE Foundation (n.d.), "iSHARE – Trust Framework for Data Spaces", https://ishare.eu.
244 International Data Space Association (2022), "Contract Negotiation", https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_4_process_layer/3_4_3_contract_negotiation.
245 Gaia-X Federation Services (n.d.), "Data Contract Service", https://www.gxfs.eu/data-contract-service.
246 Data Space Business Alliance Data Space Business Alliance (2023), "Technical Convergence. Discussion Document", Version 2.0, https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.
247 International Data Spaces Association (2023), "Dataspace Protocol", Version 0.8, https://github.com/International-Data-Spaces-Association/ids-specification/tree/main.
248 OASIS (2013), "eXtensible Access Control Markup Language (XACML) Version 3.0", OASIS Standard, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

Framework (PEF) for authorisation (access and usage control) policies. Although the implementation may vary across modules, XACML-based policy enforcement is included in both the IDSA, FIWARE and DSBA architectures. The XACML architecture for policy enforcement distinguishes a set of capabilities (and associated APIs) for managing and enforcing data-sharing policies: the Policy Enforcement Point (PEP), the Policy Decision Point (PDP), the Policy Information Point (PIP), the Policy Retrieval Point (PRP) and the Policy Administration Point (PAP). The IDSA reference architecture introduces some extensions to these capabilities. Alignment will be required on the interfaces between the XACML capabilities, and the definition language used for the policies.

The approach for (technical) enforcement of authorisation policies is generic, i.e. it is similarly applicable to each of the sectoral data space initiatives. Therefore, it is recommended not to develop or adopt mobility-data-space-specific capabilities for authorisation policy enforcement, but wherever possible, to **align with and adhere to the (synergetic) authorisation policy enforcement capabilities** and processes that will be developed generically across the sectoral data spaces.

Trust anchors

The concept of trust anchors has been introduced by Gaia-X[249]. Trust anchors are organisations entitled to underpin, verify and sign claims by participants. They can be government entities, specialised organisations or even the data space authority. In essence, trust anchors enhance trust in otherwise self-declared statements. The EMDS should adopt and adhere to generic trust anchor capabilities, in alignment with the DSSC blueprint.

Onboarding and certification

To establish trust among all participants in the ecosystem of federated and interoperable data spaces, a certification framework may be required as part of the onboarding process. Certification indicates compliance of a participant or technical components with the criteria and the evaluation method for the data space, as agreed upon under the coordination of the data space authority.

Certification can apply to either new data space participants or technical components:

- **Certification of data space participants (organisations)**
  Examples of certification of data space participants include the certified roles in the iSHARE role model[250]: (1) the iSHARE Satellite (the federated scheme administrator responsible for onboarding participants into the network of the data space), (2) the iSHARE Authorisation Register (enabling the registration and sharing of data-sharing policies by data owners), (3) the Human Identity Providers (providing verified personal credentials, with authorisations from and links to legal entities and eIDAS) and (4) IDSA certification for the operational environment of data space participants[251] (providing an assessment of the trustworthiness of the physical environment, defined processes and organisational rules).

- **Certification of data space (technical) components**
  The foundations of a data space are data sovereignty and trust. As an example, the IDSA has defined a rigorous, transparent certification process for data space components, ensuring that the IDS-connectors (as the main component) perform as intended. A certified (trusted) IDS

[249] GAIA-X European Association for Data and Cloud (2022), "Trust Anchors", https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/trust_anchors.
[250] iSHARE Foundation (n.d.), "Roles", https://ishare.eu/about-ishare/roles.
[251] International Data Spaces Association (n.d.), "Certification: the basis of trust", https://internationaldataspaces.org/offers/certification.

connector is initially foreseen for those participants in core roles requiring stringent usage policy enforcement on the sharing of (valuable or sensitive) data and/or support of the IDS information model for message exchange.

Similarly, the DSBA foresees services from certification and audit agencies which will help to validate the reliability, security and sovereignty of specific cloud services by verifying their compliance with predetermined market-wide certifications.

When executing data sharing transactions, run-time support for requesting and verifying certification status and validity of participants or technical components is needed to enable mutual trust within a data space.

Trust monitoring

To assure trustworthiness of the overall ecosystem of federated and interoperable data spaces and the data sharing transaction processes that they enable, it is important that the building blocks provide sufficient monitoring capabilities to (automatically) detect, prevent and possibly resolve potential trust or security breaches.

To this end, a data space may provide capabilities for:

- **Remote Attestation:** the verification of the integrity of security gateways at run-time, defined for security gateways (connectors) as part of the IDS Communication Protocol (IDSCP)[252];
- **Dynamic Trust Monitoring:** the verification of integrity over an extended period with the ability to trigger actions (in case of validations) and/or revocation of data space membership certificates.

Deployment in a safe and trusted cloud environment

A trustworthy execution environment is important for the deployment of data space components that handle sensitive data. This applies to both the deployment of the IT modules providing the data space infrastructure (e.g. identity management and metadata brokering, sometimes also referred to as "intermediary" functions) and for the deployment of the data space connectors. Hence, deployment of these data space components requires a trustworthy cloud execution environment. This will be further addressed in Section 13.3, which discusses the alignment of the EU initiative on data spaces with the developments on edge and cloud.

8.3. Mobility specific building blocks for data sovereignty and trust

In the context of data sovereignty and trust for the mobility sector, the EMDS should incorporate building blocks that are relevant for personal mobility and logistics.

Specific building blocks for personal mobility

- **Mobile operation of decentralised data sovereignty and trust mechanisms**
  Mobility must always account for non-internet-connected use case scenarios (i.e. train ticket control in rural areas or tunnels). Verification processes for DIDs or VCs need access to information stored in central registries, normally accessible via the internet. When train staff approach passengers they must be able to check the validity of each individual ticket immediately. Lengthy waiting times for a successful reconnect should be avoided as passengers may become impatient or need to disembark at their destinations, potentially

[252] Deutsches Institut für Normung (2019), "DIN SPEC 27070: Reference Architecture for a Security Gateway for Sharing Industry Data and Services", https://www.beuth.de/de/technische-regel/din-spec-27070/319111044.

interrupting the control process. Therefore, mobility use cases may be equipped and maintained with a mobile copy of the central registries providing the relevant information to ensure for seamless mobile operation. This means, all relevant information for validating credentials (e.g. tickets, signatures, etc.) should be available on the mobile device.

- **Integration of popular digital wallets**
  Verifiable Credentials and digital tickets need to be securely stored in digital wallets. Currently, they are often siloed in individual applications. The EMDS shall support the standard wallets (Apple, Google, etc.) allowing users to manage VCs or digital tickets without the need for multiple apps. This will help increase acceptance and enhance user experience, as tickets and other digital tokens will not be scattered across multiple wallet applications.
- **Solutions for conflict and incident management**
  Cross-border multimodal journeys can have multiple legs, with multiple tariffs and tickets, potentially involving different currencies. During a journey, many interruptions can occur such as missed connections, the need to stay overnight, or booking alternative modes of transport to arrive on time. This can result in time-consuming cross-company processes involving cancellations, additional costs, rebates, compensations, root causes, liabilities, and passenger right laws. A common EMDS should consider solutions for such incident and conflict management scenarios, providing a standard and seamless approach, so that users do not have deal with tedious and different processes across different companies involved.

Specific building blocks for logistics

- **Delegation of authorisation (access and usage) rights to third parties**
  In the logistics sector, data consumers often delegate their authorisation rights for accessing and using data to a third party. For example, when authorisations for container data (location, status and availability) are delegated from a shipper to a specific (sub-)transporter. To support delegation, the policy registry building block serves as a registry for formal data sharing policies, containing the specific access and usage conditions for IT resources to be shared. In addition, the policy registry responsible for managing data sharing policies (i.e. access and usage of control policies), must have the capability to function as a delegation registry. This registry allows an authorised data consumer to delegate its access and usage rights to other data space participants. Interviews with experts revealed that the case of delegating authorisations in the logistics domain is a common feature.
- **A policy registry as separate service**
  To support the policy delegation capabilities and create generic, re-usable services for multiple participants in a data space, the associated Policy Administration Point (PAP), the Policy Management Point (PMP) and the Policy Retrieval Point (PRP) of the eXtensible Access Control Markup Language (XACML) standard[253] need to be externalised and accessible through a well-defined API. This approach is commonly used to implement a policy enforcement framework and is also part of the IDSA RAM and the iSHARE Framework.

- **Consent management (for data and data app sharing) by entitled parties**
  Data and application service providers hold data or applications within the data spaces and make them available to other data space participants in a controlled manner. However, they may not always possess the formal rights to share data or applications, as these permissions are held by separate entities known as entitled parties. Entitled parties can, for instance, be the owner of the data or application or the subject to whom the data applies. As such, the entitled party has the right to define policies and conditions for data or application usage.

[253] OASIS (2013), "eXtensible Access Control Markup Language (XACML) Version 3.0", OASIS Standard, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

- **Data sovereignty and trust mechanism to support "event-driven smart contracting for data flow control"**
  This type of data sharing specifically refers to data sharing concepts and architectures that have been developed by the EU CEF FEDeRATED project[254]. These concepts involve advanced (and semantically defined) Identification and Authentication and Authorisation (IAA) protocols implemented between multiple stakeholders to enable the sharing of (potentially sensitive) event data between providers and consumers.[255]
  A stepwise approach may be considered in aligning (integrating) the various capabilities required to support this type of data sharing into the EMDS architecture. This approach should be based on a functional breakdown analysis of IAA-processes embedded in the FEDeRATED (and its decentralised FEDeRATED nodes), as well as the mapping of the generic building blocks for data spaces being developed in Europe.
- **Trusted connectivity layer beneath the network of a digital freight forwarder**
  Digital Freight forwarders, e.g. Sennder, Forto, Yolda, need to establish smart connections with their transport service providers without disclosing their partnerships, their conditions and rates, etc. Transport management systems should include connectors to a common EMDS to establish this layer.
- **Neutral, trusted, data sovereignty-guaranteeing instance**
  In the logistics sector, wasted kilometres as well as empty loading space are a common problem. Better cooperation and coordination between partners in logistics chains offer a significant opportunity to increase optimisation and efficiency, avoiding such scenarios. This form of cooperation (e.g. order pooling, matching and assignment) is dependent on trust and data sovereignty. A common EMDS could provide a framework to facilitate this cooperation. Nevertheless, to ensure effective cooperation and collaboration, the provisioning of data on orders, transport units, vehicles and more, is essential.
- **Fundamental data set for AI-based trust monitoring and application development**
  AI methods depend on the ability to analyse large volumes of data. A common EMDS could establish foundational data sets, which may serve AI methods in several ways. Firstly, it may support AI-based monitoring and improvement of the reliability and trust in the EMDS itself. Secondly, the data set may be used for training AI based value adding services, for which a large volume of representative data for logistics applications could elevate these methods to the next level. Thirdly, it could help to better monitor activities in AI that are enabled by the EMDS.

To support these specific patterns of entitlement, delegation, and authorisation control, it is crucial to incorporate appropriate data sovereignty and trust processes, protocols, and capabilities within the overarching architecture for the EMDS.

[254] EU FEDeRATED project (n.d.), "EU-project for digital cooperation", http://www.federatedplatforms.eu.
[255] EU FEDeRATED project (2022), "FEDeRATED Reference Data Sharing Architecture", forthcoming, http://www.federatedplatforms.eu/index.php/library/item/draft-federated-reference-architecture-document-june-2022.

8.4. Data sovereignty and trust frameworks

The Open DEI initiative[256] identifies the importance of a trust framework, defining it as "a structure that lets individuals and organisations conduct business securely and reliably online". Trust frameworks operate on both the organisational and the technical level of data spaces.

Various trust frameworks have been developed and are considered best practices:

- **Gaia-X trust framework**
  The Gaia-X trust framework[257] includes the concepts of self-description, trust anchors, and trust federation. Trust anchors, as defined in the previous section, are entities endorsed by Gaia-X[258]. These trust anchors are appointed following a formal process based on objective criteria outlined in the Gaia-X certification schema. In addition, the framework addresses trust federation through the federation of trust anchors. A federation of trust anchors can add additional rules by (1) adding more requirements for a participant to join the federation or (2) selecting new domain specific trust anchors based on new criteria.
- **The DSBA trust framework**
  The DSBA proposes a highly decentralised approach to identity management for data spaces, based on the technologies for SSI, VC and DIDs. As previously discussed in this chapter, the DSBA Technical Convergence document also distinguishes between two levels of participation identification: legal identities and data space members. The DSBA proposes the use of a Trusted Participant List, which includes the identities and associated metadata of all legal persons participating in a data space. This list is updated during the onboarding process of an entity and is managed by one or more collaborating trusted participants within the data space. It is important to note that this list is different from the EU Trusted List, which contains the identities of transport service providers authorised to issue digital certificates or seals in the EU.
- **The iSHARE trust framework**
  The iSHARE trust framework for data spaces[259] provides the main trust mechanisms discussed in the previous section. iSHARE has its origins for B2B data sharing in the logistics sector[260] and is broadly applicable as trust framework for other sectors, application areas, and data sharing scenarios within a specific data space and between multiple data spaces. The iSHARE trust framework currently provides capabilities for overarching cooperation agreements and role-specific agreements for mandated compliance with legal, operational, and technical agreements. It offers participant trust registration and administration across data spaces via iSHARE Satellites, which register data space membership, and are federated across data spaces. The framework also includes participant discovery and status information for participant discovery and participant status retrieval across the federation of satellites and data spaces, a policy registry to manage data access or usage rights for data space participants, and functions for delegation of authorisation rights. In addition, it supports data space profile registration for the discovery of data space definitions.

[256] EU Open DEI project (n.d.), "Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry", https://www.opendei.eu.
[257] GAIA-X European Association for Data and Cloud (2022), "Gaia-X Trust Framework", https://gaia-x.gitlab.io/policy-rules-committee/trust-framework.
[258] GAIA-X European Association for Data and Cloud (2022), "Gaia-X Trust Anchors", https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/trust_anchors.
[259] iSHARE Foundation (n.d.), "iSHARE – Trust Framework for Data Spaces", https://ishare.eu.
[260] iSHARE Foundation (n.d.), "For Data Spaces", https://ishare.eu/ishare/benefits/for-data-spaces.

- **The FEDeRATED trust framework**
  To support the event-driven smart contracting for data flow control type of data sharing, the EU CEF FEDeRATED project has developed advanced IAA protocols between multiple stakeholders to enable the sharing of (potentially sensitive) event data between providers and consumers. As such, it develops several of the main trust mechanisms as described in the previous paragraph and could therefore be considered a trust framework. In the implementation of the FEDeRATED conception architecture, it could additionally be considered to include onboarding and certification process as part of trust framework.

8.5. Information security

As previously discussed, data sovereignty and trust include concepts such as data access and usage control as well as truthfulness, quality, accuracy and integrity of the information. Information security is defined as the "preservation of Confidentiality, Integrity and Availability (CIA) of information"[261]. Both concepts are tightly interwoven, and information security is an important aspect to consider when addressing data sovereignty and trust in the context of a data space.

- **Confidentiality** ensures that the data is not shared with entities other than those who have been granted access rights to it. Data shared in data space may include e.g. data which is protected under GDPR or other non-public data with access restrictions set by data providers or regulations. Hence, data space participants need to be able to ensure data confidentiality within a data space.
- **Integrity** ensures that data is accurate and complete, it is not modified, added or deleted unintentionally or by unauthorised party. This is important because the value of data depends on its accuracy, completeness and truthfulness. Data becomes untrustworthy and loses its value if it does not meet these requirements adequately.
- **Availability** ensures that authorised users can access data whenever and wherever required. The significance of this aspect is closely linked to the data's intrinsic value; data that exists but is not fully accessible loses its worth. One of the primary benefits of establishing a data space is to enhance data availability.

By addressing **information security** at each level of the data space, **trust can be established and data sovereignty can be preserved** in the data space. Therefore, it is important to recognise that the confidentiality aspects of information security require the implementation of various data sovereignty and trust mechanisms, as described in Section 8.2, as building block in the EMDS, such as on identity management and authorisation. As these mechanisms are mostly generic in nature, applicable to many of the sectoral data space initiatives, it is recommended for mobility data initiatives to align with and adhere to the trust mechanisms that will be developed generically across the sectoral data spaces. However, the **integrity and availability** aspects of information security are primarily the responsibility of the data space participants. They collect and share the data and must take the lead in adhering to policies that ensure the integrity and the availability of their data. This **cannot be technically enforced** by the EMDS but should be integrated into the use cases and governance framework for the EMDS. Nevertheless, data integrity and availability capabilities can potentially be supported by means of "generic" applications that may be shared as data apps (in an app store) within and across data spaces. In fact, supporting the evolution of data quality standards is considered a value proposition of a data space by potential participants (e.g. Chapter 2).

For ensuring data confidentiality, integrity and availability, access control plays a key role. Furthermore, for effective access control, a reliable identity management system with certification

[261] ISO/IEC (2018), "27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary", https://www.iso.org/standard/73906.html.

needs to be in place. To ensure data confidentiality, encryption should be implemented and used during data exchange, and it may also be used when storing highly confidential data. Data integrity and availability can be enhanced by performing data backups and implementing backup services to protect against unexpected events such as power outages and malicious attacks. As discussed above, ensuring the integrity during data storage, is primarily the responsibility of EMDS participants, as they are the ones actually storing the data.

There are many different approaches to the use of digital identities in data spaces. A common approach is the use of digital certificates under the eIDAS regulation. Digital certificates are issued by Certification Authorities (CAs), which ensure that the identity of the certificate holder is valid. Such certificates may use PKI, in communication with other parties. For example, a file may be electronically signed using a private key of a digital certificate, to create an Electronic Seal (eSEAL) for the file's content. When a file is electronically signed using the private key of a digital certificate, it generates an eSEAL that serves a dual purpose. Firstly, the electronic seal guarantees the integrity of the exchanged files by ensuring they remain unaltered and not been tampered with during transit. Secondly, the recipient's public key comes into play as it authenticates the identity of the sender, providing a secure and reliable way to verify that the file indeed originated from the claimed source. The mechanisms of digital eIDAS certificates, which build upon PKI, ensure the identity, and authenticity of parties and their web applications in digital communication and exchange.

It is vital that information security is considered across the entire set of operations within data spaces. Because of the nature of information security, one weak point that is not carefully addressed can have significant negative effects on information security across data space. Each participant needs to have sufficient information security practices in place for the data they are handling, and the security of data exchange needs to be similarly ensured. The role of EMDS here is to provide identification, authentication and authorisation mechanisms that are accessible across the data space for participants. The EMDS should also establish a **governance for data integrity and availability** so that trust is established between participants that data is accurate and accessible.

From the questionnaires conducted it can be identified that authentication was used by 89% of the respondents, while authorisation was used by 72%. Also, data access and/or usage policies applied to 89% of the respondents. Some NAPs were the only organisations that did not require authentication.

During the interviews conducted, when participants were asked about which of the three attributes of confidentiality, integrity and availability is most important, two different answers were identified based on the type of data. When sharing non-confidential public data accessible to everyone, data integrity is the most important of the three. However, when sharing data with confidential information and access policies in place, it is not possible to prioritise one of the three attributes over others. This is because if either confidentiality, integrity or availability of the data is compromised, the other two attributes provide no additional value as information security is already compromised.

For data available without authentication, Denial-of-Service (DoS) attacks were identified in the interviews as a potential risk to information security. Additionally, poor implementations of data consumers' software for collecting data from providers may lead to unnecessarily high usage for open data services. Both of these challenges could be avoided by implementing an authentication system for accessing data.

8.6. Recommendations

Conclusion

Data sovereignty and trust are fundamental for enabling data sharing in data spaces, both within and across data spaces. Data sovereignty is the concept of retaining authority and control over one's data, empowering individuals or organisations to determine who can access their data and for what purposes. Trust establishes confidence in the truthfulness of the shared data. As such, trust includes both capabilities for data sovereignty and for information security, assuring accuracy and integrity of the shared data.

Although various trust mechanisms are available, there is no single trust mechanism that fits the diverse goals of data sharing in mobility data spaces. Multiple trust mechanisms need to be supported within the EMDS.

Various trust frameworks are being developed under Gaia-X, SIMPL, DSBA, iSHARE, and more. **Data sovereignty and trust require an aligned approach** to enable interoperable data spaces, implying that, by default and wherever possible, the trust mechanisms for a mobility data space should align with the common approach and building blocks being generically developed across data spaces, for example, as part of the DSSC blueprint. For the development of trust building blocks for the EMDS, only those aspects and features that may be mobility specific should be included as additional input for the DSSC blueprint development or integrated as specific feature within the EMDS.

Recommendations

Align with and adhere to generic data space blueprints and capabilities developed at EU level

Mobility and logistics are cross-border and cross-sector by nature, requiring interoperability not only between geographical mobility data space initiatives but also with other sectoral data space initiatives. Therefore, data sources in the mobility and adjacent data space instances should be made mutually accessible, making data space interoperability a key aspect for realising the ambition of the common European data spaces. Aligning with EU-level data space blueprints and generic building blocks (e.g., DSSC, SIMPL, EDIB) is crucial for EMDS to ensure interoperability with adjacent data spaces.

This particularly applies to the development and deployment of data sovereignty and trust mechanisms within the EMDS. These mechanisms are mostly generic in nature and can be similarly applied to many of the sectoral data space initiatives. Therefore, it is recommended to develop and adopt mobility data space capabilities for data sovereignty and trust, where possible, using building blocks that are generically applicable within and across the sectoral data spaces.

This also applies specifically to the definition and enforcement of authorisation policies for data sharing, for which multiple approaches exist. Harmonising these policies across data spaces is key for ensuring their interoperability. Hence, where possible, align with and adhere to the synergetic authorisation processes that will be developed generically across sectoral data spaces.

Support fully decentralised data sovereignty and trust mechanisms by design

The (inter-)national environment of federated data sharing and data spaces is still in development. The main European reference architecture initiatives on federated data sharing and data spaces (Gaia-X, iSHARE, DSBA, SIMPL, FEDeRATED, etc.) are moving towards fully decentralised architectures. This also applies to the associated trust mechanisms, e.g. identity management, authorisation, contract negotiation and usage control. Hence, this fully decentralised approach should be considered right from the outset in the development and deployment of the EMDS.

Take the lead in developing the data sovereignty and trust mechanisms that are of specific relevance to mobility, but may nevertheless be developed as generic capabilities

There are various data sovereignty and trust capabilities that are relevant to the mobility sector and, as such, should be part of the architecture. The EMDS should take the lead in developing these capabilities. Nevertheless, it is worth noting that these capabilities may not be unique to the mobility sector but have yet to gain significant attention in other sectoral data spaces, despite their potential value. It is recommended that the EMDS takes the lead in developing and deploying common data sovereignty and trust mechanisms. This should be undertaken in close alignment with the EU initiatives that are developing generic capabilities such as DSSC, SIMPL, and others. This approach will help determine which capabilities can be developed in a generic way for use by other sectoral data spaces as well. These recommendations also apply, for instance, to the capabilities described in 8.3.

Design the policy registry to support delegation of authorisation rights

Particularly in logistics, it is quite common that a data consumer delegates its authorisation rights for accessing and using data to a third party. The policy registry is the building block responsible for managing formal data sharing policies, containing the access and usage conditions for IT resources to be shared. The policy registry should also function as a delegation registry, allowing an authorised data consumer to delegate their access and usage rights to other data space participants. This process should include the use of ODRL for defining authorisation policies.

Enable consent management for entitled parties

Data and application services providers who store data or applications in a data space may not have the formal authority to grant consent to share this data or applications. Therefore, consent management processes, which enable entitled parties to give consent to data and application service providers to share “their” data or applications, comprise a key data sovereignty mechanism to support in mobility data spaces. These consent management processes are expected to be generic in nature and applicable across many sectoral data space initiatives. It is recommended, where feasible, to align with and adhere to the consent management processes that are being developed generically across the sectoral data spaces.

Enable FEDeRATED Identification, Authentication and Authorisation (IAA) mechanisms

The EU CEF FEDeRATED action has developed an advanced, semantically defined, architecture for sharing (potentially sensitive) event data. It is adopted by the DTLF as main means of data sharing in the logistics sector, but it may also find applicability in personal mobility and other sectors. It embeds data sovereignty and trust capabilities specifically related to identity management and authorisations. These capabilities should be considered in the overarching architecture of the EMDS.

Support multiple approaches for agreement on authorisation policies

For the EMDS, it is important to support various types of data sharing, each with its own associated usage and interaction patterns. These include bilateral (point-to-point) for persistent data and multilateral (point-to-multipoint) for streaming data. This diversity in usage and interaction patterns also implies that a one-size-fits-all mechanism for agreeing on authorisation policies is not feasible for all use cases. Hence, the EMDS should support multiple approaches such as overarching contracts, authorisation licenses and bilateral contract negotiation.

Ensure the confidentiality aspects of information security via data sovereignty and trust building blocks

The confidentiality aspect of information security requires that various data sovereignty and trust mechanisms be implemented as building block in the EMDS, including identity management and

encryption by data space connectors for data transfer. To ensure interoperability between data spaces, these mechanisms should be provided in a generic manner, making them applicable to many sectoral data space initiatives. Therefore, it is recommended for the mobility data sector, where possible, to align with and adhere to the synergetic trust mechanisms that will be developed generically across the sectoral data spaces.

Include the data integrity and availability aspect of information security into the governance framework of the EMDS

Data integrity and data availability cannot be enforced solely by the technical infrastructure of the data space. Therefore, it is proposed to include these in the EMDS governance framework, to be agreed upon and supported by the data space participants as part of the set of agreements under the data space authority. It is worth noting that monitoring information integrity and availability can potentially be supported by generic applications that can be shared as data apps (in an app store) both within and across data spaces. This may be considered as value adding trust proposition for a data space.

Include solutions for conflict or incident management

Cross-border multimodal journeys can involve multiple legs, with various tariffs and tickets, potentially in different currencies. During a journey, many interruptions can occur such as missed connections, overnight stays, or the need to book alternative modes of transport to arrive on time. This can result in time-consuming cross-company processes related to cancellations, rebates, compensations, identifying root causes, liabilities and complying with passenger right laws. To facilitate participation in the EMDS, solutions for managing such incident scenarios should be considered and provided.

Ensure mobile operation of decentralised data sovereignty and trust mechanisms

Since mobility use case scenarios frequently involve non-internet-connected scenarios, such as rural areas or on-the-move situations, verification processes, for example for identities, must account for situations where accessing information from central registries via the Internet is not possible. Therefore, decentralised and autonomous operations processes should be supported for mobile situations. One solution is to provide up-to-date distributed copy of central registries containing relevant information on mobile devices.

Ensure integration with popular digital wallets

To ensure the security of Verifiable Credentials and digital tickets, safe digital wallets are essential. Preferably, these should not be siloed within individual applications, which would inconvenience users by forcing them to install and manage multiple apps. Instead, integrating them with standard wallets (Apple, Google, etc.) can prevent scattering of tickets and other digital tokens across multiple wallet applications, and increase acceptance rates and user experience.

8.7. Building blocks

Figure 27 shows the individual building blocks recommended for data sovereignty and trust.

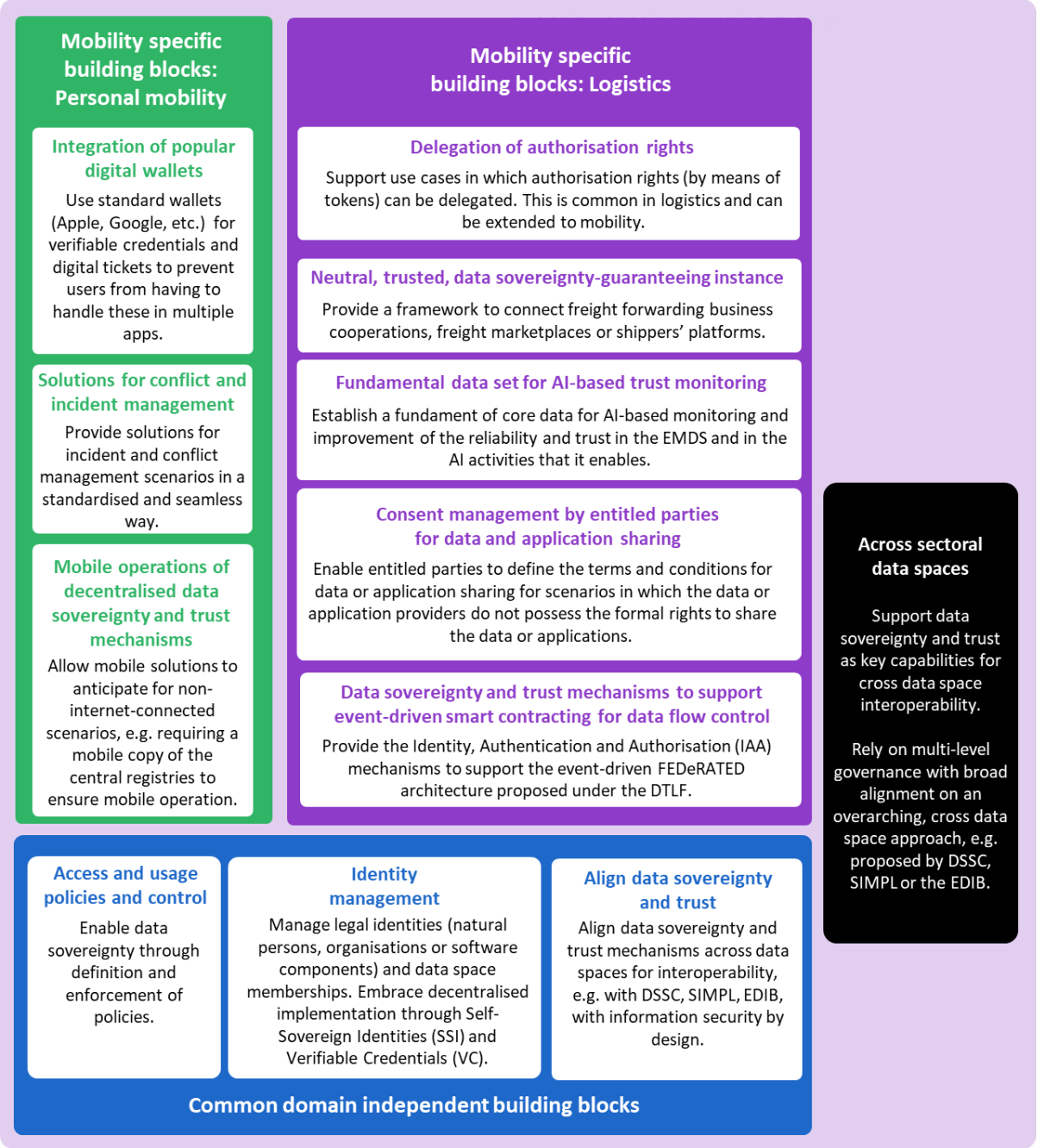


Figure 27: Building blocks for data sovereignty and trust.

9. Data value creation

9.1. Introduction

To generate value, participants in the EMDS should have the capability to share IT resources provided by its participants to enable the creation of multi-sided markets. This requires a standardised method for describing the IT resources within data spaces, specifying their associated terms and conditions (potentially including pricing), and enabling publication, discovery and accessibility. Moreover, ensuring accountability for contracts and data sharing transactions[262] is essential.

The DSSC taxonomy's data value creation pillar and its building blocks (Figure 2) address the necessary capabilities for describing, publishing, discovering, accessing, and ensuring accountability of data space IT resources.

The data value creation building blocks as outlined in the DSSC taxonomy include:

- **Data, services and offerings**
  Providing a meta-model of data, services, and offerings within a data space. It should enable participants in a data space to discover and select suitable data services and IT resources.
- **Publication and discovery**
  Enabling data space participants to publish data services and IT resources in a catalogue and enable other participants of the data space to discover and access them.
- **Marketplaces and usage accounting**
  Addressing the common mechanisms for establishing marketplaces of data and services along with the related usage accounting (e.g. for billing), to support the creation of multi-sided markets where participants generate (monetary) value from sharing data.

As highlighted in the previous chapters, it is essential for the EMDS to **build upon the common technical grounding,** particularly in terms of the capabilities for **discoverability** of data space IT resources. These capabilities are being assessed and developed under DSSC and SIMPL and play a crucial role in achieving interoperability within and across the EU's sectoral data spaces. Hence, wherever possible, it is the default approach for the EMDS to align, harmonise, and adopt the building blocks for discoverability of data space IT resources capabilities being developed by these overarching EU initiatives (Section 6.2). In addition, the EMDS faces additional requirements for mobility specific data value creation building blocks.

The following Sections 9.2, 9.3 and 9.4 address the three data value creation building blocks from this perspective. They address the generic approach for their development, augmented with mobility specific capabilities where necessary. Subsequently, Section 9.5 describes additional mobility specific building blocks for both personal mobility and for logistics. The final Section 9.6 provides an overarching conclusion, lists the recommendations, and outlines the recommended EMDS building blocks for data value creation.

9.2. Data, services and offerings descriptions

The development of the DSSC blueprint and its scope definition of IT resources is in its initial stages. This chapter builds upon this initial work, and driven by the expected relevance for the EMDS, this chapter considers the following three types of IT resource sharing to be part of the EMDS:

[262] Data Spaces Support Centre (2023), "DSSC Blueprint for Data spaces - Taxonomy of building blocks", forthcoming.

- **Data sharing**
  As previously addressed in Section 2.2, **four types of data sharing need to be supported** in mobility data spaces: (1) persistent, static or semi-static data, (2) real-time streaming data, (3) algorithms for local processing of (sensitive) data and (4) Event-driven smart contracting for data flow control.
  The first two of these data sharing types are considered "generic and traditional", involving the sharing of potentially sensitive data between data space participants. The DSSC technical grounding work is expected to develop a common implementation approach across data space instances. Special emphasis should be placed on types 3 and 4 as their relevance for the EMDS is expected to grow rapidly.
- **Application sharing**
  Applications may be shared for local access and processing of (sensitive) data within the security domain of a data provider or consumer. In Chapter 2, various types of usage scenarios for the mobility sector have been described, including:
  - To support Privacy Enhancing Technologies (PETs);
  - To support data pre-processing;
  - To support digital twin platforms.
- **Semantic model sharing**
  At the semantic level, common semantic models (e.g. common domain-specific information models) used by both data service providers and consumers offer significant advantages in minimising complexity for interconnection and collaboration. The variety of platforms, standards, models and frameworks in the application domains in mobility and logistics, as addressed in Chapter 7 on data interoperability, shows that attaining a **universal set of semantic models is challenging.** Reaching an agreed-upon set of universally used semantic models may seem challenging or even unattainable for the EMDS in its role of interconnecting the data provided through these platforms. Moreover, the EMDS, as a European initiative, is also to be embedded in the broader context, with globally operating organisations, platforms and interconnections. Take for example the multi-modal mobility data landscape. A distinction can be made between global (e.g. GBFS, MDS and GTFS) and European standard specifications (Datex II, SIRI, OJP, CDS-M & NeTEx), both of which have different application implementations and are used differently by stakeholders.

Therefore, **capabilities for semantic management need to be supported** in the EMDS. This basis is formed between a set of semantic models and mappings (referred to as the vocabulary hub in the IDSA RAM). These capabilities enable the actual configuration and execution of transformations on data shared within the data space.

The data value creation building blocks for sharing these three types of IT resources allow the mobility data space to expand its available capabilities and supported services, accommodating a growing number and diversity of use cases. Each type of IT resource sharing has its own specific requirements and considerations for the associated catalogues, publication and discovery and will be subsequently addressed in the following section.

9.3. Publication and discovery: catalogue architectures

One of the most important building blocks for a data platform is a catalogue that enhances the **discoverability of available IT resources**, representing the "Findability" in FAIR data[263]. Thus, the significance of the publication and discovery building block cannot be overstated, as it serves as the gateway for consumers and users to locate the IT resources they require before effective sharing can take place.

The following paragraphs in this section address two key aspects of the publication and discovery building block: catalogue architectures to support the sharing of three types of IT resources – data, applications, and semantic models.

Data sharing

Various initiatives have defined the scope and the capabilities of a catalogue for sharing data. The European Telecommunications Standards Institute (ETSI) describes in their white paper on context information the role of a catalogue as "To produce, interpret and exchange data, applications need to unambiguously define the data used and to share those definitions with other applications. The data relevant to a service, and the definitions that describe its format and meaning, can be called the context of the service. For example, location, time, temperature, and application-specific information must have common definitions and be understood by all the applications which manipulate it."[264] The Open DEI refers to the metadata and discovery protocol building block, stating "This building block includes publishing and discovery mechanisms for data resources and services, using common descriptions of resources, services, and participants. Such descriptions can be both domain-independent and domain-specific. They should be enabled by semantic web technologies and include linked data principles[265]. This building block enables the publication of offerings that focus on data resources and services and use common descriptions of resources, services, and participants."[266] The current version of the DSSC Taxonomy (Figure 2) offers only a brief description of a catalogue as part of the publication and discovery building block, mainly serving the purpose of publishing self-descriptions.

In parallel, various reference architectures have been developed for implementing the catalogue:

- The CEF (the CEF Digital programme 2014-2020 has concluded) used the **FIWARE Context Broker**, a core component of the FIWARE Platform, as a CEF Building Block[267].
- The IDSA has defined the **IDS Metadata Broker** building block[268] [269] as a service for publishing and searching metadata of connectors and resources between IDS-based data space

[263] Wilkinson, M. et al. (2016), "The FAIR Guiding Principles for scientific data management and stewardship", Sci Data 3, 160018.
[264] European Telecommunications Standards Institute (2019), "NGSI-LD API: for Context Information Management (ETSI White Paper No. 31)", https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp31_NGSI_API.pdf.
[265] For instance, Belgium develops a set of local standards for linked data/linking organisation (including the Linked Data Event Streams [LDES] Application Profile) for the SOLID architecture as part of the "Open Standaarden voor Linkende Organisaties (OSLO)" initiative of the Flemish government. https://data.vlaanderen.be/standaarden/erkende-standaard/applicatieprofiel-ldes.html.
[266] EU Open DEI project (2021), "Design Principles for Data Spaces. Position Paper", https://design-principles-for-data-spaces.org.
[267] FIWARE Foundation (2018), "FIWARE Context Broker Launches as a CEF Building Block", https://www.fiware.org/2018/08/08/fiware-context-broker-launches-as-a-cef-building-block.
[268] International Data Spaces Association (2022), "International Data Spaces: Reference Architecture Model Version 4", https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0.
[269] International Data Spaces Association (2022), "IDS Metadata Broker Core", https://github.com/International-Data-Spaces-Association/metadata-broker-open-core.

participants. The IDS Metadata Broker provides a collection of additional functionalities, including indexing services in order to respond to queries.

- **Gaia-X** uses a **Federated Catalogue** constituting "an indexed repository of Gaia-X Self-Descriptions to enable the discovery and selection of Providers and their Service Offerings. The Self-Descriptions are the properties and Claims of Participants and Resources, representing key elements of transparency and trust in Gaia-X."[270]
- It should be noted that **open data catalogues,** including government portals, have been widely available and operational for some time now, with many of these powered by the Comprehensive Knowledge Archive Network[271] (CKAN). However, the data spaces discussed here encompass data exchanges involving not only open data, hence requiring broader capabilities.

In both the IDSA and the Gaia-X approaches, search and discovery rely on self-descriptions. For example, "Gaia-X Self-Descriptions (SD) describe Entities from the Gaia-X Conceptual Model in a machine interpretable format. This includes **Self-Descriptions** for the participants themselves, as well as the Resources and Service Offerings from the Providers. Well-defined Self-Description Schemas (which can be extended by the Federations for their domain) help ensure a unified representation of the Self-Descriptions. The Self-Description allows finding and comparing Entities inside Gaia-X." Similarly, in IDS "A Self-Description encapsulates information about the IDS Connector itself as well as its capabilities and characteristics. This Self-Description contains information about offered interfaces, component ownership, and metadata of the data offered, such as attached policies (e.g. data usage control), commercial terms (for marketplace activities and closed data), data provenance, and quality. All these details are reflected in the self-descriptions."[272]

The operator of the connector (the data provider) provides a self-description, which (in its entirety) can be regarded as metadata and may be stored either locally in the connector's catalogue, or in one or more (federated) catalogues within the data space. **Self-descriptions are therefore a crucial component of a data space**: they provide a meta-model of data, services and offerings in a data space. This allows participants in a data space to **find and select suitable services**. A metadata model should be linked to elements in other building blocks including identities and semantics in specific domains. Self-descriptions can also **link usage policies, provenance details, technical descriptions** (e.g. the data schema, API specifications) and content-related descriptions. Once individual self-descriptions have been created, they should be **publishable in a catalogue,** enabling other data space participants to **find them**.

In the context of the EMDS, it is preferable to use a harmonised metadata broker that supports each of the four types of data sharing described in Chapter 2.

To support **Algorithm sharing for local processing of (sensitive) data**, metadata brokering capabilities are required to describe, publish and discover data processing components, such as data apps. The role and relevance of this type of data sharing, for example, to enable local pre-processing of data, to support PETs and digital twins, has also been recognised by the EU SIMPL procurement project. It distinguishes both a data sharing and a data app sharing component in its envisaged reference architecture, as will be further described in the following subsection.

---

[270] EU Gaia-X Initiative (2022), "Gaia-X. Architecture Document. 22.04 Release", https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf.
[271] Comprehensive Knowledge Archive Network (n.d.), https://ckan.org.
[272] International Data Spaces Association (2022), "International Data Spaces: Reference Architecture Model Version 4 - Metadata Broker", https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_4_metadata_broker.

To support the type of data sharing **Event-driven smart contracting for data flow control**, the Index and the Service Registry in the FEDeRATED architecture need to be analysed to explore alignment options with the generic metadata brokering capabilities under consideration in the DSSC blueprint. The FEDeRATED Service Registry is a registration component that identifies end-user endpoints in the FEDeRATED architecture, possibly with reference to a platform if that endpoint is implemented by a platform. The FEDeRATED Index is a component that enables enterprises to specify which data sets and links are shared as open and linked data, i.e. it stores linked data and enables a triple store to implement the complete FEDeRATED semantic model. By including the Service Registry and the Index functions in the local metadata brokering capabilities of the data space connector, they can be more easily accessible for **various data spaces**, including those related to personal mobility. A functional breakdown analysis of the Service Registry and the Index functions may provide additional insight into:

- How their individual functions can be taken into account by the related DSSC Expert Groups;
- What protocols are needed to be able to implement them in an interoperable, decentralised manner reflecting the decentralised FEDeRATED nodes approach, e.g. as input for the further development of the Dataspace Protocol.

Application sharing

The EMDS will require capabilities to support the execution of applications (data apps) using data provided by a data provider or used by a data consumer as input. This will be the case, for instance, to support the data sharing typology referred to as **(3) Algorithm sharing for local processing of (sensitive) data** (Chapter 2). Compute-to-data enables avoiding the exchange of the actual data. Instead, it involves the exchange of the required algorithm for the desired data analytics, allowing the consumer to apply the analytics on their side without the need to physically transfer the data. Similarly, this concept will apply to the semantic support building blocks (as will be addressed in a following paragraph in this section) and for tasks such as data quality management, data pre-processing, and data cleaning data apps.

The **IDSA** role model includes roles to support a catalogue of data apps (the **app store**) and an IDS connector architecture with capabilities for data processing at the connector. The Gaia-X architecture and the **Gaia-X Federation Services**[273] do not distinguish a separate app store building block.

The **EC SIMPL project**[274], focused on open source development of smart middleware components, distinguishes in its architecture vision document building blocks for both data sharing and application for sharing. As with IDSA, there is a recognition that not only should data be shared, but also smart services or applications: SIMPL contains "the building blocks required for providers and consumers to **exchange both data and applications**." Both concepts are closely linked.[275] Therefore, under SIMPL, the data services component contains separate blocks for data discovery and application discovery, data metadata description and application metadata description, etc.

The **DSBA,** in its recently published version 2.0 of the Technical Convergence document[276], proposes an approach of a "**Decentralised Open Marketplace Ecosystem (DOME)**" based on the federation of marketplaces. All of these marketplaces are connected to a commonly shared digital catalogue of

[273] Gaia-X Federation Services (n.d.), "Gaia-X Federation Services - GXFS", https://www.gxfs.eu/specifications.
[274] European Commission (2023), "SIMPL: cloud-to-edge federations and data spaces made simple", https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple.
[275] European Commission (2022), "SIMPL: Preparatory work in view of the procurement of an open source cloud-to-edge middleware platform - Architecture Vision", Version 4.0, https://ec.europa.eu/newsroom/dae/redirection/document/86241.
[276] Data Space Business Alliance (2023), "Technical Convergence Discussion Document", Version 2.0, https://data-spaces-business-alliance.eu/dsba-releases-technical-convergence-discussion-document.

cloud and edge services and service offering descriptions, which can be further classified as (1) data services, providing access to data, (2) application (app) services, which gather and process data, and typically deliver data results and (3) cloud or edge infrastructure services, supporting the deployment and execution of data/app services. As such, the DSBA also supports the notion of data service and data app/processing to be provided as part of the envisioned data space architecture.

A further, practical example of an **operational platform** that already offers algorithm sharing is the Ocean Protocol. As part of its **Ocean Market**, it offers not only **data sets** but also **algorithms**[277].

From a capability perspective, the data space environment in the EMDS should provide features to catalogue, discover and share data apps (further referred to as "App Store") and securely deploy them in an orchestrated environment (referred to as "App Workflow Management").

App store

The app store contains all resources required to describe, expose, discover, retrieve, and deploy data apps. Within the app store, **deployable data apps are stored** for retrieval by data space participants. On the other hand, the data space metadata broker can hold descriptions of the deployed (instantiated) data apps, providing essential information about their functionalities and availability.

The app store includes a registry containing formal descriptions of available data apps, in which data apps may, for instance, be represented as web services in Open Container Initiative (OCI)-compliant images (e.g. Docker images). OCI images adhere to open source and widely adopted industry standards. To support the app store, an OCI-compliant image registry is utilised to house all versions of the data apps, while a metadata store is employed to store the semantic self-descriptions of these data apps.

The app store serves as a platform for uploading new data apps and enables retrieval and deployment of data apps when queried or requested by a data space participant. Data apps registered in the app store must be accompanied by a sufficiently unique self-description and suitable access and usage policies. The app store is responsible for providing all available versions of the data apps. Additionally, policies may be enabled to allow filtered access for uploading data apps, allowing the deployment of certified data apps by any security gateway, or restricting access to certain data apps to a select group of users.

App workflow management

As apps may require data input from other apps, a form of **app orchestration capability** is needed. This capability enables the configuration and forwarding of input and output data flows between data apps. To avoid unwanted app interaction, shielding is implemented through the use of software containers. Furthermore, the data processing capability should be scalable, for example, by distributing multiple instances of the apps on multiple servers and splitting data in multiple streams or by using a (trusted) cloud environment. Given that the software modules deployed will be containerised, standard Docker Engine APIs are needed to deploy and execute containers.

The IDS-connector architecture includes the **Application Container Management** capability, which is used for extended control over the deployment and execution of data apps and containers. A complete workflow or set of workflows of data apps on one or multiple connectors can be seen as "Data Analytics Engine" as mentioned in Open DEI position paper[278]. Gaia-X uses the concept of

[277] Ocean Market (n.d.), "Algorithms", https://market.oceanprotocol.com/search?sort=nft.created&sortOrder=desc&serviceType=algorithm.
[278] EU Open DEI project (2021), "Design Principles for Data Spaces. Position Paper", https://design-principles-for-data-spaces.org.

computational resources which can be used to perform data app and security gateway deployment and processing tasks. The Gaia-X Federated Catalogue will include these computational resources and processing environments. This includes a metadata model to define and describe these resources, e.g. on computing capacity, location, costs, etc. The Federated Catalogue could also indicate security levels of the provided computational resources, which can for example, be used to determine if computational resources are adequate to deploy a specific security gateway handling sensitive data. The development of the Application Container Management capability is still in its initial stages, but is highly relevant for the EMDS, in particular to support the data sharing type (3) "Algorithm sharing for local processing of (sensitive) data" as described in Section 2.2. It is also important in view of the more integrated development of the data spaces and cloud infrastructures (e.g. through the EDC) as addressed in Section 6.5.

Similarly, the SIMPL initiative identifies and describes the "infrastructure discovery" capability in its architecture document allowing infrastructure services (including cloud and edge computing services) to be discovered within a data space, in addition to data and application services.

Semantic model sharing

At the semantic level, common semantic models (e.g. common domain-specific information models) used by data service providers and consumers offer significant advantages in minimising complexity for interconnection and collaboration. The diversity of semantic models used in mobility has been addressed in Chapter 2 and in Chapter 7, with insights into the strategies and considerations related to achieving seamless data integration and harmonisation across diverse semantic representations. However, reaching an agreed-upon set of universally used semantic models may seem challenging or even unattainable. As a result, **capabilities for semantic management** need to be supported in the (EMDS) data space architecture as part of the "Publication and discovery" capabilities. This is further elaborated below.

The IDSA identifies the need, role and capabilities for semantic management under the generic terminology of "Vocabulary Hub" in its IDSA RAM (Reference Architecture Model)[279] [280]. In the context of Gaia-X, the vocabulary hub is part of the Gaia-X Federated Catalogue and contributes to a Gaia-X node's self-description capabilities.

Under the generic terminology of a vocabulary hub, the EMDS requires a set of three consistent and aligned semantic building blocks:

- **Vocabulary hub:** a registry service providing facilities for publishing, editing, browsing and maintaining vocabularies and related documentation. These vocabularies include ontologies, reference data models, schema specifications, mappings and API specifications that can be used to annotate and describe data sets and data services. The vocabulary hub can mirror a set of third party vocabularies to ensure availability and resolution.
- **Semantic transformation engine:** provides semantic transformation services between data formats. It uses vocabularies and mapping specifications as provided by the vocabulary hub. The component can be integrated at the data consumer or data provider's implementation or offered as a service in a data space.
- **Data space connector semantics configurator**: enables data space participants to use vocabularies to configure the semantic interoperability of data space connector implementations. This primarily involves creating ontology-based API specifications to specify

[279] International Data Spaces Association (2019), "International Data Spaces: Reference Architecture Model", Version 3, https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf.
[280] International Data Spaces Association (2022), "International Data Spaces: Reference Architecture Model", Version 4, https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0.

the semantic interface between data provider and data consumer. Additionally, the data space connector configurator can assist in creating mapping specifications if needed. These can be used in the semantic transformation engine.

Federation of catalogues

A federated catalogue is a type of IT resource (including data, applications and semantic models) catalogue that allows discovery and access to metadata about data assets from different sources, without having to move or copy the data. A federated catalogue helps to reduce data silos and improve collaboration across different subdivisions or subsidiaries within an organisation. A federated catalogue can also help to control access to data using the source data access and control policies, ensuring that metadata can be shared without compromising data security. The Gaia-X Architecture document outlines the Federated Catalogue as follows:

"The goal of the Federated Catalogue is to:

- Enable consumers to find best-matching offerings and to monitor for relevant changes in these offerings
- Enable producers to promote their offerings while keeping full control of the level of visibility and privacy of their offerings.
- Avoid a gravity effect with a lock-out and lock-in effect around a handful of catalogue instances."

Several domain-specific implementations of metadata/context brokers are already being deployed. For example:

- The CEF programme and the i4Trust initiative use the **FIWARE Context Broker** as metadata/context broker building block, with several use cases in the logistics domain. It is based on the ETSI NGSI-LD standard[281]. The NGSI-LD (Next Generation Service Interfaces-Linked Data), a continuation of FIWARE's NGSIv2, is now a core piece of ETSI's Context Information Management (CIM) and has been standardised by its CIM Industry Specification Group (ISG). Furthermore, the EU has named ETSI NGSI-LD (as well as DCAT) as a candidate for standardisation of open data portals[282]. The importance of this standard cannot be overstated as it provides the foundations for data discovery and has been used in numerous projects in the EU, such as CEF, Living-in.eu and Fed4IoT, as well as the OASC Context Broker MIM described later. This standard consists of an information model and an API and facilitates the publishing, querying and subscribing to context information (i.e., metadata). Because of its wide adoption in a variety of domains (smart cities, smart agriculture, smart industry, to name a few) it is also a prime candidate for the federated catalogue function of a mobility data space.
- In the mobility sector, the **NAPs are essentially open data exchanges** primarily focused on public transit, traffic, infrastructure, safety, etc. Recently, many more data sets with a wider variety have been added, including 17 data sets on car sharing. Mobilithek[283], Germany's NAP, already offers numerous data sets and functions as an open data portal, designed for discovery and search along multiple dimensions. This building block perfectly embodies the required functionality, with the addition of features such as usage control (data sovereignty), trust, etc., needed for data that is not necessarily open. Their vision is closely aligned with the

[281] European Telecommunications Standards Institute (2023), "Context Information Management (CIM); NGSI-LD AP.", https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.07.01_60/gs_CIM009v010701p.pdf.
[282] European Commission (2021), "Big Data, Open Data and Public Sector Information", https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/big-data-open-data-and-public-sector-information.
[283] Mobilithek (n.d.), "What is Mobilithek?", https://mobilithek.info.

MDS, providing additional functions: "As a National Access Point, the Mobilithek will play a central role within a comprehensive mobility data ecosystem. As a cloud-based infrastructure with a web portal, high-performance support for exchanging real-time data, and a digital space for developing data-based apps, it will cooperate closely with the MDS, which is also currently being developed, and interconnect and exchange data with it. The vision in Germany is to have one central, searchable data space where all mobility related data – open and closed – are accessible and guarantee the inclusion of other building blocks."[284]

- The **OASC**[285] champions the **MIMs**. MIMs are a practical set of capabilities built on open technical specifications that enable cities and communities to replicate and scale solutions on a global scale. The OASC MIM1 is Context[286]. It is based on ETSI NGSI-LD and refers to a number of reference implementations for the context broker. While OASC has a smart city focus, mobility is implicitly included.

Despite initial implementations, the metadata/context broker capability needs further development in a mobility environment. To achieve seamless interconnection and interoperability, a metadata/context broker consolidation or interoperability strategy is crucial for the further development of the EMDS and other sectoral data spaces.

The role and positioning of the existing ETSI NGSI-LD[287] standard and the emerging **Dataspace Protocol**[288] should be considered and assessed as part of the interoperability strategy. The current version of the Dataspace Protocol specifies **DCAT-AP**[289] for interconnecting the cataloguing capabilities of data services offered by connectors and proposes to use ODRL[290] to describe usage control policies that are key for ensuring data sovereignty.

9.4. Marketplaces and usage accounting

Data spaces can support the creation of multi-sided markets, allowing participants to generate (monetary) value from sharing data. This building block describes the common mechanisms for establishing marketplaces of data and the related usage accounting including billing processes.

Marketplace services

Data spaces, by their very nature and definition, serve as platforms for data exchange. However, when a commercial component is introduced, they evolve into marketplaces, incorporating all the implications and characteristics typical for such environments. Until a few years ago, long after the realisation of concepts like "Data is the new oil" or "Data is the new gold", there was an expectation that data might not or could not be monetised. This is mostly no longer the case, as there is now a widespread understanding that while many data sets, related services and applications remain open

[284] Mobilithek (n.d.), "Mobilithek. Germany's data platform that gets you moving", https://bmdv.bund.de/EN/Topics/Digital-Matters/Mobilithek/mobilithek.html.
[285] Open & Agile Smart Cities (n.d.), "Welcome to Open & Agile Smart Cities, or OASC for short", https://oascities.org.
[286] Open & Agile Smart Cities (2022), "OASC MIM1: Context Information Management", https://mims.oascities.org/mims/oasc-mim-1-context.
[287] European Telecommunications Standards Institute (2023), "Context Information Management (CIM); NGSI-LD API", https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.07.01_60/gs_CIM009v010701p.pdf.
[288] International Data Spaces Association (2023), "Dataspace Protocol", Version 0.8, https://github.com/International-Data-Spaces-Association/ids-specification/tree/main.
[289] DCAT-AP is a metadata profile developed in the framework of the EU Programme Interoperability Solutions for European Public Administrations (ISA). DCAT-AP is a specification for describing public sector data sets in Europe, and its basic use case is to enable cross-data portal search for data sets and make public sector data better searchable across borders and sectors.
[290] The Open Digital Rights Language (ODRL) is a policy expression language that provides a flexible and interoperable information model, and vocabulary and encoding mechanisms for representing statements about the usage of content and services.

and freely accessible to the public, some data sets are commercially sensitive. The owners of these data sets will only share them under specific commercial terms and proper contractual agreements.

Different definitions for data marketplaces exist. For IDSA, for example, "Market" is a key activity and a "contract formalises the expectations regarding the behaviour of participants involved in a data exchange transaction in a declarative, technology-agnostic way. It constitutes a unique, binding agreement between the Parties on Resource usage conditions as a result of an (automated) negotiation process. Digital Usage Contracts are maintained in a safe, unforgeable manner (e.g. blockchain). They serve as the foundation for clearing and configuring the Resource's access control policies, and for perpetual evaluation and enforcement by Usage Control Frameworks"[291].

The DSBA, in its recently published version 2.0 of the Technical Convergence document, describes an approach of a "Decentralised Open Marketplace Ecosystem (DOME)". This approach is based on the federation of marketplaces, all connected to a commonly shared digital catalogue of cloud and edge services and service offering descriptions.

Within the domain of mobility, there already several mobility data marketplaces such as Otonomo[292], Mobito[293], Eco-Movement[294] and Ocean Market[295]. These data marketplaces differ from data spaces. Essentially, these **marketplaces establish commercial and contractual relationships** with data producers (e.g. automotive OEMs) and then sell the data to consumers who typically want to develop new services and apps. As an example, the company Otonomo proposes to help companies monetise all the date running through their connected vehicles. Otonomo aims to securely gather the data, modify it, and then make it available to businesses so they can use it to create apps and services for fleets, smart cities, and individual customers. Using both individual and aggregate data, the platform also enables GDPR, CCPA, and other privacy regulation-compliant solutions.

Although these vendors are aware of privacy issues and indeed go to some lengths to address these issues and provide interfaces to enable searching for data sets, they lack the comprehensive data infrastructure that underpins proper data spaces. Specifically, data sovereignty, trust frameworks, data space connectors (such as the EDC), and additional capabilities that are expected of a data space, are absent and not part of these marketplace platforms. These marketplaces are primarily designed for the exchange of data sets and facilitating monetisation of these transactions with minimal required privacy and security mechanisms. It is expected that as mobility data spaces mature (at local, regional, national and EU levels), these data marketplace players may consider connecting to mobility data spaces such as EMDS. It is also possible that the data producers who have contractual agreements with platforms like Otonomo, may prefer to connect directly to mobility data spaces, bypassing intermediaries.

As with any commercial trade, the fundamental requirement is a contract specifying all the terms. When it comes to trading data, services or apps, there are both technical and commercial terms to consider. Technical aspects can include data volume, type, format, provenance, processing applied (if any), quality, etc. Commercial/governance terms include identity verification, usage policies, cost/value, payment, billing, liabilities, SLAs, and so on.

Within this building block, **contract management** emerges as a crucial service or module that ensures effective management of contracts and agreements. It also provides support to marketplace

[291] International Data Spaces Association (2019), "International Data Spaces. Reference Architecture Model", Version 3, https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf.
[292] Otonomo (n.d.), "The Smart Mobility Platform", https://otonomo.io/.
[293] Mobito (n.d.), "Control Your Data Exchange", https://www.mobito.io/.
[294]Eco-Movement (n.d.), "EV Charging Station Data", https://www.eco-movement.com/.
[295] Ocean Protocol (n.d.), "Ocean Market", https://market.oceanprotocol.com/.

participants in navigating data exchange contracts, which are a new phenomenon in many organisations. Additionally, the building block interfaces with other essential components, such as data sovereignty, as this may affect the technical enforcement of contractual terms.

Smart Contracts[296] have undoubtedly a strong potential in this domain and have gained traction within recent blockchain developments. Most of these attributes, as detailed above, are typically part of the metadata or self-description of the data set, service, or app so that they can be easily discoverable but also to clarify contractual conditions associated with them. This includes data usage conditions and is therefore tightly connected to data sovereignty. For example, deltaDAO[297] have already set up some of this infrastructure and is using it in Gaia-X based projects, including the German Gaia-X 4 Future Mobility project family[298].

The marketplace services are intended to be generic and, as such, defined by the DSSC blueprint. These marketplace services will be part of mobility data spaces to manage and regulate the commercial exchange of data sets, data apps (algorithms), and other IT resources – this is already beginning to take place in the MDS. However, no additional mobility specific features are currently foreseen.

Usage accounting

An important enabler for market transactions is a **clearing house** function. The IDSA, for example, includes it as one of the Intermediary (Category 2) roles in its architecture document. It explains the function of the clearing house as follows: "The clearing house logs all activities performed in the course of a data exchange. After a data exchange, or parts of it, has been completed, both the data provider and the data consumer confirm the data transfer by logging the details of the transaction at the clearing house. Based on this logging information, the transaction can then be billed. The logging information can also be used to resolve conflicts (e.g. to clarify whether a data package has been received by the data consumer or not). The clearing house also provides reports on the performed (logged) transactions for billing, conflict resolution, etc.". Note that the Gaia-X Digital clearing house (GXDCH)[299] serves a different function, which is to act as the centralised platform where entities can undergo verification and certification against the Gaia-X rules in an automated way.

As defined by the IDSA, the clearing house provides the mechanism that supports **data usage accounting** and the **corresponding billing** that is required for these transactions. As with contracts, Blockchain technology can be used as infrastructure to ensure transparency and data consistency relying on its decentralised approach. Note that the clearing house does not determine pricing, tariffs, etc. These are defined by the data producer/owner (as part of their self-description) or are negotiated by the parties.

Similar to the marketplace services, the usage accounting services are expected to be generic and will be defined by the DSSC blueprint. No additional mobility specific features are currently foreseen except for possible Billing and payment functions described below.

9.5. Mobility specific building blocks

Most of the building blocks discussed so far provide the common infrastructure for data spaces (i.e., they are domain-independent) and are needed as foundational building blocks. This section discusses

[296] Tyagi, S. et al. (2023), "Study of smart contracts", Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022, available at SSRN: https://ssrn.com/abstract=4376852.
[297] delatDAO (n.d.), "The foundation for the AI & Data economy of the future", https://www.delta-dao.com/.
[298] Gaia-X 4 Future Mobility, "Gaia-X 4 Future Mobility. Gaia-X Lighthouse Project", https://www.gaia-x4futuremobility.de.
[299] EU Gaia-X Initiative (n.d.), "Gaia-X Digital Clearing house", https://gaia-x.eu/gxdch.

specific building blocks needed in a mobility context, including specific building blocks for personal mobility and logistics.

Specific building blocks for personal mobility

Identifying necessary building blocks can be guided by examining common services in mobility for people and goods transport. MaaS can be used as an example of person mobility that includes most (if not all) key services that are required for journeys/trips. Broadly, these are:

- Journey planning
- Booking and ticketing
- Billing and payment
- In-trip, real-time support and notification
- Auxiliary/cross sectoral services

Clearly, some of these services will also support transport of goods (e.g. journey planning). While this is not an exhaustive list, it covers the typical MaaS use case – travelling from point A to point B within a specified time frame, taking into account traveller preferences and service provider and operator constraints. This involves booking and ticketing for the entire trip (including, items such as codes to unlock shared vehicles), and providing a single bill with payment options. Furthermore, during the trip, it includes real-time notifications depending on dynamic changes (e.g. delays, missing the train) and recommendations on how to proceed. The main challenge in this overarching use case is the involvement and participation of multiple operators of various mobility types and additional service providers for planning, booking, ticketing, billing and payment and real-time support for a single intermodal route (i.e., a single trip with multiple transport types). This presents a significant challenge, requiring data and advanced tools, making it a crucial addition to the EMDS building blocks framework.

In this ideal case, all modes of transport, along with related services such as parking, real-time traffic, EV charging, etc., are seamlessly accessible. The ideal scenario involves the traveller receiving a single comprehensive ticket (or “ticket bundle”) that not only covers the regular public transit ticket but also includes a QR code (or similar mechanism) to unlock a shared car or bike, a parking ticket, and more.

Behind the scenes, the MaaS platform (and its operator) in conjunction with a clearing house, ensures that all the operators involved in this intermodal journey are paid for their segments. Clearly, ticketing with its tight coupling to booking, billing, in-trip changes and payment, is an important building block relying on complex data and services exchanges between the many mobility service providers. It should be noted that there are already several related EU initiatives and directives that are directly related to the types of services associated with MaaS. One area of focus is multimodal travel and is therefore closely associated with multi- and inter-modal journey planning. For example, the EU-wide MMTIS[300] and the initiative on MDMS[301]. The topic of **harmonisation of data models and data exchange APIs** for the EMDS has also been elaborated upon in Chapter 7 on data interoperability.

[300] European Commission (2019), "ITS Directive. EU-Wide Multimodal Travel Information Service - Implementation Handbook", https://transport.ec.europa.eu/system/files/2020-07/2020-02-implementation-handbook-delegated-reg20171926.pdf.
[301] European Commission (2022), "Public consultation on the initiative on Multimodal Digital Mobility Services (MDMS). Factual summary report", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2022)5397025.

Note that the **TOMP-API** functional blocks[302] are almost identical to the ones specified above. The MaaS Alliance White Paper[303] presents a more in-depth discussion of MaaS and its relationship to the IDSA-based MDS.

Other, possibly simpler use cases can also benefit from some of these services and therefore the underlying building blocks.

When discussing MaaS and the use of personal preferences utilised, for example, in a journey route planner (see Journey planning below), Personal Data Spaces (PDS) need to be considered part of the solution so as to protect personal data and preserve privacy. Indeed, PDS are referred to in the EC's European strategy for data. MaaS has a very strong link to PDS and portability of individual profiles and preferences. PDS have data portability requirements (and interoperability, legal and policy question at the same time). For example, what data is transferred or allowed to flow from one system to another and under what conditions does this occurs. Since the PDS concept is not limited to mobility data spaces, it is a topic of discussion within the DSSC and how PDSs are integrated with a mobility data space, in particular, the needs to be coordinated and co-developed with the DSSC.

In the following paragraphs, the proposed basic mobility specific building blocks are outlined and examined in more detail.

Journey planning

This building block provides basic services and capabilities that require data and information from transport/mobility service providers, as well as inputs from the traveller (i.e., personal preferences) and possibly data and information from additional service providers such as parking operators. A key capability is an intermodal routing service – a challenging task that becomes more complex the more service providers are included and the more preferences there are. Routing services are available (e.g. Open Trip Planner[304], MOTIS[305], and others), but many account only for public transportation options and do not include shared mobility or mobility on demand. Some commercial solutions are available (e.g. Jelbi in Berlin[306], Better Mobility in Aachen[307], Whim in Finland[308], and others), but no "ideal use case" at scale has been developed so far.

Booking and ticketing

Although ticketing is a topic that is related to many non-mobility related domains, the rise of smart mobility solutions in the last few years has increased the need for cross-mode coordination and demand for multimodal ticketing services. This presents a significant challenge, requiring data and advanced tools, making it a crucial addition to the EMDS building blocks framework.

Once a journey has been planned, a booking needs to be made, and a corresponding ticket or "ticket bundle" created. Here again, the challenge is that multiple segments of the journey are the responsibility of multiple operators and service providers:

---

[302] International Transport Forum (2023), "Mix and MaaS. Data Architecture for Mobility as a Service", https://www.itf-oecd.org/mix-and-maas-data-architecture-mobility-service.
[303] MaaS Alliance (2022), "Mobility Data Spaces and MaaS. Building a Common, Connected and Interoperable Ground for the Future of Mobility", https://maas-alliance.eu/wp-content/uploads/2022/10/MaaS-Alliance-Whitepaper-on-Mobility-Data-Spaces-1.pdf.
[304] OpenTripPlanner (n.d.), "OpenTripPlanner", http://www.opentripplanner.org.
[305] MOTIS project (n.d.), "Intermodel Travel Information". https://motis-project.de.", https://motis-project.de.
[306] Jelbi (n.d.), "Berlin's entire public transport and sharing services in just one app", https://www.jelbi.de/en/home.
[307] Better Mobility GmbH (n.d.), "Ihre Stadt – schlau vernetzt", https://www.bettermobility.de.
[308] Whim (n.d.), "How to get there", https://whimapp.com.

- Different regulations may be in place (e.g. at what age is a traveller considered an adult? What tariff should apply?);
- Tickets may need to be used to unlock bikes or cars or a parking lot barrier;
- Tickets may need to be updated but only along one segment; etc.

These issues create challenging interoperability requirements and the use of established standards, data formats, etc. However, this is exactly what a EMDS can establish, where ideally most or all the required data is available.

Billing and payment

As with the other building blocks, coordinating and financial settling across all operators and service providers so that the user ideally gets a single bill for a single trip is a challenge. A clearing house function is typically required and has been previously described in more detail under Usage accounting below. Similar to the interface between Booking and Planning, an interface between Booking and Ticketing and Billing and payment is required.

Furthermore, the business process extends beyond billing to include conflict management, handling unpaid bills, deductions, returns, and delayed payment interest. This complexity is prominent in MaaS ticketing, involving responsibility assignment for missed train connections and determining financial responsibility for potential accommodation and meals.

In-trip, real-time support and notification

Beyond the non-real-time (offline) blocks described so far, a key function is supporting travellers during their journey. Unexpected events may occur along the route, requiring adjustments in real time. Travellers should be promptly alerted, and alternative options should be recommended based on the user's profile and preferences. While some transport service providers (such as the Deutsche Bahn in Germany) offer some of these services, they often lack information on alternative travel modes (e.g. a shared car) and necessary details (closest shared car, current traffic situation, etc.). Furthermore, automatic booking and payment adjustment for these changes are not currently available. This building block should interface with the intermodal route planner (part of the Planning building block) to reroute, and potentially interface with Booking and Billing and payment building blocks.

Auxiliary services leveraging cross-sectoral data

Auxiliary services are additional services that typically fall outside of MaaS but are complementary and enhance the "travel experience" and the goal of seamlessly getting from point A to point B. Some of these services benefit from cross sectoral data and IT resource sharing. Services that travellers need may include real-time traffic updates, parking availability, EV charging station information, and details about nearby mobility hubs including the services offered and their availability. Some of this data may be required by the Planning building block, while other information may be available in other data spaces, for example, smart city data spaces, tourism data spaces, and energy data spaces. This building block needs to feature connectivity with adjacent data and information services, both intra and inter data space (i.e., cross sectoral functions).

Specific building blocks for logistics

As the concept of personal mobility is shifting towards MaaS, a similar transformation is occurring in the logistics domain. Freight mobility is increasingly considered as Transport-as-a-Service[309] or

[309] Simpson, C., Kemp, E., Ataii, E. and Zhang, Y. (2019), "Mobility 2030: Transforming the mobility landscape", KPMG International.

Logistics-as-a-Service. This aligns well with the idea of logistics as a service orientated function, which is evolving with approaches such as 3PL (third party logistics provider), LSPs (logistics service provider covering transport and warehousing) and 4PL (fourth party logistics provider, a service provider managing all logistics processes for a customer). While Transport-as-a-Service focuses on providing all resources and services needed for executing transportation, Logistics-as-a-Service covers the comprehensive provision of value-added services to fulfil logistics tasks, regardless of their dimension, complexity and geographic scope.

The growing demands and challenges related to **transport efficiency and safety**, careful use of available resources, and the reduction of emissions (GHG, noise, etc.) are driving the development of multimodality, combining different transport modes more flexibly.

Living in an intermodal, or even more **synchromodal, world** means combining all modes of transport and related transhipment point (terminals, ports, hubs, etc.) seamlessly. Furthermore, it involves coordinating related services (e.g. stuffing, technical inspection of the wagons, customs clearance, dangerous goods management), providing information on filling/charging stations and other service facilities, managing transport document flows, and much more, which characterises and describes the concept of intermodal logistics. Ultimately, data, information, and knowledge should be available for all these logistics components to guarantee a seamless and smooth planning, execution and monitoring.

The realisation of such seamless intermodal chains is based on an analogy with personal mobility, involving the inclusion, linkage, and coordination of multiple operators, as well as resource and data respectively service providers, covering all named items of logistics chains. Along with these actors and participants, a variety of related services such as route planning, clearance, and monitoring or visibility, are needed. This underscores a significant demand for the respective data and advanced tools, making it a fundamental complement to the EMDS building blocks framework.

Furthermore, the EMDS could and should serve as a **common base for interoperability between existing logistics platforms**, data spaces, etc. Different platforms and data spaces (e.g. cloud-based community platforms for customs clearance and freight forwarding such as DAKOSY or Port Community Systems Portbase, connecting different players of logistics chains) are already in use or under construction. It is not expected that an EMDS will replace such systems but rather should be the basis for ensuring interoperability between such diverse IT worlds. This would lead to simplified networking, cost savings, a standardised domain-specific vocabulary, and a more extensive database that enables holistic views on logistics chains. It would also improve planning and execution and promote integrated transportation management.

A standardised functional base for representing logistics within the framework of an EMDS could use the **OTM**[310] and its API. The OTM is independent of how transport within a supply chain is organised, independent of modality, human and machine readable and extensible". The OTM covers various objects for logistics modelling including locations, trips, routes, vehicles, sensors, shipments, actors, constraints, events and bundles. Possible functional building blocks should be aligned with these concepts.

The OTM should be a recommended as a standard for logistics building blocks within the EMDS, guaranteeing its openness and relevance for EMDS participants.

[310] OpenTripModel (n.d.), " OpenTripModel is a simple, free, lightweight and easy-to-use data model, used to exchange real-time logistic trip data on the web", https://www.opentripmodel.org.

Logistics visibility/shippers' control tower

Many shippers are currently striving to establish virtual control towers to oversee logistics operations. The effort requires data from different logistics service provider or transport service provider, terminals, infrastructure operators is substantial and could be reduced if basic information would be available at a single point of truth, like the EMDS.

This would allow real-time transportation visibility platforms, e.g. Shippeo, and Transporeon, to focus on collecting, linking and providing specific and logistics chain-sensitive data. An EMDS should support the business models of these providers with a dedicated building block and avoid interfering with their operations.

Transport management systems

Larger companies, including shippers and transport or logistics service providers, base their processes and management on transport management systems. The system's value significantly depends on effective connectivity combined with the timely provision and processing of the right data. This means that a wide range of data is needed, starting with geo-data on networks and locations, and extending to information about resources such as staff, vehicle types, and loading devices, also encompassing transaction data like orders, shipments, and bills or credit notes.

While a "Transport management" building block would encompass a wide range of functional building blocks, such a development would likely face resistance by industry stakeholders. Nevertheless, a foundational data sharing building block enabling better transport management could be a good starting point to avoid conflicting with economic interests of transport management systems providers, and possibly even generate new business opportunities.

Freight cost management and clearance

Logistics professionals employ an array of rates, tariffs, terms, and cost structures. While some align with global standards, some are company-specific and transparently shared with prospective clients. Others are tailor-made and negotiated on a case-by-case basis. Despite this complex landscape, pursuing the creation of a building block for "Freight cost management", though challenging, would be helpful.

Moreover, there is a need for clearing house and billing and payment building blocks in logistics. The clearing house acts as mediator to ensure that the exchange of goods and their payment are handled correctly. The billing and payment building block handles the financial fulfilment.

9.6. Recommendations

Conclusion

The data value creation building blocks for the EMDS facilitate registration, exposure and discovery of data space entities ("IT resources"). They also facilitate the sharing of data, data services, applications and semantic models. These building blocks allow participants in the EMDS to discover, access and use these IT resources, enabling the EMDS to expand its capabilities to support various use cases and enable the creation of multi-sided markets.

The data value creation building blocks are essential for interoperability, not only within the EMDS but also with other (adjacent) data spaces. Hence, the development and deployment of these building blocks within the EMDS should follow a generic and federated approach, as outlined in the DSSC blueprint. When developing data value creation building blocks for the EMDS, it is important to focus on those aspects and features that are specific to mobility.

Recommendations

Develop a multi-service federated metadata broker

A harmonised metadata broker is essential to support each of the four types of data sharing: (1) persistent (static or semi-static) data, (2) (real-time) streaming data, (3) algorithms for local processing of (sensitive) data, and (4) event-driven smart contracting for data flow control. The first two types of data sharing may be considered as "classic" or "traditional". A common approach for describing these two "classic" types of data sharing is expected to be part of the technical grounding developed by the DSSC. Special emphasis should be given to types (3) and (4) as their relevance for the EMDS is expected to grow rapidly. To potentially align data spaces for personal mobility with the data space for logistics, it is crucial for the federated metadata broker to support the type of data sharing known as **Event-driven smart contracting for data flow control.** By including the Service Registry and Index functions, as defined in the FEDeRATED architecture, in the local metadata brokering capabilities of the data space connector, they become easily accessible **across various data spaces.** This facilitates support for similar data sharing for personal mobility. Moreover, it is necessary to conduct a functional break-down analysis of the Service Registry and the Index functions. The EMDS deployment initiative should align with the DSSC blueprint initiative and the SIMPL project to ensure that all four types of data sharing become integral components of the metadata brokering building blocks in the European data spaces technical framework.

Initiate a metadata/context broker harmonisation and interoperability strategy

Numerous domain specific implementations of metadata/context brokers are already being deployed. For example, the CEF programme and the i4Trust initiative used the FIWARE Context Broker as metadata/context broker building block. Moreover, the metadata/context broker serves as the first MIMs, as defined by the OASC initiative. This capability requires further development in a mobility environment where several similar capabilities are already in operation, particularly existing metadata or context brokers in the general domain of open data portals, for example. Either a metadata/context broker consolidation or an interoperability strategy is needed for interconnection and interoperability. Given the central role and positioning of the existing ETSI NGSI-LD standard and the emerging Dataspace Protocol, the recommendation is to consider and assess these as part of the interoperability strategy.

Develop building blocks to support semantic translation

The EMDS will need to be embedded into the European mobility sector, which encompasses an extensive landscape of existing and emerging data sharing initiatives. To promote the adoption of the EMDS, it is crucial to develop capabilities for managing semantic differences in the data models used by the various data sharing initiatives, thereby reducing barriers to interconnection. Building blocks to support semantic translation such as a vocabulary hub, semantic transformation engine, and a data space connector semantics configurator, should therefore be developed and deployed within the EMDS, e.g. a vocabulary hub, semantic transformation engine, and a data space connector semantics configurator. In alignment with the DSSC blueprint initiative and the SIMPL project, it should be considered whether these building blocks can be developed as generic and federated building blocks that can also to be used for and across other sectoral data spaces.

Develop building blocks to support local execution of data apps and data app sharing

To enable data pre-processing through local execution of data apps before sharing the processed data, and to support the PETs with distributed algorithms needing local access to sensitive or private data, building blocks are required to support the local execution of data apps and make these data apps generically available across data spaces. For the former, an environment for secure, trustworthy, stable and scalable execution of data apps and for orchestrating their execution of data apps is needed. For the latter, capabilities for cataloguing data apps are needed. It is worth noting that such capabilities are envisioned as part of the IDSA role model and reference architecture, incorporating of the secure execution environment as part of the IDS connector and the app store role. For the EMDS, these capabilities should be developed and deployed. This development should also align with the DSSC blueprint initiative and the SIMPL project that explore the feasibility of developing these building blocks as generic and federated building blocks, suitable for use in and across other sectoral data spaces.

Introduce a portfolio of MaaS related services

Person mobility requirements and use cases are largely addressed by a comprehensive MaaS platform. This includes journey planning, booking and ticketing, billing and payment, and in-trip support. Pre-trip services such as planning and booking require multi- and intermodal routing that takes into account constraints and preferences. The platform should also providing the capabilities for handling a variety of ticket types and tariffs for different modes, while allowing them to be combined into single tickets (or ticket bundles) for intermodal journeys. For example, tickets should support both public transit and shared mobility options that may include means to unlock vehicles. Some of these building blocks (i.e. ticketing, billing, payment) may optionally be connected to or integrated with clearing house services, particularly for single tickets consisting of multiple segments operated by different entities. Furthermore, tickets and tariffs are directly linked to traveller preferences. For example, a user may prefer to use bikes only when it is not raining. These preferences are maintained by the user and can be part of their Personal Data Space (PDS)[311]. A user's PDS can also leverage AI tools and approaches, such as Preference Learning[312] to manage continuously growing sets of preferences as more services are made available. To the extent that some of this personal data (and commercially confidential data) is part of protected data held by public sector, it is important to note that it may be reused under specific EU or national legislation. A wealth of knowledge can be extracted from such data without compromising its protected nature, and the DGA provides rules and safeguards to facilitate such re-use whenever it is possible under other legislation[313] (see also the Open Data Directive[314]). Finally, in-trip needs to support real-time data, notifications, and (AI-based) recommendations. Similarly, an adequate base must be provided for logistics and Logistics-as-a-Service.

Initiate use case development across sectoral data spaces

This involves providing supporting services for multi-domain applications and use cases such as parking, EV charging, real-time traffic. For example, in e-mobility related use cases, the EVs serve not only as a means of transportation for people but also as mobile energy sources. In V2X applications,

[311] For more on Personal Data Spaces (PDSs), see, for example, Lähteenoja, V. (2023), "What are "personal data spaces?", WWW '23 Companion, April 30 – May 04, 2023, Austin, TX, USA, https://dl.acm.org/doi/pdf/10.1145/3543873.3587656.
[312] Wikiwand (n.d.), "Preference Learning", https://www.wikiwand.com/en/Preference_learning.
[313] European Commission (2023), "Shaping Europe's digital future – Data Governance Act Explained", https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.
[314] European Commission (2019), "Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast)", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024.

EV batteries can provide backup power, ancillary services for energy providers, and peak shaving, among other functions. These types of use cases are not solely based on acquiring data or applications from separate data spaces. Instead, they rather require data and services to be developed by other sectoral data spaces, such as smart cities, energy, tourism. Again, this underscores the need for interoperability between data spaces, focussing on key aspects like data sovereignty, trust and discoverability.

9.7. Building blocks

Figure 28 shows the individual building blocks recommended for data value creation.

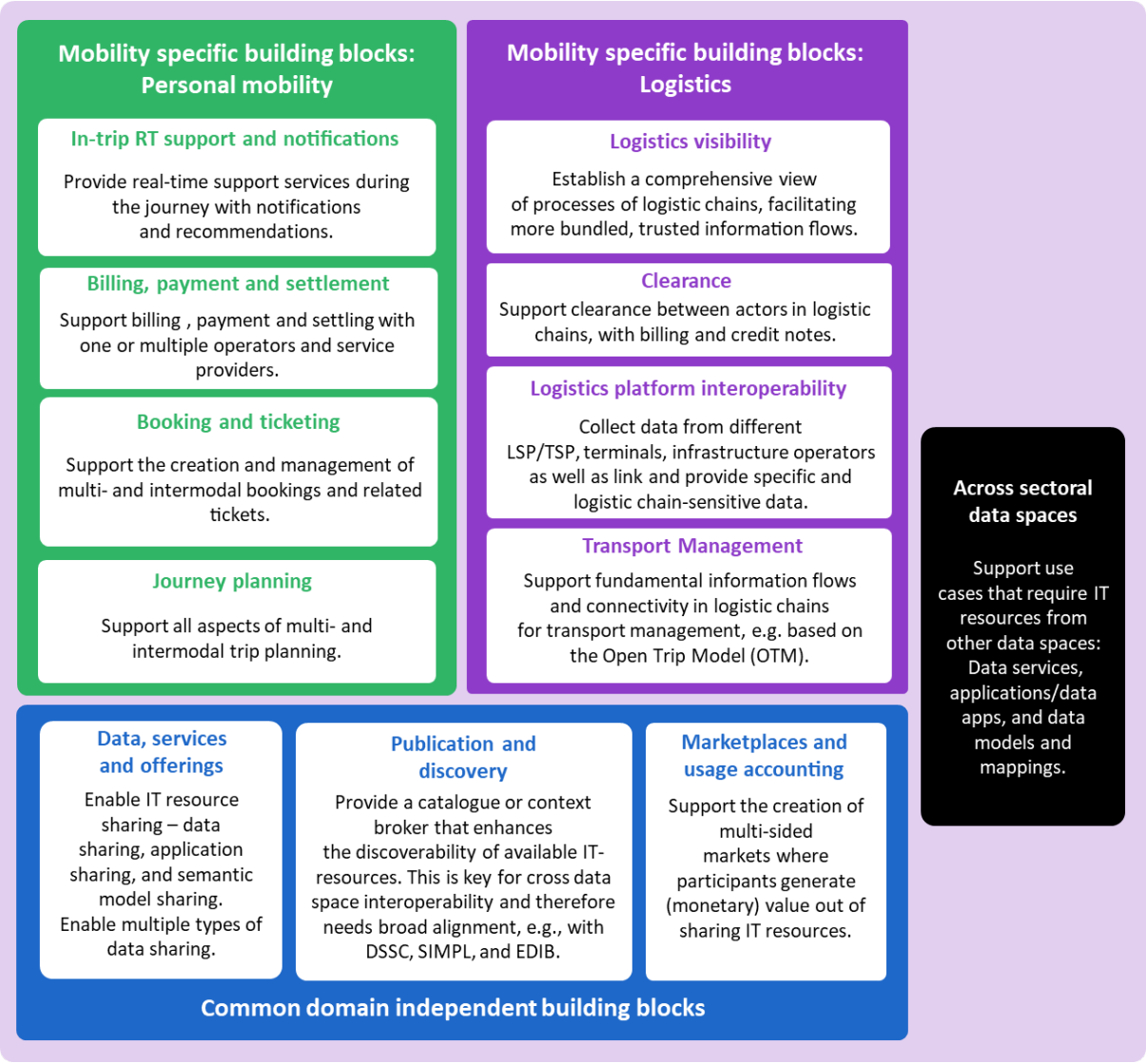


Figure 28: Building blocks for data value creation.

V. Reference architectures, alignment and conclusion

The landscape of reference architectures and technology for implementing the technical building blocks in the context of the common European data spaces is rapidly evolving. As progress continues in this domain, it becomes clear that the deployment of mobility data spaces within the larger framework of federated, interoperable data spaces is still in its infancy. Effectively navigating this early stage of development requires comprehensive guidance that addresses both architectural development and adoption strategies.

To conclude, this final section of the report offers an overarching view on the building blocks essential for the development of the EMDS. This includes reference architectures for both individual mobility data spaces (intra data space interoperability) and interconnecting multiple mobility data spaces (inter data space interoperability), discussed in Chapter 1010. 11 Chapter 11 addresses the potential for further alignment with respect to common European data space infrastructure and a common European cloud infrastructure. Chapter 1212 presents the overarching conclusion with insights on operationalising the EMDS.

10. Reference architectures: role models and building blocks

10.1. Introduction

In alignment with the DSSC taxonomy, the chapters in this report have elaborated numerous recommendations and building blocks for the EMDS. This chapter offers an overarching perspective on the EMDS building blocks through the lens of reference architectures. The goal of these reference architectures is to provide guidance for organisations in the development of interoperable data spaces in mobility and logistics. They elaborate the architecture in terms of role models and building blocks, supporting the rich set of capabilities as identified throughout this report.

The following sections describe the recommended **reference architectures** for individual mobility data space instances ("**intra data space interoperability**", Section 10.2) and for interoperability between the mobility data spaces, ecosystems and platforms to be federated under the EMDS ("**inter data space interoperability**", Section 10.3).

10.2. Intra data space interoperability reference architecture

The reference architecture for intra data space interoperability offers an overarching perspective of the role model and building blocks for individual data spaces. It primarily serves a generic framework applicable to data spaces across various sectors. Additionally, it includes mobility specific building blocks as identified in Chapter 9 on data value creation.

Recognising each data space's sovereignty to develop its policies, guidelines, and building blocks, this reference architecture should be regarded as a suggested framework for the development of mobility data space instances and the EMDS. It supports a wide range of features and capabilities. Therefore, the proposed architecture is descriptive, rather than prescriptive. However, following this reference architecture for individual mobility data space instances will provide significant benefits in terms of efficiency and preparedness for interoperability demands by their customers.

Recognising individual data spaces' sovereignty to develop its architecture, the primary goal of the reference architecture for intra data space interoperability is to offer supportive guidelines.

Architecture principles for intra data space interoperability

The architecture principles for the reference architecture for intra data space interoperability underpinning the EMDS are summarised below. Following the TOGAF Application Development Methodology[315], they include business architecture principles, Information System Architecture (ISA) principles, and technology architecture principles:

- The **business architecture principles** for the EMDS are derived from the European ambition on federation of interoperable data spaces, as expressed in the European Data Strategy, the Open DEI guidelines, and the recently initiated EU initiatives on the development of reference architectures, as described in Section 1.2;
- The **Information System Architecture (ISA)** principles translate the business vision and business architecture principles into a set of building blocks, jointly implementing the capabilities for realising the business vision;
- The **technology architecture principles** provide guidelines for the realisation of the building blocks implementing the capabilities as defined in the ISA.

[315] The Open Group (n.d.), "TOGAF 9.1", https://pubs.opengroup.org/architecture/togaf91-doc/arch.

Table 15 describes these principles in the context of the EMDS. Each business architecture principle and information architecture principle refers to a chapter for additional background. The technology architecture principle provides guidelines for implementing building blocks without needing reference to a specific chapter in this report.

Table 15: Architecture principles for EMDS intra data space interoperability.

Business, information system architecture and technology architecture principles for EMDS intra data space interoperability		
Business architecture principles	**Information system architecture principles**	**Technology architecture principles**
• Multiple types of data sharing may be simultaneously supported within the EMDS (Chapter 2, 9). • Data can be a valuable asset and must be managed as such by means of data sovereignty and trust capabilities (Chapter 8). • Data spaces enable their participants to (locally) share and deploy data apps (Chapter 2,9). • A single point of entry provides access to each data service in the federation of data spaces (Chapter 4,6).	• Data space intermediary capabilities are provided by means of federated building blocks. • The reference architecture and its building blocks are (by default and where possible) based on the DSSC blueprint and the SIMPL building blocks (Chapter 4). • IT resource sharing policies (e.g. on data and applications) are defined by entitled parties and can be managed using the building blocks within the data space (Chapter 8). • Data sharing transactions can be logged for analysis, auditing, conflict resolution and billing purposes (Chapter 9). • A single Information Model for metadata support within the data spaces should be used, based on an information model of an accepted data space reference architecture (Chapter 7).	• The building blocks, as described in the ISA, expose their capabilities by means of well-defined APIs. • The Dataspace Protocol should be used (where applicable) for interoperability between data space building blocks (Chapter 6). • Reference implementations of data space building blocks should be open source and future proof. • Building blocks should (by default) be developed for federation across multiple data spaces (Chapter 6).

EMDS: intra data space role model

The reference architecture for intra and inter data space interoperability is based on the role model of stakeholders and the building blocks (capabilities) they provide. A role corresponds to a primary activity in the overarching processes of data sharing, which may be performed by an independent organisation.

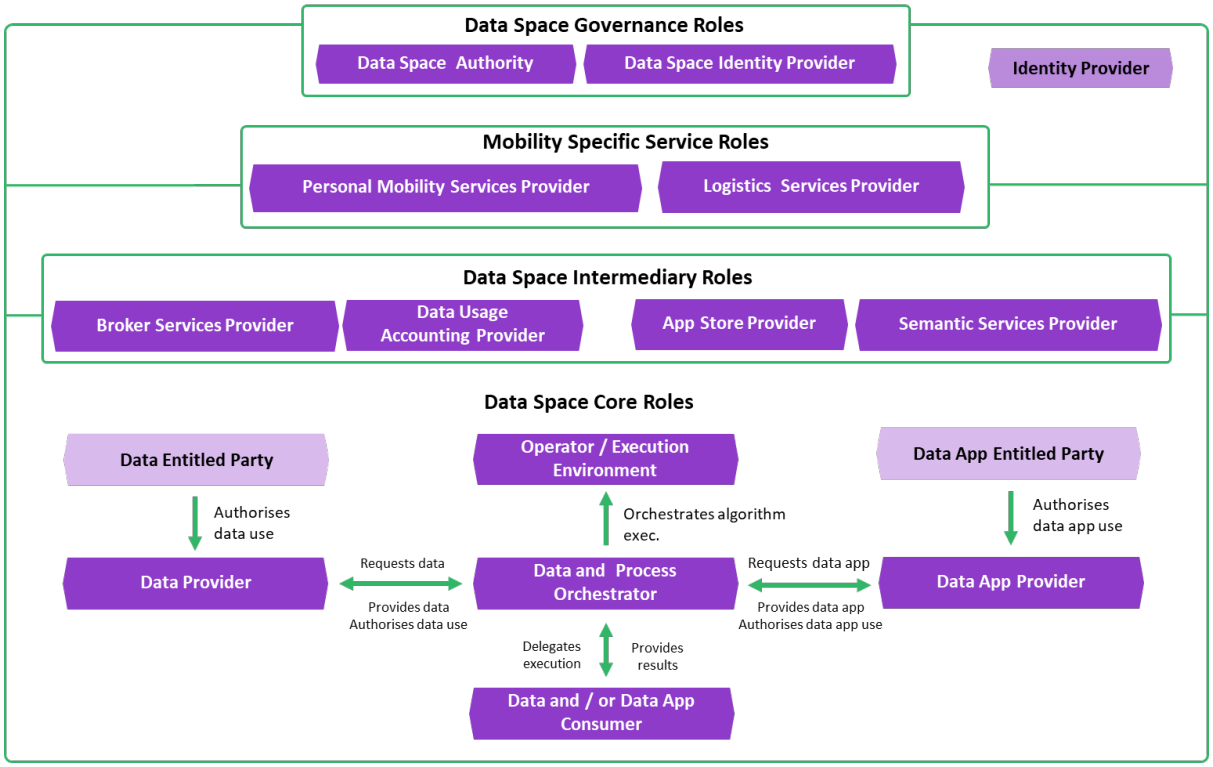


Figure 29: The role model for EMDS intra data space interoperability.

Each role can be assigned to one of the categories proposed by the IDSA role model structure[316]:

1. The **data space core roles**, encompass the core participants who are involved and required every time data is exchanged (such as data providers and data consumers);
2. The **data space intermediary roles** encompass trusted intermediary entities that are commonly considered as "platforms" and assume a rather central role compared to the great number of core participants;
3. The **data space governance roles** have the authority and the task of setting and enforcing guidelines to standardise data exchange, to create trust, and enable sustainable operation of the IDS.

These three categories and the roles they contain are **generically applicable** to a multitude of sectoral data spaces, including the EMDS. The roles in each of these three categories jointly constitute what is commonly referred to as the **"interlinking layer"** for the data space. In Figure 29 above, a **mobility specific service roles category** has been included to account for the mobility and logistics specific building blocks identified on data value creation in Chapter 9. Table 16 describes the categories of roles for data spaces and the individual roles.

[316] International Data Spaces Association (2022), "Roles in the International Data Spaces", https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3-1-business-layer/3_1_1_roles_in_the_ids.

Table 16: Categories of roles for intra data space interoperability.

The categories of roles for intra data space interoperability
Data space core roles The data space core roles are involved and required every time data, or an application is shared or executed in the data space. The role of a core participant can be fulfilled by any organisation that owns, intends to provide, consume/use or execute data or a data app.
Data provider Data providers store data in the data spaces and make this data available in a controlled manner. They manage policies for the data they hold. This includes enforcing access and usage policies and providing additional policies to the operator. Data providers also manage the quality and availability of data on behalf of data entitled parties.
Data entitled party Data entitled parties have one or more entitlements, e.g. having control over or being the subject of the data provided by a data provider. The data entitled party has the right to define the terms and conditions of use of data to which it is entitled. To manage this, the Entitled Party can use an Authorisation Registry service or define policies in connectors.
Data app provider Data app providers hold the data apps in the data spaces, which contain distributed PET algorithms, digital twin functions or data pipeline pre-processing logic and manage policies for these data apps. They manage and enforce access and usage policies and share these policies with the operator. Data app providers also manage the quality and availability of data apps on behalf of data app entitled parties.
Data app entitled party Data app entitled parties have one or more entitlements to the data apps provided by a data app provider. Data app entitled parties have the right to define terms and conditions of use for the data apps to which they are entitled.
Data and/or data app consumer Data and/or data app consumers are interested in the result of data sharing and data processing action. They receive the required results from the data and process orchestrator to which they have delegated the (orchestration of) the execution of the data processing.
Data and process orchestrator The data and process orchestrator orchestrates the intended data sharing interaction and data processing execution, ensuring that the data apps yield the intended results for the data and/or data app consumer. The data and process orchestrator properly manages the policies for the processes it orchestrates. It understands which core modules for data sharing and data processing are required and is responsible for bringing these together through orchestration, such as by identifying and bringing together relevant data and data apps. The orchestrator is also responsible for properly assessing policies that are relevant. A main added value of the data and process orchestrator is that it serves as a single-point-of-contact for the data and/or application consumer, orchestrating and integrating the interactions with all core roles and the services/building blocks they provide.
Operator/Execution environment The operator/execution environment provides a trustworthy process execution environment where the workloads defined and orchestrated by the data and process orchestrator can be deployed. This trustworthy process execution environment can be a trustworthy cloud-edge processing environment.
Data space intermediary roles The data space intermediary roles enable the processes for interaction between the core roles by establishing providing metadata, support services, and establishing trust.

The categories of roles for intra data space interoperability
Broker services provider A broker services provider offers capabilities to register, manage and expose information about IT resources available in a data space, e.g. data services, data apps and computing resources. Moreover, it can provide capabilities to support the offering of data resources and services under defined terms and conditions, which clearly describe the rights and obligations for data and service usage, as well as access to data and services.
Data usage accounting provider The data usage accounting provider manages and provides the basis for accounting access to and/or usage of resources (e.g. data, data apps) by various participants. It includes the important capabilities for recording data transactions that have taken place, serving as the basis for clearing, billing, and conflict resolution.
App store provider The app store provider offers data apps that contain applications (e.g. algorithms) which may be deployed within the secure processing environments of the data space, such as in a participant's or a (cloud) execution environment. These data apps facilitate data processing workflows. The app store provider is responsible for managing metadata on the data apps it provides.
Semantic services provider The semantic services provider offers services to manage semantics within the data space, including a registry of vocabularies (i.e., ontologies, reference data models, or metadata elements) and semantic mappings that can be used to annotate, describe and transform data sets. Additionally, the transformation of data sets can be provided as a separate service.
Data space governance roles The data space governance roles coordinate the set of commonly agreed principles within a data space and manage compliance of data space participants with these agreed principles. The data space governance roles provide the capabilities associated with the agreement framework, which is sometimes also referred to as the trust framework.
Data space authority Data spaces may potentially grow very large. In these larger data space environments, where not all participants may directly know each other, there is a need for capabilities to ensure that data sharing transactions between participants adhere to an agreed-upon protocol/approach and can be 'trusted'. The data space authority is responsible for the (legal and operational) agreements within a data space, for certification of participants and components used within the data space, and for the operations of the data space.
Data space identity provider The data space identity provider offers a service to create, manage, maintain, monitor, and validate identity information of participants and/or components within a data space. This is imperative for secure operation of the data space and to avoid unauthorised access to and usage of data.
Mobility specific service roles The mobility specific service roles take into account the specific roles in mobility and logistics along with the with the building blocks for data value creation.
Personal mobility services provider A personal mobility services provider offers data value creation building blocks that are specific for the personal mobility sector.
Logistics services provider A logistics services provider offers data value creation building blocks that are specific for the logistics sector.

Figure 29 also depicts the role of "Identity provider" which provides the capabilities to identify and authenticate natural persons, organisations, or software components as legal entities. This is a generic capability intended for use by multiple roles.

EMDS: intra data space building blocks

The preceding chapters describe the technical and governance building blocks. Figure 30 depicts how **building blocks** for intra data space interoperability can be **mapped onto the role model for intra data space interoperability**[317].

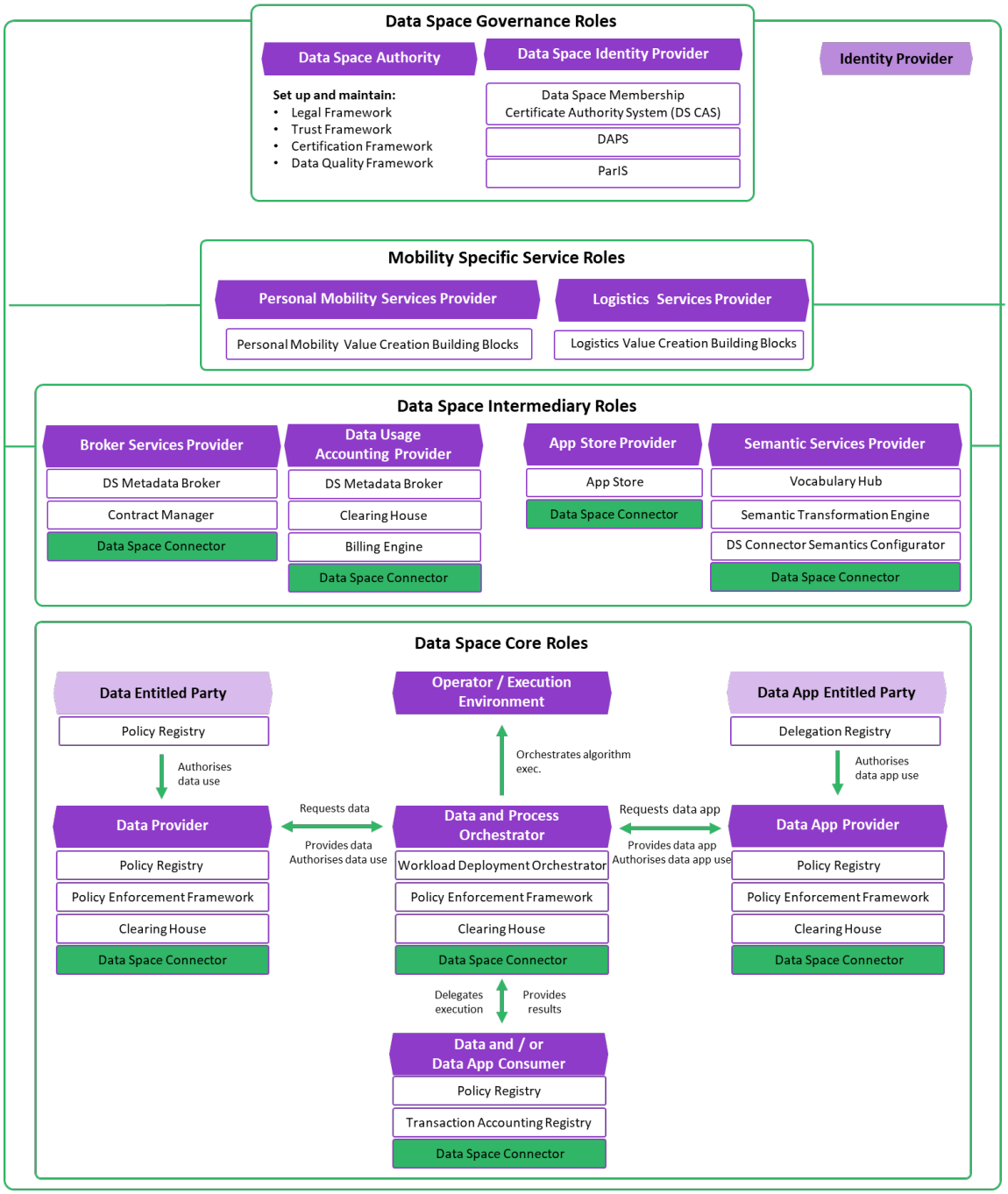


Figure 30: Reference architecture of building blocks for intra data space interoperability.

[317] Derived and adapted from: The Netherlands AI Coalition Working Group Data Sharing (2022), "Reference guide for intra AI data space interoperability", https://nlaic.com/wp-content/uploads/2023/04/NL-AIC-intra-AI-Data-Space-Interoperability-v3.2.pdf. It contains additional information on the description, API's and (open source) implementations of the individual building blocks.

Table 17 describes the building blocks depicted in Figure 30, using the DSSC taxonomy that distinguishes building blocks for “Data interoperability”, “Data sovereignty and trust”, and “Data value creation”.

Table 17: Building blocks in the ISA for intra data space interoperability.

Building blocks in the ISA for intra data space interoperability
Data interoperability building blocks Capabilities to discover semantic models and mappings and manage semantics transformations.
Vocabulary hub Registry service providing facilities for publishing, editing, browsing, and maintaining vocabularies and related documentation. These vocabularies include ontologies, reference data models, schema specifications, mappings and API specifications that can be used to annotate and describe data sets and data services. The vocabulary hub can mirror a set of third party vocabularies ensuring availability and resolution.
Semantic transformation engine Provides semantic transformation services between data formats. It uses vocabularies and mapping specifications as provided by the vocabulary hub. The component can be integrated into the data consumer or data provider implementation or offered as a service in a data space.
Data space connector semantics configurator Service to enable data space participants to use vocabularies to configure the semantic interoperability of implementations. This is primarily done by creating ontology-based API specifications to define the semantic interface between data providers and data services consumers. Additionally, the configurator can assist in creating mapping specifications, which can be used in the semantic transformation engine.
Data sovereignty and trust architecture building blocks Capabilities enabling data sovereignty and trust for the entitled party, guaranteeing that data sharing policies (i.e. access and usage control policies) can be defined and enforced.
Data space connector A data space connector is the main component that provides the interconnection between an organisation or system and the data sharing and intermediary capabilities of the data space. It serves as the foundation for a data space that enables (standardised) federated data sharing between data space participants while maintaining data sovereignty and trust for entitled parties.
Policy enforcement framework Technically enforces the applicable policy conditions (e.g. specific access and usage policies) within the security environments of the (combination of) data provider and/or data consumer.
Policy registry Manages and registers the applicable policy conditions, involving specific access and usage rights for data space participants as attributed by entitled parties to data services or data apps, including delegation of the rights to other data space participants.
Workload deployment orchestrator Provides the capabilities to deploy and execute data apps in a secure and controlled manner, either within the security environment of the data provider or data consumer or in a secure (cloud) environment provided by a third party.
Data Space Membership Certificate Authority System: DS CAS Provides certificates for participants and/or software components involved in data sharing within a data space, used to verify data space membership during data sharing transactions.
Dynamic Attribute Provisioning Service: DAPS

Building blocks in the ISA for intra data space interoperability
Manages and registers the dynamic attributes of software modules implemented by means of a data space connector, including the security profiles and certification status.
Participant Information System: ParIS Manages and registers the attributes of the participants, specifically natural persons or organisations as legal entities, including the name and address details, chamber of commerce number, and more.
Data value creation building blocks Capabilities to create value from data sharing in a data space, valorise data transactions through registration of data sharing contracts and transactions, and manage accounting and monetisation thereof.
Data space catalogue Manages, registers and publishes the IT resources available within a data space, e.g. data services, data apps and computing resources.
App store Manages, registers and publishes data apps that can be deployed within a data space connector.
Contract manager Provides capabilities to support the offering of data resources and services under defined terms and conditions, including the management of processes linked to the creation and monitoring of smart contracts. These contracts clearly describe the rights and obligations for data and service usage, as well as access to data and services.
Clearing house Handles all required pre-conditions before (sensitive and/or valuable) data can be shared. These pre-conditions may include both confidentiality aspects (e.g. for non-repudiation) or financial aspects (e.g. financial settlement). As such, a specific capability for the clearing house can involve event-driven (real-time) data flow control, often based on smart contracting. Moreover, the clearing house may also register and monitor data sharing transactions, which can be used as input for conflict resolution and billing.
Billing engine Provides the capabilities for the billing process associated to data sharing transactions, e.g. generate invoices and manage the payment process.

10.3. EMDS inter data space interoperability reference architecture

The reference architecture for inter data space interoperability provides the role model and building blocks for the development of the federation of multiple, interoperable (mobility) data spaces. As such, this reference architecture outlines (a) the horizontal relationship between federated data spaces in the EMDS, and (b) the vertical relationship between the ecosystems, and the governance and intermediary roles of a centralised data space federation governance authority, such as the EMDS.

Regarding intra data space interoperability is required to ensure interoperability, especially on the key capabilities of data sovereignty, trust and discoverability. Therefore, since the **federation of data spaces requires the adoption of commonly agreed standards**, the reference architecture and its associated protocols and standards need to be **prescriptive and widely adopted**. In this regard, the significance of the federation services and the data space protocol (Section 6.4) cannot be overstated. Moreover, they should be integrated into and aligned with the technical grounding for federation of data spaces (Chapter 6), which is being developed by the DSSC blueprint and supported by building blocks of the SIMPL initiative.

Architecture principles for inter data space interoperability

The architecture principles for the reference architecture for inter data space interoperability include business architecture principles, Information System Architecture (ISA) principles, and technology architecture principles. These principles are detailed in Table 18.

The principles listed in the table correspond to the **full and partial harmonisation modes** as described in Chapter 6 on the technical grounding. In case of full harmonisation of data spaces, individual data spaces adhere to the same harmonised requirements and principles, and adopt federated data space building blocks, especially those related to data sovereignty, trust, and discoverability. **Full harmonisation between data spaces provides major advantages** for inter data space interoperability, both in terms of functionally and increased ease and efficiency.

For **existing data spaces,** pursuing full harmonisation with other data spaces may result in a significant impact in terms of alignment and migration efforts, and costs. Therefore, **partial harmonisation** is introduced by means of a "**data space proxy**." These proxies handle the complexity of harmonising data spaces, enabling data consumers and providers within a data space to easily connect to other data spaces via their respective proxies.

Table 18: Architecture principles for EMDS inter data space interoperability.

Business, information system architecture and technology architecture principles for EMDS inter data space interoperability		
Business architecture principles	**Information system architecture principles**	**Technology architecture principles**
• A single point of entry can provide access to the data services in the federation of data spaces. • Data sovereignty and trust must be managed across the federation of interoperable data spaces (Chapter 4). • Inter data space interoperability apply to each of the levels of the EIF (Chapter 6). • Minimising dependence and reliance on trusted third parties fulfilling data space interconnectivity intermediary and governance roles should be the goal.	• The full harmonisation inter data space interoperability modes is preferred for inter data space interoperability (Chapter 6). • Full harmonisation of federated data spaces requires federated data space building blocks (Chapter 6). • Fully distributed, reference architectures for federated data sharing are emerging that will minimise the need for centralised data space interconnectivity building blocks (Chapter 6). • To encourage the adoption of federation with existing (mobility) data space building blocks, supporting tools on data space proxies for partial harmonisation should be developed (Chapter 6).	• By default and where applicable, API definitions are based on generally accepted protocols and standards such as those proposed by the Dataspace Protocol, the EU DSSC and the SIMPL initiatives (Chapter 6). • For various technical interoperability aspects (e.g. on data sovereignty, trust and discoverability), independent design decisions can be made on full or partial harmonisation.

EMDS: Inter data space role model

The role model for inter data space interoperability is depicted in Figure 31.

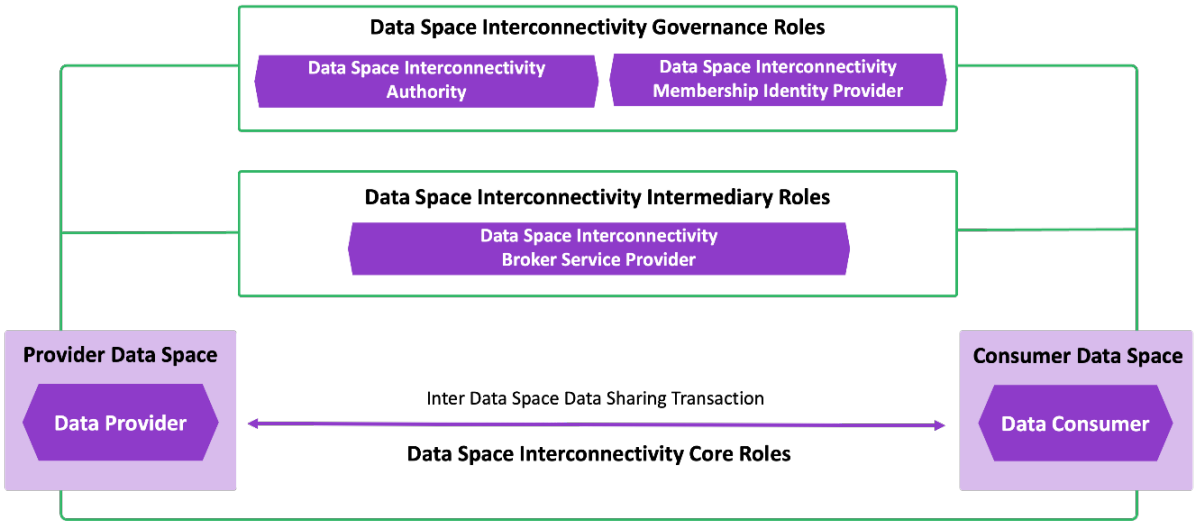


Figure 31: The role model for EMDS inter data space interoperability.

As with intra data space interoperability, three similar categories of roles are distinguished for interconnectivity between data spaces: (1) the data space interconnectivity core roles, (2) the data space interconnectivity intermediary roles, and (3) the data space interconnectivity governance roles. The description of the roles for each category is included in Table 19.

Table 19: Three categories of roles for inter EMDS data space interoperability.

The three categories of roles for inter EMDS data space interoperability and their individual roles
Data space interconnectivity core roles The data space interconnectivity core roles represent the actual data spaces where data sharing transactions are executed.
Provider data space Provider data spaces host participants that share data services and data apps with participants in other data spaces.
Consumer data space Consumer data spaces host participants that request data services or data apps from participants in another data space, i.e. a provider data space.
Data space interconnectivity intermediary roles The data space interconnectivity intermediary roles enable the interaction processes between stakeholders in different data space instances by providing metadata support services.
Data space interconnectivity broker service provider A data space interconnectivity broker service provider manages information (metadata) about individual data spaces, e.g. on the roles they support and data services and data app providers, and consumers they contain. The primary activities of a broker service provider focus on enhancing the discoverability and accessibility of data services offered by stakeholders across various data spaces.

The three categories of roles for inter EMDS data space interoperability and their individual roles
Data space interconnectivity governance roles The data space interconnectivity governance roles coordinate the set of commonly agreed-upon principles between the data spaces and manage the compliance of data spaces to these agreed principles. As such, the data space interconnectivity governance roles manage the agreement framework that governs data spaces and is often referred to as the trust framework.
Data space interconnectivity authority In larger ecosystems of data spaces, the data space interconnectivity authority is responsible for managing the (legal and operational) agreements between individual data spaces, certifying participating data spaces and handling the operations of the federation of data spaces.
Data space interconnectivity membership identity provider The data space interconnectivity membership identity provider offers a service to create, maintain, manage, monitor, and validate identity information on participating data spaces. This is crucial for secure interconnectivity between data spaces and to prevent unauthorised access to data. The provider also includes a certification authority for managing digital certificates of participating data spaces.

EMDS: inter data space building blocks

The building blocks required for realising the various roles in the role model for EMDS inter data space interoperability provides a (software) implementation of capabilities to be performed by roles in the role model.

Figure 32 depicts these building blocks for inter data space interoperability and how they can be mapped onto the role model for inter data space interoperability[318].

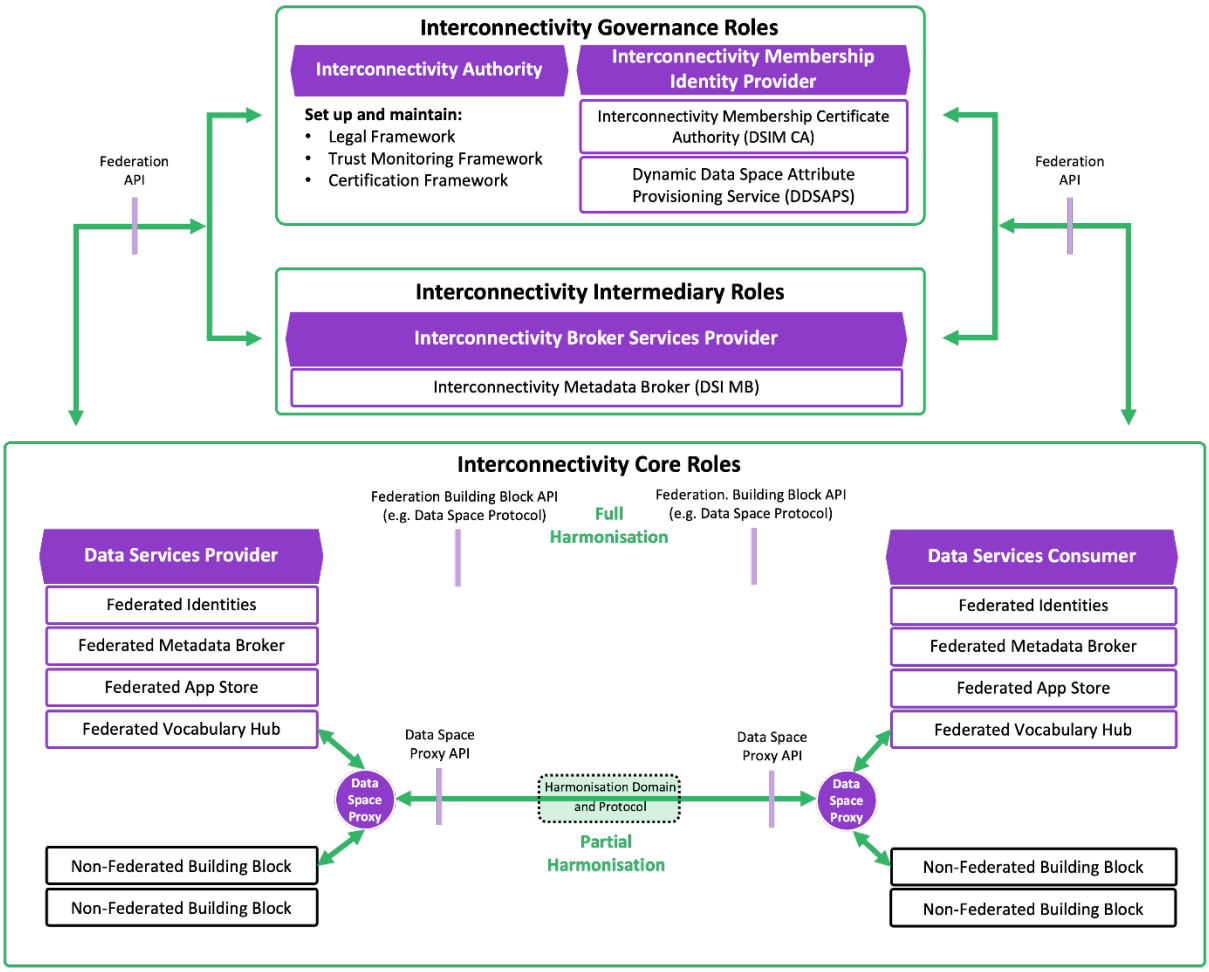


Figure 32: Reference architecture of building blocks for inter data space interoperability.

Table 20 presents an overview of the building blocks in the ISA for inter data space interoperability, categorised into building blocks for the data space interconnectivity core roles, intermediary roles, and governance roles.

Table 20: Building blocks in the ISA for EMDS inter data space interoperability.

Building blocks in the ISA for EMDS inter data space interoperability
Data space interconnectivity governance role building blocks Capabilities to manage the various types of identities for multiple data spaces.
Data Space Interconnectivity Membership Certificate Authority (DSIM CA) Provides certificates for data spaces participating in the federation of (mobility) data spaces used to verify data space membership in data sharing transactions across the federation of data spaces.

[318] Derived and adapted from: The Netherlands AI Coalition Working Group Data Sharing (2022), "Reference guide for inter AI data space interoperability", https://nlaic.com/wp-content/uploads/2023/04/NL-AIC-inter-AI-Data-Space-Interoperability-v3.2.pdf. It contains additional information on the description, API's and (open source) implementations of the individual building blocks.

Building blocks in the ISA for EMDS inter data space interoperability
Dynamic Data Space Attribute Provisioning Service (DDSAPS) Manages and registers the dynamic attributes of the participating data spaces in a federation of data spaces, including the certification status, data space interconnectivity membership status, and applicable legal agreements.
Data space interconnectivity intermediary role building blocks Capabilities to expose, find and connect to the various data spaces.
Data Space Interconnectivity Metadata Broker (DSI MB) Manages, registers, and publishes the participating data spaces in a federation of data spaces.
Data Space Interconnectivity Core Role Building Blocks Capabilities to exercise control over the sharing of data and data apps, ensuring data sovereignty for the entitled party of data or data apps.
Federated building blocks The enabling building blocks within a data space that have the capabilities to be federated with the corresponding building blocks in other data spaces, based on a full harmonisation mode. These federated building blocks can, for instance, be applied to the federated DAPS, the federated metadata broker, the federated app store and the federated vocabulary hub.
Non-federated building blocks The enabling building blocks within a data space provide partial harmonisation capabilities to interact with corresponding building blocks in other data spaces.
Data space proxy Translates between specifications and requirements from a data sharing domain to harmonised specifications and requirements (and vice versa) to achieve interoperability and trust across domains.
Harmonisation profile The harmonised (technical) protocols used within the harmonisation domain, i.e. to communicate between data space proxies.

11. Aligning the EMDS with EU initiatives

The EMDS is an integral feature of the EU Data Strategy aimed at establishing common European data spaces, which is part of a broader EU digitisation initiative. The EU Directorate General for Communications Networks, Content and Technology is responsible for advancing the development of both a common European data space infrastructure and a common European edge and cloud infrastructure.

The following sections address the necessity and potential for aligning the EMDS with both the EU data space initiatives (Section 11.1) and the EU edge and cloud initiatives (Section 11.2), respectively.

11.1. Aligning with EU data space initiatives

As described in Section 1.2, the **DSSC** aims to facilitate the creation of common data spaces that collectively establish an interoperable data sharing environment in Europe across sectoral data spaces. The results of the DSSC will provide input for the upcoming **SIMPL procurement** initiative, which is the open source development initiative of the smart middleware building blocks procured by the EC. These building blocks are intended to enable cloud-to-edge federations and provide support to all major data initiatives funded by the EC, such as the common European data spaces. Hence, the DSSC is currently a leading initiative with which to align the EMDS development and its building blocks.

At the time of finalising this report in September 2023, the work of the DSSC and its blueprint are in an early stage. However, an initial version of the blueprint has been shared with the various CSAs for their review.

As the DSSC and SIMPL form the basis for enabling interoperability of data spaces, they are key for realising the EU ambition of a common European data space. Accordingly, several recommendations can be made for the further development of the EMDS:

- For **building blocks that are key for interoperability** between data spaces, **align, co-develop and** by default **adhere** to the building blocks in the DSSC blueprint and the SIMPL initiative. As addressed throughout this report, this specifically applies to the building blocks for **data sovereignty, trust, and discoverability**.
- For EMDS **building blocks that may be generically applicable** to many sectoral data spaces, by default (and where possible) adopt and align the EMDS building blocks with those that may be developed by the DSSC and SIMPL initiatives. It is further recommended that the EMDS **cooperates with the DSSC and SIMPL in the development** of such generic building blocks. This applies for instance to the building blocks for semantic service provisioning (e.g. vocabulary hub, semantic transformation engine and the data space semantics connector configurator) and for the building blocks for data usage accounting (transaction accounting registry, clearing house, billing engine).
- For **EMDS building blocks that may currently (still) be considered to be specific** for the mobility data space, it should be jointly assessed with the DSSC and SIMPL initiatives whether these building blocks **might have broader interest and value across other sectoral data spaces.** Therefore, it is recommended to consider developing them as generic building blocks, with the EMDS being the first adopter. The EMDS deployment initiative should take the lead in **initiating discussions** on whether the EMDS building blocks should be included in the DSSC and SIMPL roadmaps and actively monitor their development. While this applies to most of the building blocks identified in this report, it specifically applies to:
    - The building blocks to support the "**Event-driven smart contracting for data flow control**" type of data sharing, as described in Section 2.2, building upon the data sharing concept and architectures developed by the **EU CEF FEDeRATED project**. The

DSSC should consider adopting the FEDeRATED Index and Service Registry as the most relevant capabilities. Alignment and integration of the capabilities needed to support this data sharing type within the EMDS architecture may be achieved via a stepwise approach. This involves a functional break-down analysis of IAA-processes embedded in the FEDeRATED (and its distributed FEDeRATED nodes), and their mapping on the generic DSSC building blocks for data spaces as currently being defined.

  - The building blocks to support "**Algorithm sharing for local processing of (sensitive) data**" (Section 9.3), including the building blocks and capabilities related to the app store and workflow management (Section 9.3).
  - The building blocks to support **trust patterns involving delegation or entitlement of authorisation rights**, e.g. including a policy registry with right delegation capabilities. Such trust patterns are often implemented by means of **token-based authorisation structure**. These patterns, commonly used in logistics, should be a key consideration in the development of capabilities within the DSSC blueprint.

- For EMDS **building blocks specific for mobility**, the EMDS deployment initiative should lead their development and make them open source for all specific mobility data space instances **under the EMDS umbrella**. This specifically applies to the data value creation building blocks (Chapter 9) specific to the personal mobility sector, including journey planning, booking and ticketing, billing and payment, in-trip, real-time support and notification and the auxiliary/cross sectoral services. It also applies to the building blocks for the logistics domain, such as logistics visibility/shippers' control tower, transport management (systems), freight cost management, and clearance.

The cross-sectoral and cross-domain character of mobility and logistics highlights the importance of interoperability in these sectors. A preferred approach for enabling federation between data spaces (Section 10.3) is full harmonisation. This approach offers significant advantages in terms of functionality, realisation, and operations. It should therefore be developed as a generic capability, particularly for the key interoperability capabilities related to trust and discoverability. Therefore, the EMDS deployment initiative should closely collaborate with the DSSC and SIMPL initiatives to develop data space interoperability.

11.2. Aligning with EU edge and cloud initiatives

Data sovereignty is a main aspect under the broader umbrella of digital sovereignty[319]. The deployment of data space components requires trustworthy edge and cloud services for both the IT modules providing data space (intermediary) building blocks and the data space connectors. This requires the alignment of the EMDS with the development of a trustworthy EU cloud and edge environment.

A specific area where the interests of the data space developments and cloud and edge services developments intersect, offering important synergies, is **Workload Deployment Orchestration (WDO). WDO**, sometimes also referred to as App Deployment Orchestration, is a building block that enables operators of data space components to define how to select, deploy, monitor and configure their (containerised) modules in the cloud at run-time. It encompasses the deployment, execution and maintenance phases[320]. WDO **requires a trustworthy cloud and edge environment**. The need for workload orchestration will increase as the availability of compute resources and services proliferates

[319] TNO report 2022 R10507, "Bridging the Dutch and European Digital Sovereignty gap", March 2022, https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf.
[320] Casalicchio, E. and Iannucci, S. (2020), "The state-of-the-art in container technologies: Application, orchestration and security. Concurrency and Computation: Practice and Experience", https://doi.org/10.1002/cpe.5668, and Casalicchio, E. (2019), "Container Orchestration. A Survey", Springer, https://doi.org/10.1007/978-3-319-92378-9_14, p. 221–2035.

from large-scale, centralised, and enterprise-grade data centre cloud infrastructures to more dynamic and resource-constrained edge environments, driven, for example, by the rollout of 5G mobile infrastructures.

For existing and emerging data spaces, the development of a WDO provides them with the capability to control the deployment of their components using trustworthy cloud and edge infrastructures. For the cloud service providers, it creates an opportunity to extend the service portfolio with aligned and trustworthy processing services that meet the demand of data spaces.

As an indication of the mutual interest, the **European Alliance for Industrial Data, Edge and Cloud,** which recently published its roadmap[321], has initiated a **task force** aimed at exploring the relationship with data space developments.

The relationship of the EMDS with the developments in the edge and cloud infrastructures will similarly apply to the deployment of other sectoral data space initiatives. Therefore, it is recommended to pursue alignment between the developments of data spaces and edge and cloud infrastructures as a common and aligned approach, such as through the **DSSC blueprint and SIMPL** initiatives.

[321] European Alliance for Industrial Data, Edge and Cloud (2023), "European Industrial Technology Roadmap for the Next-Generation Cloud-Edge", https://ec.europa.eu/newsroom/dae/redirection/document/97129.

12. Conclusions

The role of the EMDS with respect to federated data sharing is becoming increasingly intertwined with the overarching EU ambition of the common European data space. Therefore, the analysis on the building blocks for the future EMDS, as presented in this report, builds and extends upon the work of the leading EU reference architecture initiatives on (the federation of) data spaces. Specifically, this report provides recommendations and building blocks for the future EMDS for each pillar of building blocks outlined in the DSSC taxonomy:

- “Organisational and business building blocks", further distinguishing building blocks for “Business and funding”, “Governance”, and “Legal”, and
- “Technical building blocks”, further distinguishing building blocks for “Data interoperability”, “Data sovereignty and trust”, and “Data value creation”.

Driven by the need for sharing mobility and logistics data in the broader European context, it is recommended to further develop the EMDS towards operationalisation. As part of this operationalisation, three different roles of the EMDS have been identified:

- The role of the EMDS as a coordination body defining joint agreements, protocols, and standards to develop and maintain a federation of interoperable mobility data spaces, organising the community, and promoting adoption.
- The role of the EMDS serving as an operational mobility data space and as data space authority. Participants have the option to register as EMDS members, such as data service or data app providers, data service or data app consumers, or service providers. They can also establish connections with adjacent data sharing infrastructures through federation, such as the NAPs.

  The goal of the EMDS as an operational mobility data space is to accelerate seamless data sharing and promote the adoption of EMDS frameworks and guidelines by data initiatives under its umbrella and beyond. Representative and illustrative use cases for the EMDS will support this goal. The use cases should reflect the various types of data sharing identified in this report, accelerating adoption and interoperability in key areas. Further, the EMDS should be endowed with resources to support key interoperability capabilities for the federation of data spaces: data sovereignty, trust, and discoverability, both across multiple mobility data spaces and with other sectoral data spaces. It is particularly important to focus on establishing a federation between personal mobility and logistics data spaces, adhering to the DSSC blueprint and the components developed by the DSSC and SIMPL initiatives.
  The EMDS, as operational data space should be capable of simultaneously supporting a range of use cases. Some of these use cases may have already been identified as part of the EMDS deployment initiative, while others will emerge, for example under the EDIC for Mobility and Logistics Data. To accommodate these dynamics in current and future use cases, it is recommended that the EMDS be developed with an architecture that clearly separates a “business layer” that can dynamically support a multitude of use cases and a stable “infrastructure layer” equipped with a set of building blocks that can generically support the anticipated multitude and variety of use cases.
  It is worth noting that the longer-term perspective for the EMDS, as an operational mobility data space, is to become a data space instance equal to others within the ecosystem of federated (mobility and logistics) data spaces.
- The role of the EMDS as governing body representing the mobility and logistics sectors within the context of other relevant data space actors and initiatives, including the DSSC, SIMPL, the EDIC, and the EDIB. One of its primary tasks is to define and govern an agreed-upon roadmap

for the operationalisation of both a coordination body and an operational mobility data space, which may potentially involve contributions from other stakeholders.

An important criterion to consider when evaluating these roles for the EMDS is the long-term sustainability of its operations, both for the EMDS as coordination body and the EMDS as an operational mobility data space. Well-organised and well-maintained governance, decision-making and specification processes are necessary to ensure the long-term sustainability of the EMDS, both internally and within the context of other federated data spaces. Adequate representativeness within the EMDS is a key pre-requisite for success, involving both the represented thematic domains and sub-sectors, as well as a representative group of data initiatives and authorities from different countries.