Project deliverable D3.1

Report on existing regulatory frameworks and governance mechanisms for mobility data sharing

Co-funded by
the European Union

Document information

Summary					
Grant agreement	101123520	**Project short name**	deployEMDS		
Deliverable no.	D3.1	**Deliverable name**	Report on existing regulatory frameworks and governance mechanisms for mobility data sharing		
Status	Final	**Due**	M17	**Date**	28/03/2025
Authors	Jenny Lundahl (RISE Research Institutes of Sweden), Aliki Benmayor (KU Leuven), Johan Linåker (RISE Research Institutes of Sweden), Alina Östling (RISE Research Institutes of Sweden), Emmie Nordell (RISE Research Institutes of Sweden), Pauline Wernicke (TU Braunschweig), Håkan Burden (RISE Research Institutes of Sweden), Susanne Stenberg (RISE Research Institutes of Sweden)				
Dissemination level	PU				
Document history	**Version**	**Date**			
	V1.0	21/01/2025 (Internal partners, Advisory Board and EC review)			
	V2.0	28/03/2025 (Final version)			

Legal disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Table of contents

List of tables

List of figures

Project executive summary

The establishment of a common European mobility data space (EMDS) aims to accelerate the digital and green transformation of the European mobility and transport sector. The deployEMDS project contributes to the further development of the EMDS as announced in the European Strategy for Data and the Sustainable and Smart Mobility Strategy. It builds on PrepDSpace4Mobility, a Coordination and Support Action funded under the Digital Europe Programme and is the first deployment action foreseen under the EMDS initiative.

The deployEMDS project advances EU policy priorities by developing a technical infrastructure for an operational data space in the mobility sector. It aligns with the European Data Strategy's goal to facilitate data access, pooling, and sharing. The project supports the European Green Deal's aim to accelerate sustainable and smart mobility, thereby contributing to a reduction in transport emissions. Additionally, it aligns with the Sustainable and Smart Mobility Strategy, ITS Directive, and the NAPCORE project. The diverse consortium of partners implements 16 use cases across nine European cities and regions, aiming to create and deploy an operational data space with a common technical infrastructure. The project aims to make data available in machine-readable format, while facilitating innovative services and applications and contributing to the development of a European mobility data sharing ecosystem.

For further information please visit:

@deployEMDS

www.deployEMDS.eu

Deliverable executive summary

Keywords

Mobility data, data sharing, data governance, data space, policy and regulation, legal landscape

Executive summary

This report provides a preliminary overview of existing regulatory frameworks and governance mechanisms for mobility data sharing. Its primary aim is to evaluate the current situation, trends, and challenges, as well as the governance and regulatory provisions, to inform and guide subsequent project activities.

The report is divided into two main chapters. The first one analyses data sharing and governance aspects, taking into consideration mobility and data spaces. The second provides an overview of the legal framework applicable to data sharing, also outlining the relevance to mobility and this project, as well as some open points that need to be addressed.

More concretely, **Chapter 2** delves into the challenges and opportunities in the governance of mobility data sharing. The following are the focus areas of this chapter:

- After introducing key concepts relevant to our work, we provide **an overview of the current situation, trends, and challenges** in mobility data sharing from a governance perspective. Data sharing is crucial for improving various aspects of mobility. Technological advances and increased collaboration have led to a rise in data generation, sharing, and usage. However, data sharing still faces several governance challenges spanning organisational, legal, and technical aspects. We provide a detailed overview of all three. Our analysis shows that challenges frequently mentioned in the literature are largely the same as those faced by deployEMDS local implementation sites. Challenges among the sites include *organisational challenges* (such as how to organise around data sharing, limited capacity, slow digital transformation, trust issues, opaque data contracts, reluctance to share data of public interest, insufficient financial resources), *legal challenges* (such as navigating legal frameworks, data sharing obligations in tenders/contracts, legal liabilities for data breaches/misuse), *technical challenges* (such as standards harmonisation, integrating legacy systems, ensuring data sovereignty, ensuring data protection, and ensuring data quality), and challenges related to *power dynamics and asymmetries* (such as the challenge of clearly explaining purpose of data sharing and demonstrating societal value).
- **An exploration of governance principles and strategies** for mobility data sharing highlights the importance of governance and data governance for efficient data management, compliance, trust-building, and innovation. Principles such as participation, accountability, and transparency, applicable to both traditional and digital contexts, can guide the development of a governance framework for data sharing, supported by FAIR principles for data findability, accessibility, interoperability, and reusability. Data space governance extends beyond data governance to also include managing partnerships and collaborations to unlock the value of data. Evolving frameworks suggest community-based and purpose-driven approaches that consider domain-specific contexts, emphasise flexibility and adaptability, and focus on both technical and governance building blocks to ensure efficient and secure operation of data spaces.
- **A review of governance in deployEMDS local implementation sites** and similar initiatives using Elinor Ostrom's governance principles aimed to generate knowledge to help actors design governance structures suited to their local conditions (rather than creating a single governance structure). Our examination confirms the importance of the local level for mobility data sharing,

offering benefits like autonomy, community focus and better alignment with local needs. However, challenges include articulating values, strategic guidance, and coordinating across governance levels. Boundaries are not always clearly defined, values and ethical principles are not fully formalised, and rules need to be more explicit. Mechanisms to influence rulemaking are lacking (for stakeholders affected by the data sharing, e.g., local communities and organisations representing citizens), and onboarding strategies are insufficient. Monitoring mechanisms need to be more transparent, and conflict resolution strategies are unclear. We also highlight adapting to mandatory and voluntary requirements to make data spaces more sustainable and responsible. Decision-making power should remain local (to the extent possible), with support from higher levels.

Chapter 3 focuses on the legal landscape and explores opportunities and limitations of legislation on data access and sharing in the mobility sector. The chapter includes sections on the following EU laws:

- The **General Data Protection Regulation (GDPR)** is still the most prominent piece of legislation in the personal data domain, setting strict rules for data protection in the EU, even though the regulatory focus is shifting towards facilitating data sharing and reuse for socio-economic benefits. The GDPR also ensures free movement of personal data within the EU. The **Free Flow of Non-Personal Data Regulation** establishes the same principle of free movement within the EU for non-personal data, promoting digital innovation and cross-border collaboration. There are instances in the use cases of the project's implementation sites where personal data is involved. Challenges that the sites are experiencing include ensuring data subjects rights under GDPR. For data spaces handling personal data, establishing clear roles for GDPR roles is important.
- The **Data Governance Act (DGA)** and the **Data Act (DA)** promote data sharing. The DGA regulates processes and structures to facilitate voluntary data sharing, while the DA clarifies who can create value from data and under which conditions. The increased data availability and facilitation of data sharing benefits data spaces and ecosystems. The DGA also supports the creation of common European data spaces and establishes the European Data Innovation Board (EDIB) to develop guidelines. The DGA extends the legal framework for the reuse of sensitive public sector information with safeguards. It also establishes a framework for data intermediation services to facilitate controlled data sharing, and introduces data altruism, which allows data subjects to decide whether to share their data. These measures create new opportunities for stakeholders interested in accessing, sharing and reusing data. The DA is important for mobility data spaces and ecosystems in several ways. It improves access to mobility data from connected vehicles and infrastructure, fostering innovation in the mobility sector. It also enables public authorities to access and use private sector data in certain situations. It further specifies requirements for data interoperability and sharing mechanisms, ensuring that (mobility) data can be integrated across systems and platforms.
- The **Digital Markets Act (DMA)** and the **Digital Services Act (DSA)** address specific players in the digital economy and aim to create a safer digital environment, protect users' rights, and establish a level playing field for businesses. These laws can indirectly impact mobility data spaces: DMA by regulating large digital platforms and preventing anti-competitive behaviour that might otherwise hinder data sharing in the mobility sector; DSA by improving transparency and accountability of platforms within scope that may be used in mobility services.
- The **Interoperable Europe Act** is introduced to enhance the interoperability of public services across the Member States and facilitate access to and sharing of public sector data across borders. Of particular relevance to the mobility sector, this act can support the implementation of the objectives of the ITS Directive. In particular in border regions, the use of data from different Member States may be needed for development and use of ITS applications. The Interoperable Europe Act promotes cross-border interoperability of trans-European digital services and facilitates the cross-border exchange of data. It can thus contribute to the deployment and use of EU-wide ITS.
- The **AI Act** is the world's first comprehensive AI law, introduced to ensure a high level of protection from harmful effects of AI systems in the EU, while supporting innovation and improving the functioning of the internal market. Even though it deals with AI-systems, this regulation is relevant to

mobility data spaces, providing a framework for developing and using AI, especially high-risk systems, to ensure trustworthiness and safety. Data spaces can offer AI developers access to more data for learning and predictions. Interoperable data spaces facilitate data integration and analysis. The AI Act also sets data quality requirements for high-risk AI systems, which data spaces must ensure their datasets meet if they are to be used in such systems.

- The **INSPIRE Directive** facilitates public access to standardised spatial data, such as data on transport networks, which is of relevance for mobility data spaces and can benefit various applications and services in the mobility field. Some of the project's use cases focus on data on transport networks. (The implementing act on high-value datasets, see below, relies on the INSPIRE Directive in terms of actual datasets and their modes of provision for the definition of high-value datasets in the category mobility.)
- The **Open Data Directive** and the **High Value Datasets Implementing Act** enhance the accessibility and reusability of public sector information. The directive sets out the general framework for making such information available for reuse across the EU and the implementing act specifies specific datasets with high socio-economic potential that the public sector must make reusable as open data and free of charge, such as data on transport networks. This increases the accessibility of such data for various applications in the field of mobility.
- The **Intelligent Transport Systems (ITS) Directive** promotes data availability of data types relevant to ITS services in road transport, such as travel planning and real-time traffic information services. This directive and its delegated regulations require certain road, travel, and traffic data to be available in digital format. Several of the project's use cases focus on such data. Moreover, by establishing common European specifications to ensure that ITS data is accessible, standardised, and shareable across different platforms, interoperability between systems is ensured, which also benefits mobility data spaces. Additionally, the National Access Points (NAPs), where ITS data should be exchanged in all the Member States, are considered an important part of the future EMDS, ensuring that transport-related data is accessible and can be shared effectively.
- The **TEN-T Regulation** is the legal basis for the Urban Mobility Indicators (UMI), which are used to assess and improve urban transportation systems (evaluate mobility performance and identify areas for improvement). No later than 19 July 2025, the Commission shall adopt an implementing act setting out indicators in certain areas. The Member States will then have to provide to the Commission urban mobility data for these indicators covering each urban node. Several of the project's use cases focus on data for UMI indicators.
- The chapter also touches upon additional horizontal legislation that indirectly affects data, such as competition law, contract law, and intellectual property rights. The chapter also includes exploring the intersection of the laws and regulations on data and its use in general, and their impact in relation to sector-specific regulations on mobility.

The work in this report lays the foundation for understanding the current situation and provisions for mobility data sharing from a governance and legal perspective. We will continue to address governance and legal issues relevant to the development of common governance mechanisms for mobility data sharing across borders, and we will release additional deliverables in the future.

List of abbreviations and acronyms

Acronym	Meaning
API	Application Programming Interface
B2B	Business-to-Business
B2G	Business-to-Government
DA	Data Act
DGA	Data Governance Act
DSSC	Data Space Support Centre
EDIB	European Data Innovation Board
EDPB	European Data Protection Board
EMDS	Common European mobility data space
EU	European Union
FAIR	Findable, Accessible, Interoperable and Reusable
GDPR	General Data Protection Regulation
IDSA	International Data Spaces Association
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
MaaS	Mobility-as-a-Service
NAP	National Access Point
OECD	Organisation for Economic Co-operation and Development
SME	Small and Mid-size Enterprises
SWD	Staff Working Document
UN	United Nations
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific
WP	Work Package

1 Introduction

1.1 Purpose of the deliverable

Work Package (WP) 3 of the deployEMDS project focuses on developing common governance mechanisms for mobility data sharing across borders, taking into account relevant national and EU legislation. This report describes the outcome of the initial work of WP 3, which involves mapping existing regulatory frameworks and governance mechanisms for mobility data sharing. This serves as a basis for understanding the current situation and provisions for sharing mobility data. Specific governance challenges and legal aspects of governance will then be further addressed in policy labs. The WP will also develop legal tools for compliance and interoperability. Finally, the WP will develop a multi-level governance framework ready for deployment, as well as forward-looking recommendations for the future EMDS.

1.2 Intended audience

This report provides deployEMDS partners with an overview of the existing regulatory frameworks and governance mechanisms, along with the challenges and legal aspects associated with mobility data sharing. This overview can help partners navigate this complex field and lays the foundation for our subsequent project activities aimed at developing common governance and legal mechanisms for mobility data sharing. The report may also interest various actors involved in mobility data sharing across Europe, including policymakers, authorities, companies, and other stakeholders.

1.3 Methodology

The main research tools have included:

- Desk research and review of relevant documents, including legal texts, research papers and reports, deliverables from related projects, etc.
- A survey, interviews and workshop with the local implementation sites in the project.
- Virtual workshops to discuss data space governance and build understanding around the limitations and opportunities within existing regulations, processes, and structures for sharing mobility data. The first workshop focused on challenges and opportunities in data space governance, featuring internal project participants and external invitees. Related projects shared their insights and lessons learned (PrepDSpace4Mobility[1], MobiDataLab[2], GREAT-project[3], and the Open Traffic Data Ecosystem in Finland[4]). A second workshop discussed governance practices for data sharing within and between local data spaces through the EMDS.
- We did a review of governance in deployEMDS local implementation sites using Elinor Ostrom's governance principles. We used a design science research approach (Wieringa, 2014), iteratively designing and validating solutions within the framework of mobility-centric data-sharing initiatives (data spaces). The purpose was not to create one governance structure, but rather knowledge that can help actors to design a governance structure for their local conditions. In practice, this work involved: 1) a literature review of academic and grey literature; 2) a case survey of four initiatives:

[1] https://mobilitydataspace-csa.eu/.
[2] https://mobidatalab.eu/.
[3] https://www.greatproject.eu/.
[4] https://www.fintraffic.fi/en/trafficecosystem.

Trafiklab (Sweden), HSL DevCom (Finland), Mobilidata program (Flanders), and OpenStreetMap (international); 3) a semi-structured interview survey with actors from the implementation sites, focusing on Ostrom's principles and adapted to each case; and 4) an online workshop with the implementation sites along with external experts to validate and enrich the results, followed by additional interviews to address remaining knowledge gaps.

- We also participated in workshops, seminars, and webinars arranged by others for the exchange of information and experiences in (mobility) data sharing, as well as related governance and legal issues, and had discussions with related projects (e.g., DSSC[5], DS4SSCC[6] and GREAT-project[7]).

1.4 Scope and delimitations

This report aims to provide an overview of governance mechanisms and regulatory frameworks for mobility data sharing and associated challenges. It is important to note that this is only an overview and is by no means exhaustive. The field of mobility data is vast and constantly evolving. Governance models and legal considerations vary between jurisdictions and contexts. Given the subject's breadth, the report illustrates the current landscape without covering every detail. Readers seeking more detailed information are encouraged to consult additional sources. While the project focuses on deploying data spaces, this report takes a broader perspective. Many challenges and strategies to overcome challenges recur between different data sharing models. Different models can also complement each other and interact in larger data ecosystems.

1.5 Structure of the deliverable and links with other work packages/deliverables

The aim of this report by **Work Package (WP) 3** of the deployEMDS project is to offer an overview of existing regulatory frameworks and governance mechanisms for mobility data sharing. This serves as a basis for understanding the current situation and provisions, and to inform subsequent project activities.

WP 3 focuses on the deployment of common governance mechanisms across borders, taking into account relevant national and EU legislation. The work is divided into **four main tasks**:

1. We map governance and regulatory structures in mobility data sharing as our **first task**. This includes exploring the current situation and emerging trends in mobility data sharing, and related governance challenges and opportunities. It also involves a preliminary examination of how relevant laws and regulations and standards impact the landscape. This initial work lays the foundation for subsequent activities and is the focus of this report.
2. Specific legal and governance challenges are addressed in policy labs, which is the **second task** of this WP. The participatory policy lab process helps to frame, discuss, and solve policy barriers in collaboration. The partners of the consortium form the various policy lab groups that discuss and co-create in several workshop iterations, starting with the challenges and aiming to reach a common understanding of the situation and the way forward to overcome these challenges.
3. A **third task** involves the development of legal tools. This includes analysing legal challenges in the implementation of mobility data spaces and providing guidance based on entry points ("triggers"). The task also includes exploring techno-legal implementations and smart contracts. A "Report on legal tools for compliance and interoperability in the mobility data spaces" (D3.2) will provide a toolbox to facilitate the deployment of data spaces and support the further development of the EMDS.

[5] https://dssc.eu/.
[6] https://www.ds4sscc.eu/.
[7] https://www.greatproject.eu/.

4. Findings in previous tasks will inform our continued work in the **fourth task** developing governance mechanisms for mobility data sharing within and across borders. A multi-level governance framework for the urban mobility data space will be developed, along with operational recommendations for deployment and future-oriented recommendations toward the EMDS. Our final deliverable is the "Report on multi-level governance framework with business and governance mechanisms" (D3.4).

The rest of this report is structured as follows:

- **Chapter 2** delves into the challenges and opportunities in mobility data sharing governance. It begins by introducing key concepts relevant to our work, followed by a discussion on the situation, trends, and challenges in mobility data sharing from a governance perspective. We then discuss governance principles and strategies for mobility data sharing. Finally, we analyse the governance of the deployEMDS implementation cases.
- **Chapter 3** focuses on the legal landscape for mobility data sharing. It starts with an introductory overview, and then it provides detailed introductions to various laws and regulations relevant for data, both general and sector-specific data legislation. This chapter also explores the intersections between horizontal and sector-specific legislation, and includes additional legislation that serves broader purposes, such as competition law, contract law, and intellectual property rights.
- **Chapter 4** presents our conclusions and next steps.
- **References** and **annexes** can be found at the end of the report.

2 Mobility data sharing governance – challenges and opportunities

This chapter explores governance challenges and opportunities in mobility data sharing. It begins by introducing key concepts relevant to our work, followed by a discussion on the situation, trends, and challenges in mobility data sharing from a governance perspective. We then discuss governance principles and strategies for mobility data sharing. Finally, we analyse the governance of the deployEMDS implementation cases.

2.1 Key concepts relevant to our work

2.1.1 Mobility data

2.1.1.1 Data

The term '**data**' usually refers to facts, statistics, or information represented in various forms and used for reference, analysis, or calculations. It can be numbers, text, images, audio, and more, and can be structured (like databases) or unstructured (like text or images). Data can be categorised in various ways depending on its characteristics, use, context, or how it is organised. For example: structured, unstructured, or semi-structured data; quantitative or qualitative data; real-time, static, or historical data; open or closed data; personal and non-personal data; etc. There is also metadata, i.e., data about data, providing information about other datasets.

Data and *information* are related but not the same. As Daniel Keys Moran said: "You can have data without information, but you cannot have information without data". Data is the raw material from which information and knowledge are derived. When given context, data becomes information, providing valuable insights for decision-making and innovation. However, data and information are sometimes used interchangeably in legal contexts. For instance, under the GDPR personal data refers to any *information* relating to an identified or identifiable natural person.

Legal definitions of data can be found in EU legislation. In Article 2(1) of the Data Governance Act (DGA) and Article 2(1) of the Data Act, 'data' refers to 'any digital representation of acts, facts, or information and any compilation of such acts, facts, or information, including in the form of sound, visual, or audiovisual recording'. There are also other legal definitions of data and different categories of data in EU legislation. An interesting pair of definitions regarding data concerns (non-)personal data: 'data' means "data other than personal data" (Article 3 of the Free Flow of Non-Personal Data Regulation – EU, 2018), while 'non-personal data' means "data other than personal data" (Article 2 of the DGA – EU, 2022a).

Data is also defined in **standards**. ISO/IEC 2382:2015[8] defines data as "reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing", where processing can be carried out by "humans or by automatic means". The latter definition is referred to in the ISO 8000-series on data quality. The ISO/IEC 5259-series on data quality for analytics and machine learning does not make an explicit reference to a definition of data but refers to the online browsing platform[9] where

[8] International Organization for Standardization - Online Browsing Platform, ISO/IEC 2382:2015 Information technology — Vocabulary, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:2382:ed-1:v2:en.
[9] International Organization for Standardization – Online Browsing Platform, https://www.iso.org/obp/ui#home.

the definition from ISO/IEC 2382 can be found (among others). The 5259-series is among those international standards that are currently under consideration in CEN and CENELEC's work on harmonised standards for the AI Act (EU, 2024c).[10]

Note: It is **important to know which policies are applicable** for the activities and organisations under consideration as it has an impact on what data refers to and what that implies in terms of rights and responsibilities.

2.1.1.2 Mobility data

There is no single, universally accepted definition of '**mobility data**'. The definition and scope can vary depending on the context and the actors involved in providing or using the data. Furthermore, mobility intersects with various sectors such as technology, infrastructure, energy, and urban planning. This interconnectedness makes it challenging to draw clear boundaries but also highlights the dynamic nature of the mobility sector and its potential for innovation and collaboration across different fields.

Thus, mobility data can refer to **a wide range of data related to the movement of people, vehicles, and goods**. For instance, it includes data describing people's movements and modes of transport (Snaith, 2020), data generated by digitally-enabled mobility devices or services (Estrada et al., 2022), spatial data like data on transport networks (such as data as in the INSPIRE Directive and Implementing Regulation on HVDs, see Section 3.3.1 and Section 3.3.2), and transport and traffic-related data for intelligent transport system services (such as data according to the ITS Directive, see section 3.3.3).

Mobility data can be **used for** improving transportation systems, urban planning, developing smart city solutions, and more. The data can be **collected from** various sources, ranging from classical methods like standing by the street counting movements and conducting travel surveys or interviews, to modern methods enabled by the digital revolution, such as collecting data through connected devices like mobile phones, shared micromobility vehicles, app-based navigation systems, or advanced sensors on roads and streets.

The **deployEMDS project implements 16 diverse use cases** (more use cases may be added later) across nine European cities and regions: Barcelona, Flanders, Milan, Stockholm, Tampere, Budapest, Lisbon, Sofia, and Île-de-France. The implementation sites focus their use cases on for instance data for mobility planning, special travel information, public transport operation, and multimodality. This involves different kinds of mobility data. **Data products** in the use cases include, for example, road infrastructure data, traffic rule data, environmental zone data, public transport data (both static and real-time, such as bus service availability, routes, timetables, position, occupancy, passenger boarding and drop-off), multimodal data, data on dynamic incidents and roadworks, data on mobility services (e.g., micro mobility, car sharing, and bike sharing services), mobility demand, pedestrian accessibility data, electric vehicle charging information, multimodal traffic counts, dynamic and real-time traffic data, meteorological data, air quality data, MaaS usage data, and more. This demonstrates the breadth of data that can be considered for mobility use cases.

2.1.2 Open, shared and closed data

Data can be classified as open, shared or closed depending on its level of accessibility:

- **Open data** is openly accessible to all. It is data that anyone (e.g., companies, citizens and media) can access, use or share without any kind of restrictions. However, free to use does not have to

[10] CEN/CLC/JTC21 – Artificial Intelligence, Work programme, https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D.

mean free to access; there may be costs related to the access of open data, for instance it might require technological resources (DSSC, 2024).

- **Shared data** is harder to define and exists in "shades". It is data that is shared with others but has some kind of restriction and is not available for anyone to use. Use of data can be restricted due to various reasons, including intellectual property rights and data protection regimes.
- **Closed (or private) data** is data that can only be accessed by its subject, owner or holder.

To understand what data is open, or what restrictions apply to data, standardised licences are often used, e.g., the Creative Commons (CC) licences.

The Open Data Institute (ODI) has developed a data spectrum, drawing from a number of research projects, to visualise the different means and levels of access to data – from open to shared to closed data (ODI, 2020).

2.1.3 Data sharing

Data exchange can take different forms, such as a **transfer**, making data available to both partners, or **access**, which may be limited in time, content, or scope (Reiberg, Niebel, & Kraemer, 2022).

Some argue that data sharing involves controlled access for specific stakeholders, differing from open data, which is unrestricted (Global Data Barometer, 2021). However, there are **different definitions** of data sharing, and **opening data** can also be considered a form of data sharing. The important distinction between shared and open data lies in the level of access and restrictions applied (see Section 2.1.2).

A **legal definition** of 'data sharing' can be found in Article 2(10) of the Data Governance Act: "the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge".

In the DSSC's glossary, data sharing **in the context of data spaces** refers to a full spectrum of practices related to sharing any kind of data, including all relevant technical, financial, legal, and organisational requirements (DSSC, 2023). Data sharing definitions can also be found in e.g. the OECD's work (2021).

In mobility, **data sharing** and **data reporting** both involve data exchange but serve different purposes and stakeholders. According to ITF (2021), 'mobility data sharing' refers to data shared among market actors and other stakeholders that enables the delivery of mobility services and supports the functioning of transport markets, while 'data reporting' refers to data provided by stakeholders and market actors to public authorities that enables the latter to monitor, guide and intervene to enact public policy. Data reporting comprises some element of compulsion. Thus, in mobility, data flows through both data sharing and reporting, supporting market functions and public policy objectives, and contributing to the larger data ecosystem.

There is also '**data sharing by regulation**', where data sharing is obligatory under a certain regulation. It may regulate which data is to be shared, with whom, and in what way. For example, the ITS Directive requires certain actors to make specific data publicly available. Similarly, the Data Act establishes rules for public bodies to access and use private sector data for public interest purposes, allowing them to compel data holder to share data under certain conditions.

2.1.4 Governance, data governance and data space governance

2.1.4.1 Governance

There is not one, but many definitions of governance. Simply put, it is the process of making decisions about an entity (whether it is a country, organisation, or corporation); it is not about individual actions or decisions.

Here are a few examples of **governance definitions** (paraphrased):

- UNESCAP (n.d.): Governance is the process of decision-making and the process by which decisions are implemented (or not), applicable in various contexts such as corporate, international, national and local governance.
- Commission on Global Governance (1995): Governance is the sum of the many ways individuals and institutions manage their common affairs. It is a continuing process through which conflicting or diverse interests may be accommodated and co-operative action may be taken. It includes both formal and informal arrangements. (As Keping (2017) notes, this definition has four features: governance is not a set of rules or an activity, but a process; this process is not based on control, but on coordination; it involves both public and private sectors; it is not a formal institution, but continuing interaction.)
- World Economic Forum (2019): Governance involves making decisions and exercising authority to guide behaviour through rules, incentives, social norms, guidelines, standards, policies, ethical principles, or command structures. It extends beyond governments to private organisations, civil society organisations, and social contexts.
- Fritzenkötter et al. (2022): Governance covers political, institutional, and administrative rules, practices, and processes (formal and informal) for decision-making and implementation, accountability and stakeholder interactions.
- van der Waal (2020): Governance is a process, driven by a model, focusing on control and organising power within a framework of rules, relationships, systems, and processes.

At a **workshop** that we conducted in January 2024, we asked the participants to share their thoughts on what governance means to them, identify key elements of effective governance, and discuss aspects of good versus bad governance, among other questions.

- The participants provided various interpretations of governance, highlighting its multifaceted nature:
  - Many participants emphasised the importance of rules, decision-making processes, and structures.
  - Governance was also associated with responsibilities, control, and the roles of individuals and organisations in making decisions.
  - The responses ranged from conceptual definitions such as “a model and a practice” and “overarching strategies” to more practical aspects such as “rules for collaboration” and “functional data space”.
- When asked about the key elements of governance, participants identified several crucial aspects:
  - The most frequently mentioned elements were rules, roles, structure, and responsibility.
  - There was a strong emphasis on legal frameworks, agreements, and organisational aspects, indicating the importance of a solid foundation for governance.
  - Clear and transparent communication, and clarity in roles and responsibilities were highlighted as essential for effective governance.
  - Participants also stressed the importance of alignment, trust, and cultivating relationships to ensure smooth operations and effective governance.

Responses to other questions we discussed have been integrated into other sections of the report.

Governance comes in the form of **principles, models, structures, and mechanisms**. Definitions for these sub-concepts can vary depending on context and organisation, but here are some ideas:

- **Governance principles** can be said to be the fundamental rules, guidelines or values that shape the overall approach to governance and, at a high level, inform decision-making and behaviour. In the context of data sharing, these principles can include transparency, accountability, data privacy and security, to ensure that data is shared responsibly and ethically.
- **Governance models** can be said to be the practical implementations of the governance principles (i.e. how governance should be structured and implemented). In our context, the governance model outlines the approach, framework or system to, on the one hand, manage, control and create value

from data, on the other hand, manage and oversee the organisation/data space. A governance model can be centralised or decentralised. A centralised model might involve a single authority overseeing all data sharing activities, while a decentralised model might distribute responsibilities across multiple entities. Each model has its own advantages and challenges, depending on the context and objectives. For instance, a centralised model might be better suited to ensure consistency and standardisation, while a decentralised model might allow more flexibility but, on the other hand, require stronger coordination. There can also be federated models that combines elements of both centralised and decentralised models, which might balance control and flexibility.

- **Governance structures** can be said to be the organisational setups chosen to support the governance model. This includes defining the roles and responsibilities within an organisation or a data space/ecosystem. For example, a governance structure can define who has the authority to make decisions (for instance about data sharing), who is responsible for compliance, how different stakeholders should interact, etc. Organisational setups can involve establishing boards, committees, and working groups to facilitate governance.
- **Governance mechanisms** are then the specific tools, methods or processes to implement and enforce the governance principles and models on how data should be shared and managed in the organisation (a specific organisation or the data ecosystem). In the data sharing context, these mechanisms can include policies, procedures, audits and reviews, and technologies that ensure data is shared according to the established rules. Examples can also include detailed guidelines, data access controls and compliance monitoring systems. In comparison to governance principles, governance mechanisms are more detailed guidelines.

In **summary**, based on the above, the governance principles are the high-level guidelines (e.g., transparency, security); the models, the practical implementations of the principles (e.g., centralised vs. decentralised); the structures, the organisational setups (e.g., roles, responsibilities); and the mechanisms, the tools and processes (e.g., access controls, audits). However, it should be emphasised once more that there is no uniform taxonomy for these concepts, and it is difficult to draw sharp boundaries between them. In Section 2.1.4.2, we explore the concept ‘data governance’, and in Section 2.1.4.3 the concept ‘data space governance’.

2.1.4.2 Data governance

Despite its widespread use, there is no consensual definition for ‘data governance’. Instead, there are **multiple definitions** (Abraham, Schneider, & vom Brocke, 2019; Farrell et al., 2023). The definitions can differ based on, for example, the context, focus, and scope. The term was initially predominantly technical in nature, but its interpretation has expanded over time.

Broadly it can be defined as “a system of rights and responsibilities that determine who can take what actions with what data” (Curry et al., 2022) or “the exercise of authority and control over the management of data” (Abraham et al., 2019).

Abraham et al. (2023) reviewed 145 publications on data governance to identify common characteristics, leading to the following definition: “Data governance specifies a cross-functional framework for managing data as a strategic enterprise asset. In doing so, data governance specifies decision rights and accountabilities for an organization’s decision-making about its data. Furthermore, data governance formalizes data policies, standards, and procedures and monitors compliance.”

There are also **other definitions** in the research field (e.g., Benfeldt, Persson, & Madsen, 2020; Farrell et al., 2023; Janssen et al., 2020; OECD, 2022a; Micheli et al., 2020) that range from broad to more detailed, vary from technical to socio-technical focus, and emphasise different aspects (such as rights and responsibilities, control and authority, governance methods, or lifecycle management). By recognising these definitions with their varying focuses and emphases, we can appreciate the multifaceted nature of data

governance. Depending on the specific context and needs, one definition (or a combination of definitions) may be more suitable than another.

Note that a distinction should be made between *data governance* and *data management*: the former refers to what decisions must be made and who makes those decisions, whereas the latter is about making those decisions as part of the day-to-day execution of data governance policies (Abraham et al., 2019).

The are definitions in the **standards landscape** as well. For instance, the Institute of Electrical and Electronics Engineers (IEEE) defines data governance as the "Execution and enforcement of authority over the definition, production, and usage of data and data related assets".[11] The definition is then reused in the ISO/IEC 5259-series (mentioned above in Section 2.1.1.1). There are a number of standards that relate to governance in terms of quality management (ISO 9001 on quality management systems, ISO/IEC 27001 on management of information security, ISO 42001 management of Artificial Intelligence systems, etc.) which can further describe how and when execution and enforcement is carried out.[12]

What about **legal definitions**? The Data Governance Act (DGA) (see Section 3.4.1) does not define data governance. There are other regulations that explicitly refer to data governance, such as Article 10 of the AI Act (see Section 3.7), but do not provide an explicit definition.

According to Torre-Bastida et al. (2022), **data governance entails** defining, implementing and monitoring strategies, policies and shared decision making over the management, collection, analysis, sharing and use of data assets as well as related aspects, such as data rights, data privacy, and data security, among others.

Moreover, they explain that the meaning of data governance varies across **different levels**. At the **micro level** (intra-organisational), it focuses on maximising the value of data assets within the organisation. At the **meso level** (inter-organisational), it involves common principles and rules agreed upon by a group of organisations within a trusted data community. At the **macro level**, it encompasses measures supporting national or international policies, strategies, and regulations regarding data. However, despite the varying goals and scopes at each level, they should be aligned throughout the data life cycle, forming a governance continuum. For instance, the GDPR is a macro-level governance measure that requires internal translation within organisations at the micro level to ensure compliance (Torre-Bastida et al., 2022).

Data governance levels are also discussed in, for example, Davies (2022), who argues that at an **organisational level**, data governance generally translates into a focus on internal policies and their implementation, compliance with external regulations, and the creation of cross-functional frameworks and responsibilities for managing and extracting value from data as a business asset. At the **state level** – whether national, regional, or international – this can lead to a focus on the development and implementation of policies, standards, laws, regulations, agreements, and practices that cover the management of data within countries and the transfer of data across jurisdictional boundaries. Abraham et al. (2019) divides the organisational scope of data governance into (a) intra-organisational and (b) inter-organisational. The **intra-organisational scope** determines data governance within a single organisation (at the project or organisational level) while the **inter-organisational scope** encompasses data governance between organisations or for ecosystems of organisations.

[11] Institute of Electrical and Electronics Engineers, 7005-2021 - IEEE Standard for Transparent Employer Data Governance, https://ieeexplore.ieee.org/document/9618905/definitions#definitions.
[12] International Organization for Standardization, Management system standards, https://www.iso.org/management-system-standards.html.

In Section 2.1.4.1 on the concept of governance, we described governance principles, models, structures, and mechanisms. According to Abraham et al. (2019), **governance mechanisms in data governance** comprise structures connecting different functions such as business, IT, and data management, processes and procedures for decision-making and monitoring, and practices supporting active participation and collaboration among stakeholders. These mechanisms help the organisation plan and control data management activities to ensure data is managed effectively, aligns with organisational goals, and complies with regulations. Governance mechanisms in data governance include both structural and procedural elements. **Structural mechanisms** encompass roles and responsibilities and the allocation of decision-making authority, while **procedural mechanisms** comprise a data strategy, policies, standards, processes, procedures, contractual agreements, performance measurement, compliance monitoring, and issue management. Moreover, there are **relational mechanisms** for facilitating stakeholder collaboration, which involve communication, training, and the coordination of decision-making.

2.1.4.3 Data space governance

Data space governance goes beyond *data governance* by also focusing on how to govern the partnerships and collaborations needed to unlock the value of data. Data space governance serves as the cornerstone for overseeing data spaces comprehensively while also ensuring compliance with legislation, ethical standards, and interoperability between data spaces.

It is relevant to differ between *organisational governance* (governing the data space) and *data governance* (governing the data). Both aspects of governance help ensure that the data space operates effectively, and that the data being shared is reliable and useful. Organisational governance might include issues such as legal structure (organisational form), purpose and scope, overarching strategies, roles and responsibilities, rules and policies, decision-making, risk management, and conflict resolution. Data governance might include issues such as how data is collected, stored, protected, and shared, how data quality is ensured, ensuring it is accessible to intended actors, and ensuring compliance with laws and regulations (e.g., GDPR).

In the glossary developed by DSSC (2023), '**data space governance**' refers to "the processes to develop, maintain and enforce the governance framework of a particular data space". The explanatory text states that it includes organisational governance and data governance, whose scope is within a particular data space. In the glossary, the term '**data space governance framework**' refers to the set of "principles, standards, policies (rules/regulations), agreements and practices that apply to the governance, management, and operations (including business and technology aspects) of a data space as well as to the enforcement thereof, and the resolution of any conflicts".

According to Torre-Bastida et al. (2022), **governance in the data space context encompasses** business, legal, sociological, political, and organisational aspects. It can span from contractual, organisational, and operational agreements to technical standards and tools, and from goals and principles to laws and regulations. It is implemented through overlapping legal, administrative, organisational, business, and technical measures and procedures that define the roles, rights, and responsibilities of each participant.

2.1.5 Data spaces and similar concepts

2.1.5.1 Data spaces

Data spaces have been around for quite some time, but the concept got a real boost through the European Strategy for Data (European Commission, 2020a). Data spaces can be seen as data sharing facilitators. In essence, they provide a structured yet flexible environment where data can be accessed and shared under agreed-upon terms and conditions. By bridging the gap between data providers and consumers, they make it easier to share data while maintaining control and security.

Data spaces can be understood and analysed from both governance and technical angles (data.europa academy, 2023). **From a governance perspective**, they are federated data ecosystems with shared policies and rules, where users can securely, transparently, reliably, easily, and uniformly access data, while data owners have control over access and use of their data. **From a technical perspective**, they can be seen as a data integration concept without needing common database schemas or physical data integration but based on distributed and integrated data stores as needed.

A useful definition of '**data space**' can be found in the DSSC's glossary: a "distributed system defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and enables one or more use cases" (DSSC, 2023). Among other things, this definition means that the governance framework should enable secure and trustworthy data transactions between participants and support trust and data sovereignty. This means that it is more to data transactions than just data transfer; the terms and conditions governing these transactions are important. The DSSC's definition has evolved over time, with changes reflecting a growing emphasis on governance, security, and practical implementation aspects. The DSSC also define '**data space initiative**' as "a collaborative project of a consortium or network of committed partners to initiate, develop and maintain a data space".

There are also **other definitions** of data space, for instance by the OPEN DEI initiative (Nagel & Lycklama 2021), Gaia-X Hub Germany (Reiberg, Niebel, & Kraemer, 2022), International Data Spaces Association (IDSA, n.d.), and Data Spaces Business Alliance (DSBA, 2023), with commonalities as well as differences. Several definitions emphasise the importance of trust and security in data sharing. Most definitions mention some form of infrastructure (decentralised, federated, or standardised) that supports data sharing. Most definitions highlight the need for commonly agreed principles, policies, rules, or standards to facilitate data sharing. Several definitions specifically mention data sovereignty. The concept of a data ecosystem involving various stakeholders is also a recurring theme. The DSBA definition explicitly mentions value creation, while it is an implicit goal in the other definitions.

It is also relevant to take a look at similar concepts and how they are defined, for example the concept of '**data ecosystem**'. There is no generally accepted definition for the concept. According to Oliveira et al. (2019), a data ecosystem may be defined as a complex socio-technical network that enables collaboration between autonomous actors in order to explore data. Such ecosystems provide an environment for creating, managing, and sustaining data sharing initiatives. Reiberg, Niebel and Kraemer (2022) explain that a data ecosystem can be regarded as a higher-level unit compared to a data space. In addition to the exchange processes that are the content of the data space, the data ecosystem includes upstream and downstream processes of obtaining and processing data.

There are also other structures that stakeholders can adopt to manage, control, and create value from their data. There is **no one-size-fits-all approach** to data collaboration or its governance; principles, processes, and practices can be customised in numerous ways to be "fit for purpose" (Fritzenkötter et al., 2022).

Some examples of **data sharing models** (note that these models are not set in stone; they can occur in combination or in hybrid forms) are presented in the following:

- In '**data partnerships**', organisations agree to share and mutually enrich their datasets, including through cross-licensing agreements. This facilitates joint production or cooperation with suppliers, customers, or even competitors, and enables the data holder to create additional value and insights that a single organisation could not achieve alone. Challenges include ensuring fair data-sharing agreements between partners with different market power, and addressing privacy and intellectual property concerns. In partnerships between competing companies, data sharing can risk implicit collusion, such as cartels and price fixing. Public-private data partnerships also pose challenges due to the dual role of governments as both authority and service (data) provider, raising questions about applicable rules and what the private sector should exchange in return for the data (OECD, 2020).

- '**Multi-party data sharing agreement**' is when multiple parties make an explicit agreement regulated by a contract to share a specified set of data, often triggered by the need of only a few of the participants to access data owned by others. The model is for one-time data sharing which is time- and purpose-bound and one-directional (from the suppliers to the requesters) (Huyer & Cecconi, 2020).
- A '**data pool**' involves entities transferring and aggregating data in a jointly controlled medium. This communal approach allows data subjects and data holders to jointly decide on norms and principles for data collection, usage and access. It enables access to aggregated data that would otherwise be unavailable. However, there is no clarity or agreement as to the legal status or concrete mechanisms governing such pooled resources (Bayamlioğlu & Benmayor, 2023).
- '**Data commons**' can be described as a collective governance system of a shared data resource and its use (Ruhaak et al., 2021). To address societal goals, data as a commons requires the participation of a broad range of stakeholders in articulating what public value means (Bria et al., 2023). There are some key principles that characterise healthy commons (see Section 2.5 for details).
- A '**data trust**' is a form of data stewardship which binds the trustee and the trustor under certain fiduciary duties. Trustees must act in the best interests of trustors. Data trusts integrate data from multiple sources, involve diverse stakeholders, and can use collaborative or centralised models depending on the context and purpose. 'Public' or 'civic' trusts establish relationships between data subjects or legal entities and public bodies, allowing public bodies to access, aggregate and use data held by individuals and entities (Bayamlioğlu & Benmayor, 2023).
- A '**data marketplace**' is a transactional "market" where data providers and users buy and sell data. It informs buyers about data quality, scope and content. Data marketplaces are typically electronic venues or platforms that provide infrastructure for participants to meet and define data use terms and other contract elements. Various technical solutions and services enable transparent tracking of data transactions (Bayamlioğlu & Benmayor, 2023).
- The Data Governance Act (DGA) introduces '**data altruism organisations**', allowing citizens to share their data with third parties to support public interest goals. Data altruism means "the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest" (Article 2 DGA).
- A '**data lake**' is a repository for storing structured and unstructured data at any scale, without the need for prior structuring. It supports various analyses, from dashboards and visualisations to big data processing, real-time analytics, and machine learning. Accessing the data lake means accessing all its data (but not necessarily in an organised manner). Using a fishing analogy, a data lake requires users to catch the fish themselves, while data spaces are like fish markets (data.europa academy, 2023).

2.1.5.2 Common European data space(s) and the EMDS

The European Strategy for Data (European Commission 2020a) aims to create a single EU market for data, allowing data to flow easily between countries and sectors while respecting European values and rules.

Common European data spaces are "purpose or sector specific or cross sectoral interoperable frameworks for common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives" (recital 103 of the Data Act).

The Commission has proposed common European data spaces to facilitate trusted and secure data pooling and sharing **in strategic sectors**, such as manufacturing, agriculture, health and mobility. These will

gradually be interconnected to form a pillar of the single market for data (European Commission, 2022a; European Commission, 2024).

In addition to data sharing obligations set out in legislation, data in the common European data spaces will be made available on a **voluntary basis** and may be reused against compensation, including remuneration, or free, depending on the decision of the data holder.

Over time, the sectoral data spaces may **harmonise** their technical, operational, functional, and legal aspects, leading to a more uniform "soft infrastructure" encompassing design decisions, rules, agreements, and processes for sharing, managing, and using data. This harmonisation should enable citizens, companies, and governments to maintain control over their data even across different sectors and applications (Nagel & Lycklama 2021, 2022; Farrell et al., 2023).

The European Data Innovation Board (**EDIB**) will support the development of these data spaces by publishing guidelines and identifying necessary standards and interoperability requirements.

The **common European mobility data space (EMDS)** was announced by the European Commission in the Strategy for Data (European Commission 2020a) in February 2020 and later mentioned in the Sustainable and Mobility Strategy (European Commission 2020b) in December 2020. It aims to accelerate the transport sector's digital transformation and leverage data for sector-wide and societal benefits.

Some **key points**[13] about the envisioned EMDS are summarised:

- The EMDS will make **large amounts of mobility data available** in machine-readable format from various sources, such as transport companies, travel agencies, and authorities, accessible to all Member States. It will facilitate access and sharing of data from existing and future transport and mobility data sources, **build on existing initiatives** and promote **interoperability**. It will not create one vast centralised database but will provide a framework for **interlinking and federating different data ecosystems**. It will be based on a **decentralised approach**, where data remain with participants or in existing domains and databases. The EMDS will help actors more easily find, access, and use relevant data, benefiting sectors like automotive and public transport.
- It will build on existing **legislation and infrastructures**, promoting interoperability through tools supporting convergence on governance and infrastructure. Recent legislative initiatives, such as the revised ITS Directive, contain obligations to share data relevant to the EMDS (see Section 3.3.3).
- **Participants** in the EMDS include data providers and data users (incl. data intermediaries and data-altruism organisations), as well as marketplaces and service providers that want to create value by offering, discovering, accessing and using mobility data across the vast range of ecosystems.
- The **EMDS framework** will have technical (e.g. infrastructure elements) and governance dimensions (a set of rules, procedures, roles and responsibilities, etc.) that will include building blocks, standards, an interlinking layer, and a governance structure. The framework will facilitate data access, reuse and sharing in a federated, trusted and secure environment between mobility data ecosystems and with other sectoral data spaces.
- The Commission will analyse existing **standards**, focusing on data quality, comparability, level of service, and accessibility. They may issue non-binding recommendations to foster standardisation convergence and enable interoperability within a federated framework.

[13] This is based on information in the European Strategy for Data (European Commission 2020a), the Sustainable and Mobility Strategy (European Commission 2020b), the Commission's communication on EMDS (European Commission 2023a), and the Commission's two staff working documents on common European data spaces (European Commission, 2022a; European Commission, 2024).

- The **interlinking layer** of the EMDS will connect existing and emerging mobility and transport data spaces, enhancing data discoverability and accessibility.
- The **governance structure** must align with relevant EU legislation, define clear roles and responsibilities to ensure its effective establishment and operation, ensure the active participation of different stakeholders, and respect principles of fairness and transparency.
- The EMDS **components** will adhere to requirements in the EU's cross-sectoral data legislation and will align with the generic framework for common European data spaces, incorporating recommendations from the EDIB, the DSSC, and relevant building blocks, e.g., provided by SIMPL. The envisioned concept of the EMDS will necessarily evolve as implementation progresses and requires a certain flexibility so that the overall framework can be adapted.

The EMDS will leverage **preparatory and complementary initiatives** backed by the Commission. One of these initiatives was the preparatory Coordination and Support Action (CSA) PrepDSpace4Mobility[14] (October 2022–September 2023), which provided recommendations on common design principles and building blocks, and explored options for a unified data-sharing framework in the mobility and transport sector. Another initiative is this deployment action, deployEMDS[15] (launched in November 2023), which aims to implement data space building blocks through use cases focused on urban mobility data sharing. Additionally, a CEF study[16] (launched in January 2024) focuses on the EMDS governance and a layer that will interlink the various domains, followed by a deployment action (planned Q2 2025). Other relevant actions supported by the Commission include the Data Spaces Support Centre (DSSC)[17] and the open-source smart cloud-to-edge middleware platform (SIMPL)[18] initiative.

2.2 Current situation and trends in mobility data sharing

Data sharing is not an end in itself but a means to address real mobility challenges and improve urban mobility. This section of the report delves into the current state and trends in mobility data sharing.

Data sharing to address urban mobility challenges

By integrating methods of data sharing in the mobility sector, we can achieve more efficient transport systems, improved traffic management, and better-informed urban planning. By leveraging data sharing, actors can create innovative solutions that address urban needs and promote sustainable mobility. Data sharing can provide insights into, for example, traffic patterns, public transport usage, and pedestrian flows. There are also environmental benefits, as mobility data can help identify strategies to reduce emissions and promote sustainable transport options. Additionally, data on accidents and road conditions can improve road safety by identifying high-risk areas. Real-time data allow users to make informed travel decisions, avoiding congestion and choosing efficient routes and modes of transport. Collaboration among authorities, private companies, and the public can create smarter, more efficient, and sustainable mobility systems.

[14] https://mobilitydataspace-csa.eu/.
[15] https://deployemds.eu/.
[16] Study in support of the creation of the common European mobility data space (EMDS) for the European Commission by the consultants Ricardo Nederland B.V. and Ricardo, in collaboration with VTT and Wavestone. Study contract no. MOVE/B4/2023-463.
[17] https://dssc.eu/.
[18] https://simpl-programme.ec.europa.eu/.

The **deployEMDS current 16 use cases** aim to optimise transportation systems and infrastructure through mobility planning, provide travel information to users, enhance the efficiency and reliability of public transport services, facilitate seamless integration between different transport modes, and more.

Increased data sharing can drive innovation and competitiveness in the EU economy, particularly in AI development, leading to more innovative products and services, smarter and greener cities, and reduced carbon footprints through optimised energy use and traffic management (European Parliament, 2023). AI is becoming essential for transport automation in all modes (European Commission, 2020b, 2024). For instance, AI can help automated vehicles (AVs) handle more complex tasks and achieve higher automation levels (Lundahl, 2024a). Other examples include AI solutions for predictive awareness in road traffic safety contexts, which need to be fed with different categories of mobility data (AI Aware Scale Up, 2023). AVs, as well as advanced driver assistance systems (ADAS) and navigation systems, need access to various data related to the road network and its attributes, such as traffic rule data (Lundahl, Sobiech & Thidevall, 2023).

Situation and trends in mobility data sharing

The last decade has seen an **exponential increase in data generation, collection, and use**, driven by the datafication of daily life. Digitally connected devices, data infrastructures, and platforms have enabled new forms of data generation and extraction at an unprecedented scale (Pavel et al., 2022). Data, a non-rival good, can be shared and reused across various applications and users for analyses, product development, decision-making, and more.

However, the benefits depend on data availability and accessibility. **Access to data unlocks its potential value** and determines who can benefit (Coyle et al., 2020a). Wider accessibility allows more individuals and organisations to leverage data for insights and applications, maximising its use and distributing its benefits more broadly. However, data sharing and use can generate externalities (positive or negative), impacting those not directly involved (Coyle et al., 2020a; OECD, 2020, 2022a). This is something to consider from a governance perspective to ensure that the benefits and costs of data use are fairly distributed.

Data sharing is evolving due to technological advancements and increasing recognition of its value. Trends include new data streams from different sources, growing platforms and ecosystems for data sharing, more open data from governments through web portals, and cloud services connecting data across companies. There is a shift towards decentralised models where data remains at its source but is accessible to others, an approach to balance data control and accessibility. Privacy-preserving technologies are being developed to allow data sharing without compromising privacy. Trends can also be seen in policy and legislation. Since 2020, with the European Strategy for Data and new data legislation, the EU has sought to facilitate and increase trust in data sharing.

Until now, bilateral data sharing based on contracts has been common. **New models** are emerging, such as centralised data hosting infrastructures and data marketplaces that enable discovery and reduce transaction costs where data is not held in a central repository. The next step in the evolution of data spaces involves creating links between participants in a federated, distributed data model, with tools for searching and accessing data across industries, companies, and entities (data.europa academy, 2023). Several data ecosystems and spaces have emerged in recent years (PrepDSpace4Mobility, 2023), such as the German Mobility Data Space[19], Fintraffic's Traffic Data Ecosystem[20], and Eona-X[21]. Reference architectures, building

[19] Mobility Data Space, https://mobility-dataspace.eu/.
[20] Fintraffic, Traffic Data Ecosystem, https://www.fintraffic.fi/en/trafficecosystem.
[21] https://eona-x.eu/.

blocks, and data-governance mechanisms are provided by initiatives such as the IDSA[22], NAPCORE[23], Gaia-X[24], the FEDeRATED project[25] and iSHARE[26].

However, **data sharing remains limited** (IDSA 2024a; (Tenopir et al. 2011; Gabelica, Bojčić & Puljak 2022; Watson 2022) due to cultural, mandate, and coordination challenges, as well as privacy, security, and resource constraints. (Read more about data sharing challenges in Section 2.3.)

Data sharing in the **dynamic mobility field** can give rise to challenges as well as increased potential for innovation and collaboration across different fields. Compared to other domains, mobility involves a particularly diverse set of stakeholders, each bringing their own perspectives, constraints, and information needs. Stakeholders include public transport authorities, urban planners, and private companies, each with different priorities and standards. Transport modes operate under different regulations and technologies, and transport systems vary geographically due to local policies and infrastructure. The domain is evolving with new mobility providers such as car sharing, bike sharing, and ride sharing, as well as public transport operators introducing new services to serve the changing needs of their riders, such as on-demand options, and enhanced customer interactions through mobile apps, digital ticketing, and real-time information (MaaS Alliance, 2021). These trends are noticeable in what the deployEMDS use cases are focused on.

Mobility-as-a-Service (MaaS) integrates various mobility services, including public transport, car sharing, ride sourcing, and bike sharing, into a single service (Smith, 2020), which requires stakeholders to share data for seamless mobility (PrepDSpace4Mobility, 2023). MaaS providers integrate different transport options and services into a unified digital solution, managing data across operators, modes, and locations, sometimes across borders. However, transport data is often proprietary or localised, complicating inter-communication (MaaS Alliance, 2021). An open, cooperative framework is needed for technical and operational interoperability (PrepDSpace4Mobility, 2023). Public authorities would also benefit from better traffic management through integrated data analysis. Currently, data is shared in both persistent (semi-static) and streaming formats but remains fragmented and organised in silos. Nonetheless, existing mobility data ecosystems can be found across Europe and new ones are constantly emerging.

Connecting various mobility data platforms using data space concepts can create a comprehensive and integrated data ecosystem. Mobility data are often generated and used on a regional level, either by communities or by fleet operators in the private economy, and mobility data platforms are often created on a regional level, e.g., by smart city initiatives, to pool local services. Additionally, there are national data platforms with various focus areas and also commercial data services. Integrating these different platforms into a broader ecosystem using data space concepts can **make regional mobility data visible on a national level** (Pretzsch, Drees, & Rittershaus, 2022).

The Sustainable and Smart Mobility Strategy (European Commission, 2020b) emphasises data sharing for the digital and green transformation of the mobility domain and calls for a common **EMDS** to facilitate this. The creation of the common EMDS will need to take into account the fragmented nature of the mobility domain, with diverse stakeholders bringing their different perspectives and needs, and a significant legacy of initiatives that have their own governance, architecture, and platforms (European Commission, 2021).

[22] https://internationaldataspaces.org/.
[23] https://napcore.eu/.
[24] https://gaia-x.eu/.
[25] https://www.federatedplatforms.eu/.
[26] https://ishare.eu/.

2.3 Data sharing challenges

2.3.1 Common data sharing challenges from a governance perspective

Keeping in mind that data sharing is not an end in itself but a means to address real mobility challenges and improve urban mobility, this subsection focuses on the challenges of data sharing. Compared to Section 2.3.2 (challenges perceived by the project's local sites), this section addresses challenges commonly experienced in data sharing.

We consider governance challenges within organisational, legal and technical arrangements of data sharing, as well as power dynamics and asymmetries between actors that are affected by, or have an effect on, how data is accessed, controlled, shared and used. We sort the challenges according to this categorisation, while being aware that there may be other conceivable categorisations and different perceptions of which category a certain challenge belongs to. Many challenges are also interconnected and influence several aspects of governance. Addressing multifaceted challenges might require a holistic approach that considers organisational practices, legal frameworks, technical solutions, and the broader power dynamics at play.

2.3.1.1 Organisational challenges

Here we explore the organisational challenges related to the governing of data and data sharing, e.g. transparency, accountability, responsibility, oversight/monitoring, representation of participants in data governance bodies and their ability to contribute to the decision-making processes, enforcement, etc.

Capacity limitations

An OECD report (2023) states that smart cities generate vast amounts of real-time data to improve public services, but their ability to manage this data is strained. Challenges include rapid growth in data volume, multiple stakeholders, insufficient financial resources, lack of business models for financing data collection, limited access to skilled experts, compliance issues with data legislation, and data security risks.

PrepDSpace4Mobility (2023) highlights that some organisations struggle to offer data or engage in data sharing due to a lack of skills and expertise. They emphasise the importance of improving technical support and addressing this skills gap to facilitate active participation, especially among potential data providers.

In Sweden, as an example, the Agency for Digital Government (DIGG) coordinates and supports the digitalisation of public administration. According to DIGG (2020, 2022, 2023; see also an interview with DIGG in "& Fika", 2022), public administration faces significant challenges in digitalisation. Challenges include varying digital maturity, insufficient capacity and expertise, and technical debt. Collaboration among authorities is limited. Public administration has valuable data but lacks awareness of its location and how to make it accessible and specified. Efforts to open and share data face low motivation, requiring external pressure, e.g., by EU legislation. Political support and clear governance are necessary to drive progress.

Other European countries face similar challenges in digitalisation, and it is not limited to digitalisation in public administration but also in businesses. Statistics from Eurostat (2024) show that many European countries face issues such as varying digital maturity, insufficient capacity and expertise, and disparities in digital infrastructure. While some countries like Finland and Sweden are leaders in digital skills and technology adoption, others lag behind. Common challenges include shortage of skilled workers and need for better digital infrastructure. Digitalisation efforts vary by region and sector, and addressing these challenges is crucial for a uniform and effective digital transformation across Europe.

An example of digitalisation in public administration relevant for our project is the digitalisation of traffic regulations. Reliable traffic rule data is increasingly needed as road transport systems become more automated and connected. National traffic rules are often supplemented by local or regional traffic regulations

which often make up the largest share of traffic rules in a country. Digitalising them presents significant challenges. A Swedish study (Lundahl, Sobiech & Thidevall, 2023) found that many municipalities lack the necessary human resources, technical solutions, and financial resources. The lack of financial resources is a major obstacle, preventing investments in IT solutions necessary for the digitalisation of traffic regulations. When local and regional authorities do not digitalise their traffic regulations themselves, the quality of the traffic rule data can be affected.

Data ownership[27] issues and unwillingness to share data

A study on urban data platforms (Sheombar et al., 2020) highlights challenges of unclear or fragmented data ownership, hindering data sharing in cities. Data is often owned (controlled) by system suppliers (who cannot or do not want to share data with the city) or locked into specific systems in municipal departments. Most data collected in cities is designated for a specific system and not shared with anyone else. This means that data ownership is not always clear. They argue that if it is not clear who owns a dataset (the one who gives others access to the dataset and sets the rules and conditions for access and use), then it should not be shared, even as open data. Scattered data ownership is also problematic, as stakeholders cannot access data stored by third parties, such as a parking garage operator who cannot share data owned (controlled) by the company that manages the signs and displays in the parking garage.

Bria et al. (2023) argue that urban data, mostly controlled by private companies, should be more accessible for public good. Private companies collect and control most urban data in public spaces but are reluctant to share it. There are often no legal requirements for companies to share this data. Sharing only happens under limited circumstances. This limits access for city administrations, citizens, and the innovation ecosystem. The authors argue for the development of legal tools, organisational capabilities, and digital public infrastructures to ensure urban data benefit society. They suggest urban data should be considered a data commons, open and free to use for society unless valid reasons to keep it private. It calls for citizens and stakeholders to define public value and interest and determine the best ways to govern data for public good.

A World Bank report (2021) notes that data holders may hesitate to share data due to data protection and security concerns, needs to recover investments, or attempts to gain market power. This creates tension between data dissemination and the incentives to accumulate data for private commercial gain.

OECD (2019) mentions that social and economic risks associated with the possible revelation of confidential information, e.g., personal data and trade secrets, are often the main rationale for individuals and organisations not sharing their data. Farrell et al. (2023) highlights similar concerns. Private operators like ridesharing providers are often reluctant to share data collected as a by-product of delivering their services (see also Bria et al., 2023). Administrations can attempt to establish ad-hoc public-private data sharing agreements, but these may be suboptimal due to high costs and low data granularity.

Those who share data may lack visibility or control over third-party uses but bear the burden of responsibility and reputational impact misused (Coyle et al., 2020b), inhibiting willingness to share data. Coyle et al. also mention problems with uncertainty about others' behaviour from ambiguity in norms, regulations, licensing,

[27] The notion of 'data ownership' is complex but is often used as a legal shorthand to describe for example a party's control over specific data. However, it lacks a clear legal definition at the EU level, and it is not clear what the scope of such an ownership right would be. It is complex especially since data differs fundamentally from physical goods – it is, for example, non-rivalrous, non-exclusive, and inexhaustible. Traditional civil law ownership is unsuitable for data. Intellectual property rights may apply to specific types of data, such as creative works or databases involving significant investment, but these rights are limited in scope. Recent EU legislation, particularly the Data Act, moves away from the ownership paradigm and instead focuses on regulating access and usage rights (Graux, 2024b).

or terms and conditions, and limited ways to assess trustworthiness.

Many organisations value data but are reluctant to share it, sometimes even within their own departments. IT departments often manage data access and may not approve all requests from data scientists in line-of-business areas (Davis, 2018). This reluctance may stem from concerns about data security, privacy, or resource constraints. Additionally, internal barriers to effective data sharing and use include a lack of awareness between departments about what data the organisation has available.

Further highlighted by PrepDSpace4Mobility (2023) is stakeholders' reluctance to share data without legal mandates, particularly in B2G settings. Public entities struggle to acquire desired data due to the lack of a regulatory framework compelling commercial companies to share it. The report suggests cities could include contract clauses requiring private mobility companies to share relevant mobility data, but ideally, a comprehensive regulatory framework would eliminate the need for such individualised efforts.

While some cities are more advanced in settling agreements with private operators (of shared mobility services), others are confused about which data to request or how much to push. This confusion stems from privacy issues, lack of capacity, or a missing clear purpose, among other reasons (Estrada et al., 2022).

Identifying the right data owner can also be challenging due to data silos from various data ownership structures. Stakeholders' concerns about privacy, data sovereignty, data quality, and commercial sensitivity complicate the process. While stakeholders are generally aware of data relevant to their value creation, they struggle to identify and access the data. Effective data-sharing mechanisms hinges on accurately identifying the right data owner (PrepDSpace4Mobility, 2023).

From the data owner's perspective, it can also be challenging to identify shareable data and define the scope and conditions for access and reuse, especially for individuals and SMEs (OECD, 2019).

Incentive shortfalls

OECD (2019, 2022) highlights that it may require significant investments to collect data and enable its sharing and reuse. Investments include overcoming legal, technical and skills-related barriers, and reducing risks through technology solutions. Data holders may lack incentives to share data if costs and risks outweigh their benefits. Individuals are more likely to share personal data if they expect benefits. Both organisations and individuals need sufficient returns on investments, such as through licensing fees or value-added services, to encourage data sharing. Incentives are often too low when returns on investments are insufficient.

Others also note that lacking, low or misaligned incentives create barriers to data sharing (e.g., Coyle et al., 2020b; World Bank, 2021; European Commission, 2020d; Fritzenkötter et al., 2022). For instance, Coyle et al (2020b) explains that the incentives of those who collect data, those who could use data, and those who are affected by it, are mismatched, and there are trade-offs to consider when increasing access to data for public good. Organisations may have little visibility or control over third-party uses but bear liability and reputational risks if misused. Also, assessing current and future value of data is challenging and costly, making it hard to justify improving data quality or accessibility.

Costs of providing or sharing data

Bria et al. (2023) note that significant transaction costs hinder data sharing. Coyle et al. (2020a) also highlights the costs of creating, maintaining and publishing data, leading governments to consider charging for public sector data, but charging can impede the use and value of data. Other sources also mention the costs of engaging data users for the effective reuse of open data (see below).

Engaging users to ensure reuse of open data

Open access alone does not guarantee effective reuse of data. Beyond technical measures like APIs, additional efforts are often required to engage users effectively (OECD, 2019). For instance, Transport for London incurs annual costs of approximately GBP 1 million to publish open data, with a significant portion allocated to maintaining and facilitating communities of data users (Deloitte, 2017). This highlights the importance of investing in user engagement to maximise the value of open data.

Balancing openness and protection

Open data is the most prominent approach used to enhance access to data (OECD, 2015, 2019). This approach is widely adopted by governments, organisations, and institutions to promote transparency, innovation, and public participation. Many governments have open data portals where they publish datasets on various topics, such as transportation, health, and the environment. These initiatives help to improve access to information and can drive economic growth by enabling new services and products.

However, openness brings risks to privacy and data protection, intellectual property rights, digital and national security, and ethical concerns (OECD, 2022b). As more data, especially personal data, are shared and reused, the risks of misuse increase as well (World Bank, 2021). The optimal level of data openness depends on the context, including social, economic, and cultural factors (OECD, 2019). The OECD (2022b) stresses balancing risks with benefits like innovation and improved public services, recommending robust data governance frameworks to protect privacy and security while enabling responsible data use.

There are also risks with aggregated open data, as large amounts can pose national security risks. Organisations need to consider these risks when opening additional data (Nationell dataverkstad, 2022).

Coordination problems and information asymmetries

The data economy faces coordination issues and information asymmetries (Coyle et al., 2020b). Coordination issues arise when those who have data do not know who needs it, and those who need data do not know who has it. Information asymmetries occur when some have more knowledge about datasets, including knowledge about quality, usage, or existence. There may be various reasons, but among other things, information asymmetries stem from data being an “experience good” – its value is known only after use, making quality assessment difficult until data is acquired. This can lead to lower prices for high-quality data and its eventual exit from the market (OECD, 2022c).

Information asymmetries can, in turn, result in or exacerbate power imbalances, where those with more information can exploit it to their advantage, or inefficiencies in the data economy through, for example, missed opportunities for innovation and collaboration.

Balancing stakeholder interests in data spaces

A challenge for data spaces is that stakeholders may have divergent goals and specific data needs, which can be difficult to reconcile (ENISA, 2024). Finding common ground and resolving potential conflicts is crucial for effective data sharing and collaboration, benefiting all stakeholders.

Trust issues

The importance of trust – both between actors and for engaging actors – in data sharing contexts has been emphasised by many (e.g., PrepDSpace4Mobility, 2023; World bank, 2021; Arnaut et al., 2018; Dutkiewicz et al., 2022; Curry et al., 2022; Farrell et al., 2023; European Commission, 2020d; Sheombar et al., 2020; Eisenträger et al., 2024). A lack of trust is often mentioned as a barrier for data sharing (World bank, 2021; Huyer & Cecconi, 2020; European Commission, 2020a).

Trust issues, including understanding how to build trust and mitigate challenges in data cooperation, are perceived as challenges at the local implementation sites (see Section 2.3.2) and were selected as one of the topics for the project's policy labs in task 3.2. Thus, we will address this challenge in the policy labs.

2.3.1.2 Legal challenges

Here we explore the legal challenges related to the governing of data and data sharing, e.g. complex legal landscape, legal compliance and risks, data protection, etc.

Unclear legal nature of data

Despite data being the centre of policy discussions, it remains difficult to clearly delineate 'data' from a legal perspective. The 'data' definition we have is a technical one (see standard ISO/IEC 2382-1:1993, then replaced by ISO/IEC 2382:2015) which has been integrated into various EU laws. Different EU laws also introduce neighbouring to 'data' notions that encompass or are based on data. Examples include software, databases, digital services and digital content. EU law also distinguishes data per category, such as personal data (GDPR), non-personal data (Free flow of non-personal data Regulation) or dynamic data (Open Data and ITS Directive). Moreover, data is increasingly being seen as a transactional object with value, reflected in new laws treating data as a commodity. Data are therefore heterogeneous and under EU law serve different functions. This leads to the next challenge – a complex and fragmented legal landscape.

A complex and fragmented legal landscape

Several reports highlight the complex and fragmented legal landscape surrounding data sharing (e.g., PrepDSpace4Mobility, 2023; Bayamlioğlu et al., 2022; Bria et al., 2023). This is because 'data' are not treated homogeneously under EU law, so several pieces of legislation can apply simultaneously. Dealing with data protection, liability issues, and IP rights creates legal challenges (European Commission 2021). Moreover, stressed by Curry et al. (2022), there is a tension between horizontal and sector-specific regulation of data, and how to position the role of the data spaces in this tension field constitutes a challenge. Varying legal definitions of data add complexity, making it challenging to understand which legal requirements apply. In addition to data-related legislation, a large body of EU legislation indirectly affects data sharing, contributing to the legal patchwork (Dutkiewicz et al., 2022).

This fragmentation is evident in the diverse legal structures that individual actors must navigate, often leading to confusion and difficulty in understanding legal obligations. The existence of many and sometimes conflicting laws introduces legal risks in data sharing, hindering effective data utilisation (Bria et al., 2023).

In chapter 3, we describe legal frameworks that are relevant to data and data sharing. It should be noted that several legal frameworks can apply simultaneously and overlap. Determann (2018) states that the intricate net of legal frameworks, together with multiple parties involved in data creation, contributes to uncertainty around data ownership. This challenge is amplified when data is created and shared across national borders. (Therefore – contracts to fil the gap, see further below.)

Lack of an EU mandated data ownership right

While many stakeholders use the term "own" when referring to data, no such right exists under EU law. Ownership has traditionally been used for property, i.e. physical goods where possession of a good by one party automatically excludes the use by another. One exception is intellectual property rights, where ownership is attributed to an intangible asset, based on legal fiction. But the same cannot apply *mutatis mutandis* to data given its nature. Data are essentially non-rivalrous, ubiquitous (easily duplicable and transferable without detrimental effect to the original data) (OECD, 2015) and not excludable (Martins 2020).

Graux (2024b) examined whether data can be "owned" under traditional civil (property) law, intellectual property rights, or data protection law, and concluded that none of these legal regimes support a data

ownership right. He stressed that data “ownership” is a concept problematic under EU law but also moot as the key point is not “ownership”, but rather who has the right and ability to access and use it. That is why in the Data Act, the Commission focuses on data holders rather than “owners” and on providing access and usage rights relating to those data holders.

Legal uncertainty and fragmentation in transposition of laws

Legal uncertainty creates barriers to sharing data. Bria et al. (2023) highlight the difficulty in respecting the rights of individuals and companies under data protection laws when sharing data. Uncertainty is furthered when the transposition of EU directives is not harmonious, i.e., Member States may have adopted different approaches to a legal regime. One example concerns the transposition of the 2019 Open Data Directive which has some exceptions to the general obligation to make public sector information available for reuse, such as confidential data or data covered by third-party intellectual property rights. A study from 2018 – so concerning the law that preceded the Open Data Directive – revealed the divergences in adoption. For example, the national rules on reuse excluded documents containing personal data in Estonia, Greece, Ireland, Italy, the Netherlands, Slovenia and Sweden. Conversely, in France, Germany and Poland, documents containing personal data were not excluded (Deloitte, 2018).

The same holds true for the implementation of the ITS Directive (and its delegated regulations) and the deployment of National Access Points (NAPs) to facilitate the exchange and reuse of data. In 2021, the European ITS Platform published a report on NAPs (covering the EU Member States, Norway and the United Kingdom) (EU EIP – Annual NAP Report 2020). The report sets out that real-time traffic information is the most implemented NAP. Indeed, currently, 23 countries have a (partly) operational NAP for such information. Four other countries are implementing or have concrete plans to implement a NAP. However, only 16 Member States have NAPs for multi-modal travel information services, either fully or partially operational. In eight other Member States, the NAPs are in progress or there are concrete plans to implement them.

Ensure data protection

Ensuring data protection when sharing data remains a challenge. When it comes to personal data, the challenge already starts with the definition of what this is. The definition of personal data in the GDPR is very broad. Almost any data can potentially become personal data, making it difficult to distinguish between personal and non-personal data (Bayamlioğlu et al., 2022). Personal data under the GDPR is information that, in itself or in combination with other information, can be linked to a natural person. Different pieces of information can together lead to the identification of a certain person and thus constitute personal data. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data. Personal data that has been made anonymous so that the individual is no longer identifiable is not considered personal data, but for the data to be truly anonymous, the anonymisation must be irreversible (see Section 3.2.1). Moreover, some mobility data that are personal data are difficult to anonymise (Bayamlioğlu et al., 2022). Additionally, as several reports by the OECD (2015, 2019) highlights, advancements in data analytics and AI, combined with the increasing volume and variety of available datasets and the ability to link them, make it easier to identify individuals from data that initially appeared to be anonymous. This suggests that anonymised data may not be as anonymous as one might think. The dynamic and ever-expanding nature of the notion of personal data makes it difficult to clearly designate non-personal data once and for all (Bayamlıoğlu, 2021). As Dutkiewicz et al. (2022) note, technological advances can make it possible to turn anonymised data into personal data, so it is always safer to treat all data as personal. Also, according to the World Bank (2021), the distinction between personal data and non-personal data is becoming increasingly blurred due to the widespread mixing and processing of different data sources using sophisticated algorithms that may render non-personal data personally identifiable. There are also mixed datasets consisting of both non-personal and personal data. The GDPR applies in the case of mixed datasets even if personal data represents only a small part of the dataset. Personal data is present in several of the deployEMDS use cases (see Section 3.2.1).

According to the European Union Agency for Cybersecurity (ENISA, 2024), there are two main privacy challenges in data sharing environments like data spaces: the input privacy problem, which is about allowing the processing of shared data while ensuring it cannot be reverted to its original form, and the output privacy problem, which is about preventing individuals from being singled out or identified after the computations performed by the sharing environment have taken place. Both issues are critical for data privacy and security and must be addressed with appropriate technical measures while adhering to GDPR principles.

There are additional challenges with personal data under the GDPR, such as obtaining meaningful consent, which can be revoked (ITF, 2022). This complicates using consent as a legal basis for processing personal data. Furthermore, the meaningfulness of consent can be questioned. Studies show that it would take the average person 76 days a year to read all consent documents for websites and apps (Madrigal, 2012).

In our project, mobility data is in focus. Mobility data can contain elements that make it possible to directly or indirectly identify a person, for example through time and location of a vehicle/object (if it can be linked to the person) or even direct information about a traveller's identity. Speed of travel can, if indicating a speeding violation (a criminal offence in several countries) (and linked to a certain individual, e.g., through a vehicle's registration number), be considered 'sensitive personal data' and require special protection measures. See Section 3.2.1 for more information.

Contracts to fill the gap

As already mentioned, the complex legal landscape and involvement of multiple parties in data creation lead to uncertainty around data ownership, especially across borders (Determann, 2018). Accordingly, stakeholders often turn to contract law to define rights related to data control, access, and use (OECD, 2019; PrepDSpace4Mobility, 2023). While contracts can be tailored to specific needs, uncertainties can increase transaction costs and disadvantage those in weaker bargaining positions like individuals and SMEs. This can be attributed to a lack of incentive to share data, and where there are arrangements they can be perceived as unfair (OECD, 2019). OECD further mentions that this has prompted government initiatives to guide data sharing agreements. (Although not mentioned as a solution here, data spaces can manage data sharing, respecting data owners' rights and enabling collaboration. They offer legal, technical, and organisational infrastructure to address data ownership complexities and promote a more equitable data economy.) However, contract law is largely national, which brings challenges considering different jurisdictions.

Lacking legal mandates to share data

Some data sharing challenges have both organisational and legal dimensions. There is sometimes a lack of willingness to share data when there is no legal mandate. Some even say that data sharing occurs only under narrow, predefined circumstances, with few laws introducing rights and obligations for data sharing (Bria et al., 2023). The EU's Data Act, for example, allows public bodies to access and use private sector data for public interest purposes under certain conditions (see more on this in Section 3.4.2). Another example is the ITS Directive requiring certain actors to make specified ITS data publicly available. National examples include the German Transport Act (Bria et al., 2023), the UK's Bus Services Act 2017[28] mandating bus operators to open data on bus timetables, France's legislation on sharing private sector data in the public interest (OECD, 2019), and Finland's pioneering law requiring transport service providers to open essential data, such as data on routes, stops, timetables, prices, availability and accessibility, in machine-readable form via open interfaces (Pursiainen, 2020).

[28] Bus Services Act 2017, www.legislation.gov.uk/ukpga/2017/21/contents.

However, these examples are exceptions. The problem still remains that stakeholders – primarily private ones – can refuse to share their data under different justifications or pretexts, often because they prefer to monetise them rather than make them open. While contractual freedom is a legally guaranteed right and entering contractual negotiations is always possible, the situation can become particularly problematic for valuable data held by powerful stakeholders, creating an imbalance in power dynamics.

Public bodies sometimes use contractual obligations to access data of private actors. This can be done as license terms agreed with operators running a service or activity in a city, as a condition in public procurement, or as a condition for receiving public funding, etc. For example, municipalities and electric scooter operators have entered into voluntary agreements including provisions on sharing data about how the scooters are used in the city (Müller, Andersson, Fjällström & Lundahl 2024; Lundahl, Stenberg & Faxer, 2023). However, our discussions with city administrations, for instance at a project internal workshop and other project meetings, have revealed several challenges. There is often a lack of awareness and established procedures to ensure access to data, such as including data sharing obligations in procurement and contracts. There is sometimes a lack of knowledge on how to formulate these obligations effectively, ensuring that the city actually receives the necessary data in the end. Additionally, a data platform may be needed to receive and analyse data, which can be a financial obstacle for some cities. Experiences from other projects (e.g., the Network Micromobility[29]) show that cities can help each other by exchanging experiences and discussing solutions around data sharing obligations. This is something we could do in our project.

Unclear or missing licensing information for datasets

Farrell et al. (2023) note that unclear or missing licensing information in datasets hinders efficient reuse. Cross-border scenarios complicate this further due to language differences, risking copyright infringement and breach of access conditions. This issue primarily falls under legal governance but also has organisational aspects, such as managing and communicating licensing information effectively.

Unclear role of data intermediation services

The European Commission's data strategy put forward as one key aspect of increasing data sharing the creation of data intermediation services. These services are meant to act as neutral facilitators in data spaces, aiming to build trust and facilitate transactions. The Data Governance Act (see more in Section 3.4.1) regulates these services, imposing duties and obligations. Currently, according to the EU registry, only a few companies have been registered as intermediaries. As the legal framework of operation is recent, it remains to be seen how it will involve and whether it will serve its purpose, or additional challenges will emerge.

2.3.1.3 Technical challenges

Here we explore the technical challenges related to the governing of data and data sharing. This includes aspects such as how to implement the FAIR principles[30], issues related to data and technology sovereignty, data quality, security and data protection, common standards, etc. Such issues are relevant for the technical governance layer of a data space/ecosystems (the governance of technical aspects in the data collaboration).

Tools and technology solutions for data management and sharing

Inadequate tools and technology are barriers to data acquisition. Easy-to-implement solutions can enhance access and participation in data sharing (PrepDSpace4Mobility, 2023).

[29] https://www.drivesweden.net/en/project/network-micromobility-phase-2.
[30] https://www.go-fair.org/fair-principles.

Having the technologies and tools for data sharing and management, and accessible to all relevant stakeholders, is both a technical and governance challenge. The absence of technologies and tools can hinder effective data management and sharing. However, this lack is often due to organisational issues like budget constraints, insufficient technical expertise, or other priorities (Lundahl, Sobiech & Thidevall, 2023).

A challenge within data spaces is to achieve efficient data access and smooth integration of actors and systems in the case of heterogeneity in technologies, standards and architectures (Farrell et al., 2023).

Data governance in practice

Data governance, sometimes referred to as technical governance, is often highlighted as important in the digital era, but there are still knowledge gaps about how to implement it in practice (Bayamlioğlu & Benmayor, 2023) and a holistic view of is lacking (Abraham et al., 2019).

Implementing the FAIR principles

The FAIR-principles (see Section 2.4.5) aim to improve the Findability, Accessibility, Interoperability, and Reusability of digital resources. The principles have been widely adopted since their introduction in 2016 by Wilkinson et al. (2016). They are intentionally broad and flexible, allowing tailored implementations. However, this flexibility has led to inconsistent interpretations and implementations that can hinder interoperability (Jacobsen et al., 2020). To address this, Jacobsen et al. propose 'FAIR implementation considerations' to guide communities towards consistent and widely usable implementations, encouraging communities to either adopt existing solutions or develop new ones that can be shared and reused by others.

Data quality issues

The origin and handling of data can affect its usefulness and reliability for end users. For data to be useful to the end user, it must be of sufficient quality for the intended use. This means that we must consider data quality throughout the data value chain, from creation to end user. Poor data quality can limit usefulness.

Low data quality is a generally recognised factor that impedes the wider use of open data. Data publishers often lack the expertise and resources to ensure that data is published in an optimal way, fully standards-compliant and with complete metadata (Neumaier et al., 2018). According to OECD (2019), uncertainties about data quality can deter stakeholders from engaging in data-sharing arrangements. Many datasets lack the requisite quality. Additionally, the absence of a common understanding of data quality is a significant source of uncertainty among organisations. Some argue that data quality should be considered a key determinant of trust in data sharing. The World Bank (2021) also highlights that data sharing in practice is limited by difficulties in assessing the quality and accuracy of data.

The importance of data quality can vary across applications. One example where data quality plays a major role is the need for reliable traffic rule data for automated vehicles (Lundahl, Sobiech, & Thidevall, 2023; Lundahl, 2024b). Poor data quality can result in incorrect interpretations of traffic rules, increasing the risk of accidents. Another consequence may be that these vehicles cannot drive in automated mode on some roads. What further complicates the issue is that the mandates for deciding on traffic regulations in many countries are divided between national, regional and local authorities. Each may have different ways of designing and digitalising traffic regulations, or no ways at all for digitalising them.

Interoperability issues

Neumaier et al. (2018) believes that factors hindering the potential of open data include the lack of a definite metadata standard and poor interoperability between data providers. Publishers often lack expertise and resources to ensure optimal, standards-compliant data publication with complete metadata. Incomplete and heterogeneous metadata, along with poor interoperability, limits sophisticated search functionality across

datasets. Search in open government data catalogs is limited to metadata fields and ignores embedded semantics in the datasets. Metadata descriptions do not link to external knowledge bases, ontologies, or other datasets and data catalogs, risking the creation of data silos instead of interconnected data portals.

According to PrepDSpace4Mobility (2023), stakeholders in the mobility domain use a variety of data formats, structures and naming conventions for similar data, leading to inconsistencies. Differences in interfaces create challenges for data integration and analysis. In addition, incomplete or insufficient metadata and inaccuracies in datasets from different platforms further complicate the situation. For example, while there are standards to support data availability for ITS data, which are to be exchanged via the National Access Points (NAPs), differences exist between the EU Member States in the adoption and use of these standards. Additionally, the NAP operators also have a different interpretation of what data quality means

In the data space context, Nagel and Lycklama (2022) highlight that interoperable data spaces are more of a coordination challenge than a technology problem. Achieving this will require good coordination, involving the balancing of interests, input, and energy from both private and public actors.

Referencing data and digital resources

Farrell et al. (2023) highlight that a challenge for data spaces is associated with the encoding and sharing of data, especially across providers and countries. Using commonly agreed data models, specifications and vocabularies can improve data interoperability. Persistently exposing the vocabularies on the web through codelists allows providers to use unique resource identifiers, making data encoding language-independent.

2.3.1.4 Power dynamics and power asymmetries

Here we explore challenges related to power dynamics and power asymmetries when it comes to the governing of data sharing. These are challenges related to imbalances in control, influence, and benefits among different stakeholders involved in the production, sharing, and use of data.

For example, Gangneux (2023) notes that stakeholders understand and prioritise value creation from data differently (data understood as a commodified asset and source of revenues – the models of the data marketplace and data brokers – or data as a public good), which can create tensions in the governance of data. The interests of private companies, centred on economic incentives, can also create cultural and organisational barriers.

Farrell et al. (2023) note substantial asymmetries between governments, big tech corporations and other private entities in data collection and access. Public entities, especially local and regional governments, are often in a weaker position and may struggle to find sustainable methods to access privately held data.

Pavel et al. (2023) highlight power asymmetries in digital ecosystems, where a few dominant companies control significant data and digital infrastructure. Strong power imbalances between individuals, companies, and states, reduce people's agency over their data. Weak application of regulations reinforces these imbalances. They propose interventions such as transforming infrastructure into open ecosystems, reclaiming control over data from dominant companies, and establishing non-commercial institutions to rebalance power and create a more equitable digital ecosystem that benefits society as a whole.

Fritzenkötter et al. (2022) stress that a good governance system for a data space should balance the rights of those with market and state power with those of less powerful stakeholders, in the interests of the system as a whole. Without such governance, large corporations will overshadow small primary producers and broader societal interests throughout the production, retail, use, and recycling chain.

2.3.2 Governance challenges perceived by local implementation sites

After having identified the abovementioned challenges (see Section 2.3) through our desk research, we sent a survey to the local implementation sites of the project to gather their input on the governance challenges they experience in terms of mobility data sharing. The set of questions (see Annex 1) was based on challenges repeatedly mentioned in the literature and categorised in the same way as above: organisational, legal, and technical challenges, as well as challenges related to power dynamics and asymmetries. The survey was sent to all nine implementation sites, and six of them replied.

2.3.2.1 Organisational challenges

We asked the local implementation sites about organisational challenges related to the governance of data sharing. They were asked to select from a list of challenges and to elaborate on the challenges they had selected. Below, the main results are summarised briefly. A more detailed summary of the responses can be found in Annex 2 (and the questions in Annex 1).

The results reveal that *five out of six sites* experience or are affected by these challenges:

- How to organise around data sharing (decide on legal form, governance authority, assign roles and responsibilities, develop an effective governance framework, etc.).
- Limited capacity for data management (lack of human resources, skills, or technical solutions).

Additionally, *four out of six sites* experience or are affected by:

- Slow digital transformation.
- Trust issues (including understanding how to build trust and mitigate trust issues among actors involved in data cooperation).
- Opacity on data contracts.
- Unwillingness (by other actors) to share data of public interest.
- Insufficient financial resources (e.g., due to high costs related to collecting, processing, distributing, and sharing data).

Beyond these responses, the results were more scattered, but challenges that *half* of the respondents reported were a lack of data-sharing culture, limited cross-silo collaboration, and the consensus process and reciprocity in data cooperation.

Additional challenges include the absence of a formal data strategy, ensuring fair representation in data governance bodies, and maintaining transparency, accountability, oversight, and enforcement in data cooperation. In addition, public organisations face challenges in transitioning to prioritise data sharing, dealing with resource mismatches, and vague data contracts.

2.3.2.2 Legal challenges

We asked the local implementation sites about legal challenges related to the governance of data sharing. They were asked to select from a list of challenges and to elaborate on the challenges they had selected. Additionally, we inquired about some specific legal issues. Below, the main results are summarised briefly. A more detailed summary of the responses can be found in Annex 2 (and the questions in Annex 1).

The results reveal that *all six sites* that responded to the survey experience or are affected by the challenge of understanding how new regulations, such as the Data Governance Act and the Data Act, impact or change the existing obligations under the Open Data Directive and the ITS Directive.

Additionally, *four out of six sites* experience or are affected by these challenges:

- Navigating and dealing with a complex and fragmented legal framework around accessing and sharing data.

- Challenges related to including data sharing obligations in tenders and contracts with suppliers of products and services.
- Addressing legal liabilities in case of data breaches or misuse.

Beyond these responses, the results were more scattered, but challenges that *half* of the respondents reported were lack of clarity on the laws applicable to data, mapping roles and responsibilities under different legal regimes (for instance, between the GDPR and the DGA), challenges related to entering into data contracts with private companies (for instance, voluntary data agreements with private companies), and understand how to benefit from data intermediary services and what the potential implications might be.

Additional challenges include lack of clarity on applicable laws, mapping roles and responsibilities under different legal regimes, entering into data contracts, and understanding the benefits and implications of data intermediary services. GDPR compliance, particularly data portability and the right to be informed, pose significant challenges. Examples of legal barriers include restrictions on ANPR data use and legal ambiguities delaying data sharing with private companies.

2.3.2.3 Technical challenges

In this part of the survey, we asked the local implementation sites about technical challenges related to the governance of data sharing. They were asked to select from a list of challenges and to elaborate on the challenges they had selected. Below, the main results are summarised briefly. A more detailed summary of the responses can be found in Annex 2 (and the questions in Annex 1).

The results reveal that *four out of six sites* experience or are affected by these challenges:

- Standards harmonisation.
- How to ensure data sovereignty (i.e., the possibility for individuals and organisations to control, govern, and ensure the protection of their own data).
- How to ensure (and understand) data quality.
- How to ensure data privacy and data protection (e.g., how to implement privacy-preserving mechanisms and privacy by design).
- Integrating legacy systems with new data sharing technologies.

Beyond these responses, the results were more scattered, but challenges that *half* of the respondents reported were how to implement the FAIR principles, how to ensure technological sovereignty, how to ensure data interoperability (decide on common standards, specifications, formats, languages etc.), discovery of data (finding other relevant data sources and also enhancing data discovery of your own datasets), and identifying shareable data that the city/region holds and define scope and conditions for access and reuse (and knowing others' need of data, i.e., what data would be valuable to others if distributed/shared).

Additional challenges include ensuring data security, setting and implementing usage control policies, measures for identity, authentication, and access control, linked data, open-source software, and managing data storage and scalability. GDPR compliance challenges (from a technical viewpoint) involve ensuring data is properly anonymised, maintaining data accuracy and integrity, implementing strict access controls, and continuously monitoring data management practices.

2.3.2.4 Power dynamics and power asymmetries

In this part of the survey, we asked the local implementation sites about challenges related to power dynamics and asymmetries in the governance of data sharing. They were asked to select from a list of challenges and to elaborate on the challenges they had selected. Below, the main results are summarised briefly. A more detailed summary of the responses can be found in Annex 2 (and the questions in Annex 1).

The results reveal that *four out of six sites* assess that they have or are affected by the challenge of clearly explaining the purpose of data sharing and reuse for each use case and demonstrating its societal value/public benefit.

Additionally, *half* of the respondents reported that they have or are affected by the challenge of how to level the playing field in terms of data sharing and reuse between different types of stakeholders. The same proportion reported that they have or are affected by the challenge how to abide by the principles of technological and data sovereignty with particular attention to avoiding vendor lock-ins.

Additional challenges include the challenge of creating tangible societal value and public benefits of data sharing and use; and the challenge of aligning data cultures, organisational goals, technological maturity, and interests between private and public organisations. The need for a 'killer app' to showcase the benefits of data spaces and drive engagement was highlighted. Ensuring that data sharing initiatives are aligned with environmental sustainability goals and EU data governance standards was also noted. In cross-border data sharing, challenges include different speeds and levels of maturity between countries and disparities in markets leading to unequal conditions in data sharing agreements.

2.3.3 Conclusions and next steps

Our analysis shows that data sharing is not without challenges. The challenges frequently mentioned in the literature are largely the same as those faced by our local implementation sites. When you see all the challenges compiled in this way, it is easy to get overwhelmed, but it is important to remember that not all use cases have the same challenges; it depends on the individual case. And it is important to know the problems; otherwise, it will be difficult to know what needs to be done. Additionally, the potential of data sharing to address mobility problems suggests that it may be well worth getting involved.

The survey with the local implementation sites revealed various challenges in the governance of data sharing (listed below in bullet points, followed by a table of the most common challenges):

- The sites reported significant **organisational challenges**, including how to organise around data sharing, limited capacity for data management, slow digital transformation, trust issues, opacity in data contracts, and unwillingness to share data of public interest. Financial constraints due to high costs of data processes were also noted. Additional challenges include a lack of data sharing culture, limited cross-silo collaboration, and difficulties in achieving consensus and reciprocity in data cooperation. Issues such as the absence of a formal data strategy, ensuring fair representation in data governance bodies, and maintaining transparency, accountability, oversight, and enforcement in data cooperation were also highlighted. Public organisations face challenges in transitioning to prioritise data sharing, dealing with resource mismatches, and vague data contracts.
- Challenges related to **legal governance** include understanding the impact of new regulations like the Data Governance Act and the Data Act on existing obligations under the Open Data Directive and the ITS Directive. The sites struggle with navigating a complex legal framework, including data sharing obligations in tenders and contracts, and addressing legal liabilities in case of data breaches or misuse. Other issues include lack of clarity on applicable laws, mapping roles and responsibilities under different legal regimes, entering into data contracts, and understanding the benefits and implications of data intermediary services. GDPR compliance, particularly data portability and the right to be informed, pose significant challenges. Examples of legal barriers include restrictions on ANPR data use and legal ambiguities delaying data sharing with private companies.
- Challenges related to **technical governance** include standards harmonisation, ensuring data sovereignty, understanding and maintaining data quality, ensuring data privacy and protection, and integrating legacy systems with new data sharing technologies. Implementing the FAIR principles, ensuring technological sovereignty, data interoperability, discovering relevant data sources, and identifying shareable data were also noted. Specific issues included ensuring data security, setting

and implementing usage control policies, measures for identity, authentication, and access control, linked data, open-source software, and managing data storage and scalability. GDPR compliance challenges involve ensuring data is properly anonymised, maintaining data accuracy and integrity, implementing strict access controls, and continuously monitoring data management practices.

- Challenges related to **power dynamics and asymmetries** include clearly explaining the purpose of data sharing and reuse for each use case and demonstrating its societal value and public benefit. Levelling the playing field between different types of stakeholders and abiding by the principles of technological and data sovereignty, particularly avoiding vendor lock-ins, were significant issues. Aligning data cultures, organisational goals, technological maturity, and interests between private and public organisations is also challenging. The need for a 'killer app' to showcase the benefits of data spaces and drive engagement was highlighted. Ensuring that data sharing initiatives are aligned with environmental sustainability goals and EU data governance standards was also noted. In cross-border data sharing, challenges include different speeds and levels of maturity between countries and disparities in markets leading to unequal conditions in data sharing agreements.

Table 1 – Common challenges faced by the deployEMDS local implementation sites

Category	Challenge
Organisational governance	• Understanding how to organise around data sharing • Limited capacity • Slow digital transformation • Trust issues (including understanding how to build trust and mitigate trust issues) • Opacity on data contracts • Unwillingness (by other actors) to share data of public interest • Insufficient financial resources
Legal governance	• Understanding how new regulations (DGA, DA, etc.) impact or change existing obligations under the Open Data Directive and the ITS Directive • Navigating and dealing with a complex and fragmented legal • framework around accessing and sharing data • Challenges related to including data sharing obligations in tenders and • contracts with suppliers of products and services • Addressing legal liabilities in case of data breaches or misuse
Technical governance	• Standards harmonisation • Ensuring data sovereignty • Ensuring (and understanding) data quality • Ensuring data privacy and data protection (technically) • Integrating legacy systems with new data sharing technologies
Power dynamics and asymmetries	• How to clearly explain purpose of data sharing and reuse for each use-case and demonstrate this societal value/public benefit

As mentioned, understanding the problems is crucial to determine necessary actions. Moreover, data sharing's potential to solve mobility issues makes involvement worthwhile. **An analysis investigating the**

benefits (value to citizens, businesses, and society) of sharing mobility data will be conducted later in the project.

Several of the challenges evident in the survey results are now being addressed in the project's **policy labs** (task 3.2). For instance, the policy labs currently address the topics trust issues in data sharing, unwillingness to share data of public interest, data quality issues, and the challenge of ensuring data privacy and data protection. The participatory policy lab process helps to frame, discuss, and solve policy barriers in collaboration. The partners of the consortium form the various policy lab groups that discuss and co-create in a number of workshop iterations, starting with the challenges and aiming to reach a common understanding of the situation and the way forward to overcome these challenges. The results of the policy labs will be presented in a separate document later. The project also has other activities to discuss challenges and possible strategies to overcome them.

A similar (not identical) survey has also been conducted with the project's **Network of Follower Cities and Regions**[31], yielding similar results. Many of the governance challenges are common between the local implementation sites and the follower cities and regions. Both surveys were more focused on cities and regions than on the private sector. More needs to be learned about the challenges faced by private actors, such as industry players and platforms represented in the project's **Innovation and Scaling Group**[32]. We plan to continue activities to address this.

2.4 Governance for mobility data sharing

The governance dimension of a data space (or any entity or organisation) is crucial to ensure its effective functioning, address the diverse needs of participants, ensure financial sustainability and legal compliance, and ultimately achieve the data space's goals.

In this section, we explore the governance principles, structures, models, mechanisms that exist or have been proposed for (mobility) data sharing (for instance, in data spaces). We also look more broadly to draw from governance principles that are not specifically about data sharing contexts but are relevant for cooperation around the sustainable management of shared resources.

2.4.1 Importance of governance in data space contexts

Governance and **data governance** play a central role in data spaces and ecosystems, where data is shared and exchanged among various stakeholders. Regarding the concepts, see Section 2.1.4.1 on 'governance' and Section 2.1.4.2 on 'data governance'.

A common **framework for data governance** can act as the backbone to ensure data integrity, security, quality, and usability by establishing clear policies and procedures. Furthermore, it can ensure compliance with regulatory requirements and ethical standards. Where data spaces involve sensitive information, such as personal data or proprietary business data, governance frameworks help comply with legal obligations and protect the rights of individuals and businesses. Data governance can also promote trust among participants by defining and enforcing rules for data access, use, and sharing, creating a transparent

[31] The deployEMDS Network of Follower Cities and Regions is a group designed to engage with external local and regional public entities interested in shaping the future of the common European mobility data space (EMDS) by supporting the development of the deployEMDS project. The Network is dedicated to engaging authorities of different sizes, experience levels, and stages of maturity, ensuring a diverse representation from various Member States.
[32] The deployEMDS Innovation and Scaling Group (ISG) fosters collaboration between deployEMDS stakeholders and external entities, mainly from the private sector, with the objective to develop use cases, promote knowledge exchange, and ensure technical and governance developments meet private actors' needs.

environment. It can also enable effective data management, assign responsibility for data assets, and ensure accountability. This promotes responsible data practices and helps resolve issues related to data misuse or breaches. Additionally, data governance can support innovation and value creation. By providing a structured approach to data, it allows organisations to leverage data as a strategic asset, facilitating the development of new products, services, and business models within the data space/ecosystem.

Governance of the data space/ecosystem itself is equally important. It involves setting rules and policies that govern the interactions between participants, the use of shared infrastructure, and the overall operation of the ecosystem. It ensures that the data space/ecosystem operates smoothly and efficiently, providing a fair and transparent environment for all participants.

In **summary**, governance is crucial for data spaces and ecosystems, providing frameworks to manage data efficiently, ensure compliance, build trust, and drive innovation, while also overseeing the proper functioning of the data space/ecosystem as a whole. Its importance should not be underestimated, as it underpins the very foundation of collaborative data environments.

2.4.2 Ideas on good governance and governance principles for collective action

While it is beyond the scope of this report to delve deep into different proposals for good governance and governance principles for collective action, this section provides insights into a few important proposals that can inform the discussion on **governance principles** within our data sharing and data space context.

As already mentioned (see 2.1.4.1), governance is the process of making decisions about an entity. However, *good g*overnance is vital to making the *right* decisions. So, what is good governance?

The **United Nations Economic and Social Commission for Asia and the Pacific**[33] suggests that good governance has eight major characteristics (UNESCAP, n.d.) (paraphrased):

1. Participatory: Involves informed and organised participation by all, including men and women.
2. Consensus oriented: Mediates different interests to achieve broad community consensus.
3. Accountable: Government, private sector, and civil society are accountable to the public and stakeholders. Generally, organisations are accountable to those affected by their actions.
4. Transparent: Decisions and their enforcement follow rules and regulations, and information is freely available and directly accessible to those affected.
5. Responsive: Institutions and processes serve all stakeholders within a reasonable timeframe.
6. Effective and efficient: Processes and institutions meet societal needs efficiently, utilising resources wisely while also promoting sustainable use of natural resources and environmental protection.
7. Equitable and inclusive: Ensures all members of society have a stake and are not excluded, especially the vulnerable.
8. Rule of law: Requires fair legal frameworks, protection of human rights, and an independent judiciary.

Similar principles can be found among the 12 Principles of Good Democratic Governance[34] established by the **Council of Europe** to promote responsible public affairs and resource management (paraphrased):

1. Fair elections, representation, and participation: Ensure free and fair elections and citizen engagement.
2. Responsiveness: Adapt objectives, rules, structures, and procedures to meet citizens' needs.
3. Efficiency and effectiveness: Make the best use of resources to meet agreed objectives.

[33] http://www.unescap.org/.
[34] https://rm.coe.int/12-principles-of-governance-poster-a2/1680787986.

4. Openness and transparency: Make decisions according to rules and provide public access to information.
5. Rule of law: Ensure compliance with laws and judicial decisions.
6. Ethical conduct: Prioritise the public good and preventing corruption.
7. Competence and capacity: Enhance professional skills in governance.
8. Innovation and openness to change: Seek new solutions and modern methods.
9. Sustainability and long-term orientation: Consider future generations in policies.
10. Sound financial management: Practice financial prudence and multi-year budgeting.
11. Human rights, cultural diversity, and social cohesion: Uphold human rights and foster social cohesion.
12. Accountability: Ensure decision-makers are responsible and can be sanctioned.

Elinor Ostrom, a Nobel Prize-winning political scientist and political economist, identified eight principles for the effective governance and management of common-pool resources (CPRs). She spent decades studying self-governing CPR institutions and identified underlying design principles that successful CPR institutions share, as well as how these design principles affect the incentives of appropriators so that the CPRs themselves and the CPR institutions can be sustained over time (Ostrom, 1990).

Ostrom's eight governance principles:

1. Clearly defined boundaries: Individuals or households who have rights to withdraw resource units from the CPR must be clearly defined, as must the boundaries of the CPR itself.
2. Congruence between appropriation and provision rules and local conditions: Appropriation rules restricting time, place, technology, and/or quantity of resource units are related to local conditions and to provision rules requiring labor, material, and/or money.
3. Collective-choice arrangements: Most individuals affected by the operational rules can participate in modifying the operational rules.
4. Monitoring: Monitors, who actively audit CPR conditions and appropriator behavior, are accountable to the appropriators or are the appropriators.
5. Graduated sanctions: Appropriators who violate operational rules are likely to be assessed graduated sanctions (depending on the seriousness and context of the offense) by other appropriators, by officials accountable to these appropriators, or by both.
6. Conflict-resolution mechanisms: Appropriators and their officials have rapid access to low-cost local arenas to resolve conflicts among appropriators or between appropriators and officials.
7. Minimal recognition of rights to organise: The rights of appropriators to devise their own institutions are not challenged by external governmental authorities.

And for CPRs that are parts of larger systems:

8. Nested enterprises: Appropriation, provision, monitoring, enforcement, conflict resolution, and governance activities are organised in multiple layers of nested enterprises.

Several proposals have been made on how Ostrom's principles can be applied to data and 'digital commons' and for designing governance for sustainable data sharing. See, for example, Coyle et al. (2020a) and Ruhaak et al. (2021). They suggest **using the principles (in their data economy parallels)** to ensure that data is managed more efficiently and equitably.

In this report, we use Ostrom's principles as a lens to systematically **analyse the governance of the deployEMDS local implementation sites** (see Section 2.5).

There are many similarities between the natural resource nested problem (overconsumption) initially examined by Ostrom and the technology platform anticommons problem (overexclusion). Both "feature institutions for collective self-governance that face similar problems of free riding and rent seeking in resource provision, facilitating credible commitments, and designing rules for monitoring and enforcing sanctions against opportunistic platform users" (Simcoe, 2014). Unlike natural resources, technology platforms

normally have positive consumption externalities, or network effects, i.e. the more participants are added, the more marginal benefits are produced (e.g. more data can be shared and combined to increase its value). Hence, a key threat to a technology platform is not overuse, but over-exclusion (Simcoe, 2014). While CPRs regulate access to prevent overconsumption, technology platforms tend to encourage coordination and try to prevent over-exclusion (Simcoe, 2014).

At a **workshop** we conducted in January 2024, we asked the participants to share their thoughts on what governance means to them, identify key elements of effective governance, and discuss aspects of good versus bad governance, among other questions.

- The responses to the question "What is good governance" highlighted several key aspects, such as:
  - Clear processes; participation and inclusivity; transparency and accountability; efficiency and effectiveness; strategic and sustainable growth; trust and relationships.
- The responses to the question "What is bad governance" identified aspects such as:
  - Lack of transparency; inefficiency and ineffectiveness; lack of purpose and direction; trust issues; accountability issues; unfairness and undemocratic processes.

Responses to other questions we discussed have been integrated into other sections of the report.

2.4.3 Principles for a value-based digitalisation

Europe is committed to a value-based digitalisation. As more and more of our lives are lived in the digital realm, it becomes more important that the same rights and principles that apply offline also apply fully online in the digital space. This is central to the EU's vision for digitalisation.

Therefore, the EU has signed the **European Declaration on Digital Rights and Principles**[35], placing Europeans at the heart of the EU's digital transformation and promoting a digital transition shaped by European values. This declaration, the first of its kind in the world, serves as a reference point for EU citizens and guide policy makers and companies in developing digital technologies. Thus, they will be reflected in the EU's actions, future work, and engagement with global partners. The principles are shaped around six themes:

1. Putting people and their rights at the centre of the digital transformation.
2. Supporting solidarity and inclusion.
3. Ensuring freedom of choice online.
4. Fostering participation in the digital public space.
5. Increasing safety, security and empowerment of individuals (especially young people).
6. Promoting the sustainability of the digital future.

Also, the **Berlin Declaration on Digital Society and Value-Based Digital Government**[36], signed by all Member States in December 2020, outlines principles for value-based declaration:

1. Validity and respect of fundamental rights and democratic values in the digital sphere.
2. Social participation and digital inclusion to shape the digital world.
3. Empowerment and digital literacy, enabling all citizens to participate in the digital sphere.
4. Trust and security in digital government interactions, enabling everyone to navigate safely and securely in the digital world.

[35] European Declaration on Digital Rights and Principles for the Digital Decade, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001.
[36] Berlin declaration on Digital Society and Value-Based Digital Government at the ministerial meeting during the German Presidency of the Council of the European Union on 8 December 2020, https://ec.europa.eu/isa2/sites/default/files/cdr_20201207_eu2020_berlin_declaration_on_digital_society_and_value-based_digital_government_.pdf.

5. Digital sovereignty and interoperability, which are keys to ensuring that citizens and public administration can make decisions and act self-determined in the digital world.
6. Human-centred systems and innovative technologies in the public sector.
7. A resilient and sustainable digital society.

The Berlin declaration builds on the political commitments of the Tallinn Declaration on eGovernment[37], taking the user-centricity principles in the Tallinn Declaration a step further by enhancing public administrations' role in driving value-based digital transformation in Europe. It reaffirms European leaders' commitment to fundamental rights and European values, emphasising the importance of digital public services (European Commission 2020c).

2.4.4 Comparing principles

In the sections above, we explore well-regarded principles emphasised in governance frameworks in contexts ranging from traditional good governance and management of common resources to digital governance. From this, we can identify recurring governance principles across different initiatives that may be important to consider for the needs in our project. These principles can provide insights into governance principles and mechanisms that may be needed when developing a governance framework to ensure trust and cooperation in data sharing. They provide overarching guidelines for data collaboration, which can be further detailed in more specific governance mechanisms. Examples of recurring principles across different contexts and initiatives include participation, accountability, transparency, responsiveness, efficiency, rule of law, fairness and sustainability. These principles can be applied in our context as well.

Recurring principles across different initiatives:

- Participation (common to UNESCAP, Council of Europe, and European initiatives on digital rights).
- Accountability (common to UNESCAP, Council of Europe, and Ostrom).
- Transparency (common to UNESCAP and Council of Europe).
- Responsiveness (common to UNESCAP and Council of Europe).
- Efficiency and effectiveness (common to UNESCAP and the Council of Europe).
- Rule of law (common to UNESCAP and Council of Europe).
- Equity and inclusion (common to UNESCAP and European initiatives on digital rights).
- Sustainability (common to UNESCAP, Council of Europe, and European initiatives on digital rights).

In this report, we place extra focus on **Ostrom's principles** by using them to analyse the governance of the deployEMDS local implementation sites (see Section 2.5). Some of her principles have no explicit counterpart in the other initiatives, which focus more on broader governance principles, but there are thematic similarities, and they can help enhance our understanding of effective governance. Here is how her principles might align with the other explored initiatives:

1. Clearly defined boundaries: This principle is specific to the management of resources and does not have a direct counterpart in the other initiatives.
2. Congruence between appropriation and provision rules and local conditions: The idea of tailoring rules to local conditions is somewhat similar to the responsiveness principle stressed by UNESCAP and the Council of Europe, which emphasise adapting to meet the needs of citizens.
3. Collective-choice arrangements: This aligns with the participatory principle stressed by several of the frameworks, as both principles involve those affected by the rules having a say in their modification.

[37] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017, https://ec.europa.eu/newsroom/dae/redirection/document/47559.

4. Monitoring: While not explicitly mentioned, the concept of monitoring is related to transparency and accountability, as it involves oversight and the availability of information.
5. Graduated sanctions: This principle is about enforcement, which can be seen as part of the rule of law and accountability principles.
6. Conflict-resolution mechanisms: The need for mechanisms to resolve conflicts is a part of responsive governance, ensuring that institutions serve stakeholders within a reasonable timeframe.
7. Minimal recognition of rights to organise: This is related to participation and inclusion, as it involves recognising the rights of individuals to form their own institutions.
8. Nested enterprises: The idea of multiple layers of governance is not part of the listed principles in the other initiatives but is mentioned in the text of UNESCAP.

As already mentioned (see Section 2.4.2), there are several suggestions on how Ostrom's principles can be applied in the digital context to ensure that data is managed more efficiently and fairly. **Her principles, in their data economy parallels**, may include establishing clear rules for data access and use, ensuring that those affected by data governance decisions can participate in making these decisions, monitoring data use to prevent misuse, providing easily accessible conflict resolution to maintain trust and cooperation between stakeholders, and allowing data communities to self-organise and create their own governance structures. For larger data ecosystems, governance should be organised in multiple layers, with smaller (local) governance structures nested within larger, overarching frameworks (on this topic, see Section 2.4.7 regarding governance levels and multi-level governance of data spaces). We have included a list of questions for (self-)evaluation of data spaces based on Ostrom's principles in Annex 3 of this report.

We will revisit Ostrom's principles and their application to data economy parallels in Section 2.5, where we use her principles as a lens to systematically **analyse the governance of the project's local implementation sites**.

In **summary**, the comparison of governance principles across different frameworks highlights several recurring themes that are important to consider when developing a governance framework for data sharing that is effective and fair. Key principles that are consistently emphasised across frameworks such as participation, accountability, transparency, and responsiveness can provide a foundation for ensuring trust and cooperation in data collaboration. We will take these into account in our continued work to develop a multi-level governance framework with business and governance mechanisms for mobility data sharing.

2.4.5 Synthesis of ideas on good data governance

In Section 2.4.2, we explored ideas on *good governance* to identify recurring principles across different initiatives that may be important to consider when developing a governance framework to ensure trust and cooperation in data sharing. Now, what is *good data governance*?

Depending on the definition (there are many to choose from, see Section 2.1.4 on the concepts), *governance* is the process of making decisions about an entity, while *data governance* is the exercise of authority and control over the management of data. Both governance and data governance are crucial in data spaces and ecosystems, where data is shared and exchanged among various stakeholders.

The **purpose** of data governance is to increase the value of data (seek to maximise the benefits from data) while addressing and minimising related costs and risks (Abraham et al., 2019; Farrell et al., 2023). Good data governance should both **promote benefits and minimise harms** at each stage of relevant data cycles (Davies, 2022).

Since data governance involves allocating authority and control over data and exercising this authority through decision-making in data-related matters, Janssen et al. (2020) explain that to achieve its goals, data governance should **focus not only on the data itself but also on the systems** through which data is

collected, managed, and used. People are essential in these systems (Benfeldt, Persson, & Madsen, 2020); therefore, data governance should provide incentives and sanctions to encourage desirable behaviour. Beyond a single organisation, data governance relies on collaboration between organisations and individuals. This multi-organisational context requires trusted frameworks to ensure secure and reliable data sharing while complying with relevant laws (Janssen et al., 2020).

Benfeldt, Persson, & Madsen (2020) notes that the lack of a widely accepted definition of data governance continues to affect the research field. **Different research streams** offer varying perspectives on its purpose and implementation:

- One research stream views data governance as a means to resolve poor **data quality**, focusing on compliance, effective reporting, and customer management. For instance, Otto (2011) emphasises setting direction for data quality management, while Wang and Strong (1996) highlight the subjective nature of data quality as 'fit for use by data consumers'.
- Another research stream, based on Weill and Ross' (Weill & Ross, 2004) IT governance concept, argues that data governance should **increase the value of data** as organisational assets. This involves aligning data management with organisational goals, assigning accountability, and achieving objectives like efficiency improvement, business growth, and risk reduction.
- Defining data governance for data quality involves deciding by whom and for what data is to be used, and assigning accountabilities and rights accordingly. In contrast, defining data governance in relation to data value involves determining how data can be used to achieve organisational objectives, with accountabilities and rights similarly assigned (Benfeldt, Persson, & Madsen, 2020).

Although data governance is essential in the digital era, significant **ambiguities and knowledge gaps** about its practical implementation remain (Bayamlioğlu & Benmayor, 2023). Additionally, there is still a lack of a holistic view that could guide both practitioners and researchers (Abraham et al., 2019). Organisations may face challenges in practical implementation, such as the complexity of managing data across systems and departments, ensuring consent management, integrating privacy by design, and addressing data subject rights effectively.

As mentioned above, good data governance includes, among other things, minimising harm and risk and complying with relevant laws and regulations. **Principles** such as *accountability* and *rule of law* are also often highlighted in proposals for good governance in general (see Section 2.4.2). Thus, it is relevant that there are **requirements for data governance in EU legislation**, such as in the GDPR and the AI Act:

- The **GDPR** focuses on the protection of personal data. Whether data is considered personal does not necessarily prevent the collection or sharing of such data, but it triggers additional care in the processing and handling. Data governance requirements for GDPR compliance include, among others: lawfulness, fairness, and transparency (ensuring a lawful basis for processing, that processing is fair, and that the data subject is informed); purpose limitation (only collecting data that is necessary for the specified, explicitly stated, and legitimate purposes); data minimisation (never processing more personal data than is necessary for the specified purpose); accuracy (ensuring that personal data is accurate and up-to-date); storage limitation (retaining personal data only for as long as is necessary); integrity and confidentiality (implementing appropriate security measures to protect personal data, for example, so that it is not accessed by unauthorised persons and so that it is not lost or destroyed); and accountability (organisations must be able to demonstrate that they comply with the GDPR). Moreover, the GDPR gives individuals rights regarding their personal data, such as access and rectification, which must be integrated into data governance processes.
- The **AI Act** sets out certain requirements, such as specific data quality requirements for high-risk AI systems in Article 10. Datasets must meet these requirements if they are to be used in such systems.

Read more about these and other laws and regulations relevant in the context of mobility data sharing, with requirements that must be considered and that may need to be integrated into data governance processes relevant to (mobility) data sharing in chapter 3.

The Data Governance Act (DGA) (see Section 3.4.1 about the DGA) does not define data governance but introduces the European Data Innovation Board (EDIB). The **role of the EDIB** is to advise and assist the Commission on topics such as cybersecurity, reuse and interoperability in relation to data transactions. The Commission can in turn adopt implementing acts establishing model contractual clauses for data intermediation services or a rulebook establishing requirements on "appropriate technical and security requirements […] for the storage and processing of data". In short, the Commission has a governing role in how data is managed in a European context.

If we return to what was said earlier – that data governance, to achieve its goals, must focus not only on the data itself but also on the systems through which data is collected, managed, and used, where people are essential (Janssen et al., 2020; Benfeldt, Persson, & Madsen, 2020) – we can seek help from **international standards** to understand the phases of data life cycles as well as the roles and responsibilities related to data governance (see below). As mentioned in Section 2.1.4.2, there are several standards that relate to data governance and governance in terms of quality management.

Since data processing serves as a means to an end, there should be an intended purpose or use behind the processing and quality of the data assessed as to what extent it satisfies the needs considering the given conditions (Burden & Stenberg, 2024). By synthesising the life cycles described in ISO/IEC 5259-3 and ISO/IEC 25024:2015, we suggest seven phases for a **data life cycle** (see Figure 1):

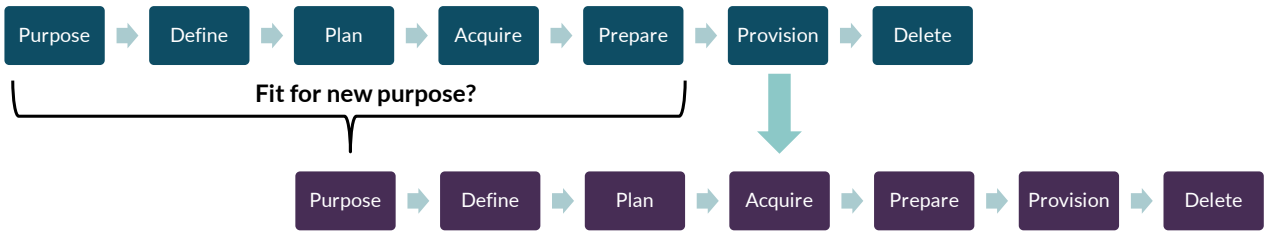
Figure 1 – The data life cycle

1. Describe the purpose of processing specific data.
2. Define requirements for the data, such as formats, provenance and content.
3. Plan how to meet the requirements depending on if it is available within the organisation or there are external dependencies.
4. Acquire the data by collection, generation and/or combining existing datasets.
5. Prepare the data, e.g. by filtering or transforming the data to fit another metamodel.
6. Provision the data by making it available where it is needed or should be stored. This could be done through APIs and/or cloud services.
7. Delete the data when the data is no longer needed or the reason for processing expires.

Over the life cycle it is important to monitor and evaluate to what extent the current implementation serves the vision.

In a data transaction context, it is worth remembering that the provision of one party can be the acquisition of another and that the steps leading up to provision then should reflect the purpose behind the acquisition in the second life cycle. The steps are more elaborately described in the standards. See Figure 2 below.

Figure 2 – Provision and acquisition of data



Roles and responsibilities in relation to data are defined in both regulations and standards:

- For instance, the Data Act defines roles such as 'data holder' (someone who has the right or obligation to use and make data available) and 'user' (someone who owns a connected product), each with their own rights and responsibilities. The Data Governance Act introduces similar roles where a 'data holder' has the right to grant access to data, and a 'data user' is someone who has the right to access and use data. Since the role of the data holder is slightly different between the two acts, it is important to know which acts are applicable when making decisions related to data governance.
- The ISO/IEC 5259-series defines four roles in relation to data governance that we find interesting, all with their own set of rights and responsibilities (the roles and responsibilities are synthesised and summarised by us, the details of the roles and responsibilities are further described in the ISO/IEC 5259-series):
    - Governing body: Those who are responsible for the performance and compliance of data management, typically found at an executive level within an organisation.
    - Data holder: Those who have the mandate to authorise data processing, often at a managerial level within an organisation.
    - Data originator: Those who created the data. Can be found within or outside the own organisation and their rights vary according to the nature of the data and its processing.
    - Data user: Those who have the mandate to perform the processing, often at an operational level within an organisation.
- The roles are not necessarily orthogonal. Data originators can have rights under the Data Act in terms of access to the data as users, including the right to mandate that the data is to be processed outside of the governing bodies organisation.
- It is also worth underlining that the same actor may to take on different roles at different phases of the data life cycle. And the roles can be used within as well as across organisations, depending on the context (Burden, Stenberg & Olsson, 2023).

In this section, we should also mention the **FAIR principles**[38], as they are relevant to data sharing by ensuring data is managed in a way that makes it easier for others to find and reuse, which is an aspect of effective data governance. The principles are a set of guidelines designed to improve the Findability, Accessibility, Interoperability, and Reusability of digital assets. These principles are widely endorsed (Jacobsen et al., 2020) and have become a cornerstone in the movement towards open science and data-driven research. The principles emphasise machine-actionability, meaning that computational systems should be able to find, access, interoperate, and reuse data with minimal human intervention.

[38] The FAIR Guiding Principles for scientific data management for stewardship, https://www.go-fair.org/wp-content/uploads/2022/01/FAIRPrinciples_overview.pdf. The principles were published in 2016 by Wilkinson et al.

The FAIR principles:

- Findable: Data should be easy to find for both humans and computers. This includes assigning a globally unique and persistent identifier to the data, describing the data with rich metadata, and registering or indexing the data in a searchable resource.
- Accessible: Once found, it should be clear how the data can be accessed, possibly including authentication and authorisation steps. Metadata should be accessible even if the data are no longer available.
- Interoperable: Data usually need to be integrated with other data and interoperate with applications or workflows for analysis, storage, and processing. Interoperability involves using a formal, accessible, shared, and broadly applicable language for knowledge representation; using vocabularies that follow FAIR principles; including qualified references to other data.
- Reusable: The ultimate goal of FAIR is to optimise the reuse of data. To achieve this, data and metadata should be well-described so they can be replicated and/or combined in different settings. This includes providing a clear and accessible data usage license and detailed provenance.

The FAIR principles are highly relevant to data spaces. They ensure that data assets within the space can be easily discovered by participants, guide the implementation of clear access protocols to make data available to authorised users while protecting sensitive information, and promote interoperability through common standards and vocabularies. Additionally, for data spaces to be effective, the shared data must be reusable in different contexts. The FAIR principles encourage careful documentation and licensing to support this reuse. By following these principles, data spaces can increase the value of shared data, promote innovation and collaboration, and maintain trust and transparency among participants.

By incorporating the FAIR principles, a governance framework can ensure that a data space is not only technically sound but also reliable and transparent. Thus, the FAIR principles can guide the development of a governance framework for data spaces. Notably, a reference to the FAIR principles in connection with common European data spaces can be found in the preamble to the DGA (point 2).

In **conclusion**, good data governance is essential for ensuring trust, cooperation, and effective management of data within data spaces and ecosystems. Effective data governance should promote benefits and minimise harms at each stage of the data cycle. It involves not only focusing on the data itself but also on the system through which data is collected, managed and used. By integrating principles such as accountability and rule of law, organisations can navigate the complexities of data governance. Additionally, the FAIR principles provide a framework for enhancing the findability, accessibility, interoperability, and reusability of data, thereby promoting innovation and collaboration. International standards help define the phases of data life cycles and the roles and responsibilities related to data governance. Monitoring and evaluating the implementation against the vision is crucial throughout the life cycle. Roles and responsibilities are also defined in regulations such as the DGA and the DA. Roles can vary between legal acts, so it is important to know which acts are applicable when making decisions related to data governance. The lack of a widely accepted definition of data governance continues to affect the research field, with different perspectives on its purpose and implementation. As the digital era continues to evolve, addressing ambiguities and knowledge gaps in data governance will be crucial for both practitioners and researchers to develop holistic and practical approaches that maximise the value of data while minimising associated risks and costs.

2.4.6 Synthesis of ideas on data space governance

For the concept 'data space governance', see Section 2.1.4.3. In this section we explore ideas on data space governance. As already mentioned, *data space governance* extends beyond *data governance* to include the management of the partnerships and collaborations needed for unlocking the value of data. This broader governance is fundamental for overseeing the data space comprehensively and ensure compliance with laws, ethical standards, and interoperability.

A report by Farrel et al. (2023) suggests that **there is no single approach** for the technical and governance aspects of data spaces that can be applied for their setup. Therefore, a **community-based approach** through co-creation of data spaces that considers the domain-specific context is the only feasible way forward to ensure buy-in by a broad spectrum of stakeholders.

Fritzenkötter et al. (2022) suggests a **purpose-driven approach** to data space governance and **three components of the governance framework**: principles, processes and practices. That is, a clear organising purpose should inform the development of principles, processes, and practices, to ensure that all data-related activities are pursued with consideration of the broader technical, social, political and economic contexts within which data is produced and consumed. The **purpose should influence every subsequent element** of the collaborative's design and of its governance.

The Data Spaces Support Centre (**DSSC**)[39], funded by the European Commission as part of the Digital Europe Program (DIGITAL), plays a significant role in defining data space governance frameworks. It identifies the needs of data space initiatives, defines common requirements, and establishes best practices and guidelines to accelerate data space design and implementation. An important activity of the DSSC is delivering the evolving Data Spaces Blueprint[40], which outlines building blocks and decisions for each, identifying options and common standards, and providing guidelines for their integration. It acknowledges that future business and technological innovations may change the landscape, but currently, a 'one size fits all' solution is unlikely. Therefore, the approach ensures flexibility and adaptability as data spaces evolve. The DSSC also promotes adoption through support activities, a knowledge-sharing platform, a help desk, toolboxes, and active stakeholder engagement.

The idea of focusing on **building blocks** for the design and implementation of data spaces was proposed in a position paper by taskforce 1 of the OPEN DEI project[41]. Technical and governance building blocks form the structure and framework for efficient and secure operation of a data space (Nagel & Lycklama, 2021, 2022). The DSSC has further developed the OPEN DEI building blocks in a comprehensive blueprint. They also offer resources such as a starter kit, conceptual models, and a glossary to help users understand and apply the building blocks.

In the **DSSC's Data Spaces Blueprint** (DSSC, 2024), building blocks come in two categories:

- Business and organisational building blocks relate to business models of data spaces and the governance of data spaces as well as the legal frameworks that data spaces must comply with.
- Technical building blocks relate to the technical aspects of a data space and the technical agreements that the participants and trusted data space intermediaries must adhere to.

[39] DSSC, https://dssc.eu/.
[40] The Data Spaces Blueprint is being developed by the Data Spaces Support Centre (DSSC), which started in October 2022. This blueprint is a work in progress. The first version of the blueprint, 0.5, was released in September 2023 as a preliminary version. The second version, 1.0, was released in March 2024, and the third version, 1.5, was released in September 2024. New versions of the blueprint will be released every six months. The last version of the blueprint is expected in January 2026.
[41] OPEN DEI, https://www.opendei.eu/.

These two categories are interlinked. The legal requirements can influence the technical functioning of trusted intermediaries, and technical innovations might impact governance and business models.

The **business building blocks** form the foundation for stakeholders creating a business plan for their data space. They provide advice and tools for developing a business plan for the data space, identifying necessary stakeholders, and ensuring financial sustainability. The building blocks revolve around the relationship between data products and services, their utilisation by stakeholders and customers, and the integration into a financially sustainable model. Data products and value-added services support use cases, which are the basis of the business model. Data space intermediaries also play a crucial role in navigating regulatory requirements. The DSSC proposes business building blocks for: business model development, use case development, data product development, and data space intermediary.

The **building blocks of governance** emphasise establishing a robust organisational form and governing authority for effective decision-making. Participation management should focus on streamlined processes to identify key elements of participant engagement and maintain a data governance framework that promotes collaboration and legal adherence. The governance building blocks are central to shaping the structure, decision-making, and participant engagement within data spaces. The *organisational form and governance authority building block* explores possibilities for the organisational form, including the type of legal entity the data space may assume, and aspects to consider when establishing the governance authority and governance framework. The governance authority handles rule-setting, defining governance scope, ensuring compliance, and resolving conflicts, fostering trust and data quality. The *participation management building block* streamlines governance processes and identifies key elements crucial for participants. It focuses on participant onboarding and offboarding. It also highlights risks associated with poorly managed participation, and the need for clear rules, inclusive governance, and adherence to legal requirements.

The legal building blocks help navigate legal frameworks to ensure adherence, covering the legal implications of data transactions, roles of data space intermediaries, and the importance of a structured contractual framework that binds participants to agreed-upon rules and obligations. The *regulatory compliance building block* highlights key compliance elements measures, examining legal frameworks from the perspective of triggers (key elements or criteria that prompt the application of the legal framework). The *contractual framework building block* describes key contracts, including data space and data transaction agreements. These building blocks provide a common basis for organising compliance, guiding towards resources and additional reading, as legal requirements and contractual needs vary across sectors and design choices.

Before implementing any building blocks, the core partners of the data space initiative should clearly define its **purposes, objectives, values, and design principles** to guide coherent actions and decisions. The governance framework and business model will translate these high-level strategic foundations into concrete business choices and policies, which the designated dataspace governance authority will put into practice.

With respect to governance mechanisms, evolving recommendations by the DSSC will be an important source for the project.

Examples of other initiatives developing governance approaches for data spaces and ecosystems:

- **IDSA Rulebook**[42] by the International Data Spaces Association (IDSA) provides a common governance framework for data spaces, focusing on data sovereignty and interoperability, with agreements on functional, technical, operational and legal aspects.

[42] International Data Spaces Association (2023), "IDSA Rulebook", White Paper, https://docs.internationaldataspaces.org/ids-knowledgebase/v/idsa-rulebook/front-matter/readme.

- **Gaia-X Framework** and **Gaia-X Trust Framework**[43] defines technical requirements and rules for Gaia-X, ensuring interoperability and governance across ecosystems while allowing user control.
- **iSHARE Trust Framework**[44] offers specifications and agreements for legal, functional, operational, and technical dimensions to facilitate data sharing and ensure governance, interoperability, and trust.
- **SITRA Fair Data Economy Rulebook**[45] guides the creation of fair data economy networks with agreement templates and other tools, emphasising transparency, fairness, privacy, and security.
- **MyData Global**[46] promotes human-centric data governance, empowering individuals with control over personal data and contributing to sustainable governance models.
- **A NewGovernance**[47] aims to develop a human-centric personal data network with a governance body, competitive data operators, and shared infrastructure, aiming for global standards and compliance with laws and regulations.
- The German **Mobility Data Space**[48] can also be mentioned here, as its data space structure, including its governance structure, is intended to serve as a blueprint and guidance for other data spaces/ecosystems.

At a **workshop** that we conducted in January 2024, we asked the participants to share their thoughts on what governance mechanisms in data spaces should focus on and considerations for governance frameworks for data spaces. Participants highlighted that **governance mechanisms for data spaces** should focus on: ensuring openness, transparency, and fairness; community building and trust-building measures; clarity on roles and responsibilities; interoperability; effective data management practices, including sharing, storage, and ensuring data quality. When asked about **governance frameworks for data spaces**, the participants highlighted that such frameworks should be: clear and easy to understand and adopt; guiding and practical; informed by real cases; developed collaboratively and agreed upon; and purpose-driven. (Other considerations were also mentioned, but these were the key points emphasised.) Responses to other questions we discussed have been integrated into other sections of the report.

In **conclusion**, effective data space governance is essential for unlocking the full value of data through comprehensive management of partnerships and collaborations. A community-based, purpose-driven approach that considers domain-specific contexts is crucial for ensuring stakeholder buy-in and addressing the diverse technical, social, political, and economic environments in which data is produced and consumed. The DSSC's evolving blueprint, along with other governance frameworks, emphasises flexibility and adaptability, recognising that there is no one-size-fits-all solution. Instead, there is support available to help data spaces develop their own tailored solution. By focusing on both technical and governance building blocks, these frameworks help ensure that data spaces operate efficiently and securely. In our project, we plan to use the aforementioned guidance and tools moving forward.

[43] Gaia-X, "Gaia-X Framework", https://docs.gaia-x.eu/framework and Gaia-X (n.d.), "2. Gaia-X Trust Framework", https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/gaia-x_trust_framework.
[44] See https://ishare.eu/home/about/trust-framework/ and https://framework.ishare.eu/is/.
[45] Sitra (2022).
[46] MyData, https://www.mydata.org.
[47] aNewGovernance, https://www.anewgovernance.org.
[48] Mobility Data Space (MDS), https://mobility-dataspace.eu/. MDS is funded by the German Federal Ministry of Digital Affairs and Transport (BMDV) as well as its shareholders. The holding company of the MDS is the DRM Datenraum Mobilität GmbH, a non-profit with the majority shareholder being acatech serving as a neutral actor. The MDS offers a data catalogue and infrastructure for decentralised data exchange, allowing providers and purchasers to control the access and use of their data.

2.4.7 Governance levels and multi-level governance for data spaces and ecosystems

Governance levels

In Section 2.1.4.2, we learned that data governance can expand in its organisational scope to encompass different units (or levels) of analysis: intra-organisational (micro-level) – within the organisation; inter-organisational (meso-level) – between organisations, possibly within ecosystems; and government (macro-level) – national or international policies, strategies, and regulations (Abraham et al., 2019; Davies, 2022; Torre-Bastida et al., 2022).

The **governance levels for data spaces and ecosystems** can also be categorised into: EU level, Member States level, and local level (data space level). The different levels will need to interoperate with each other. (Note that 'local' does not have to mean a specific geographical area such as a city or region, even if that often is the case. It can also refer to a collaboration, for example, between several cities on the same use case.)

The **local level** is very important in the larger ecosystem for several reasons. Mobility data is often generated locally, for example, by local authorities managing transport systems, infrastructure, and urban planning. Additionally, many private actors in the mobility sector operate primarily at the local level. Often, the mobility problems that mobility data can help solve are located at the local level. Local authorities are often in the best position to understand and address the unique mobility needs of their residents. They are also responsible for policymaking, and access to mobility data can help them plan and implement better local policies that, for instance, improve public transport. Local authorities are also closest to citizens and can engage them in the data-sharing process. This can help build trust and encourage participation in mobility initiatives. Therefore, the local level is crucial for the EMDS. However, for a coherent and interoperable data environment, the local level will need to ensure that their data practices are consistent with the broader EMDS framework. In return, they benefit through e.g. access to a wider range of data sources and increased cross-border connections and cooperation (see more on this further below).

The **Member States level**, with national authorities, is important for facilitating data sharing and interoperability within the countries and helping bridge the gap between local data spaces and ecosystems and the EMDS.

At the **EU level**, the overall governance of the EMDS takes place, setting standards and rules to ensure data harmonisation and interoperability. However, considering the local and national levels in the EMDS and ensuring their engagement is crucial to leverage the value of sharing and using mobility data, which often originates locally, and to maintain a user-centric focus and responsiveness to local, regional, and national needs.

It is important for a functioning whole that the **different levels "talk to each other"**. For example, there may be a clear will and strategy at the EU level, but when the practical work needs to take place primarily at the local level, it is important that they are on board. The EU level can coordinate and guide the overall movement, but it is crucial to **bring EMDS to the local level** by engaging local authorities and actors, giving them ways to influence, and supporting them with guidance and tools. Additionally, national authorities can coordinate and facilitate the movement towards the EMDS within the countries and help bridge the gap between the local level and the EMDS.

EMDS requires multi-level governance

For the common EMDS, which will involve a complex ecosystem of stakeholders, PrepDSpace4Mobility (2023) recommended a **multi-level governance system**, consisting of autonomous data space instances

interconnected through federation. These data spaces, driven by various use cases and regulations, will converge towards federation, interoperability, and alignment. An overarching (European) EMDS authority will govern this, possibly following a geographic or thematic logic. The principle of subsidiarity would allow decision-making at the individual data space level. The EMDS should facilitate a synergistic approach, ensuring balanced stakeholder representation and recognising existing data space investments and other pre-existing data platforms. This approach incorporates the principles of subsidiarity while aligning with the EU strategy for common European data spaces.

Governance scenarios for the EMDS framework

With respect to the long-term operationalisation of the EMDS and its governance, several **possible scenarios** were anticipated by PrepDSpace4Mobility (2023), ranging from a strong role of the EMDS in operating a data space to a more limited role in providing guidelines for interoperability:

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.

All the scenarios imply strong involvement of existing data initiatives, as presented in the Commission's communication on the EMDS (European Commission 2023a).

The governance dimension of the EMDS framework and involvement of the identified stakeholders is within the task of a technical support study[49] launched in January 2024 under the CEF programme (EMDS study).

The **EMDS study** has further explored the scenarios proposed by the PrepDSpace4Mobility, renaming them in the process:

1. EU entity: An initiative or organisation established by the EU would manage the data space with a mixed funding model and stakeholder involvement in supervisory or advisory capacities.
2. Member State-driven consortium such as an EDIC: Member States would lead through a consortium such as an EDIC, funded primarily by contributions from participating Member States and potentially supplemented by EU and national grants. Once established, the consortium could operate as a legal entity, facilitating deployment of cross-border infrastructure, use cases and joint services.
3. European association of mobility data spaces: A European association or a decentralised network of mobility data spaces would set frameworks, requirements, and guidelines, managing interoperability among existing data spaces. Temporary funding would expedite harmonisation and interconnection.
4. EU regulatory framework: This scenario envisions a regulatory framework focused on enforcement and compliance, without the need to establish a new legal entity. The Commission acts as the overarching governing body responsible for setting policies, regulations and certifications.

[49] Study in support of the creation of the common European mobility data space (EMDS) for the European Commission by the consultants Ricardo Nederland B.V. and Ricardo, in collaboration with VTT and Wavestone. Study contract no. MOVE/B4/2023-463.

5. Expert group: A group of specialists from various fields would advise and provide guidelines on best practices and policies to ensure that the EMDS and relevant mobility and transport data ecosystems operate effectively in alignment with EU requirements.

The EMDS study's **main findings and recommendations** were presented at a final webinar on 14 March 2025. The study conducted a comparative analysis of the five scenarios and evaluated their strengths and weaknesses. Scenario 3 scored negatively on more than two of the minimum requirements in the analysis, fell short in several key areas, and was therefore excluded from further consideration. Next, the study concluded that a single scenario alone would not be able to effectively cover all the needs of the EMDS framework. For example, scenarios 1 and 2 are suitable for implementation projects but cannot define rules at EU level without the necessary regulatory framework by scenario 4. Conversely, scenario 4 can define the rules, and scenario 5 could provide guidance, but neither can carry out implementation in practice. Additionally, scenarios 1 and 2 require specific EU legal acts to define their mandate and activities. Therefore, combining the scenarios would better cover rule setting, guidance, and implementation. The study proposes a **staged hybrid governance model**, where stage 1 focuses on alignment and foundation building, stage 2 on implementation and operationalisation, and stage 3 on scaling up and value creation.

The study's **primary recommendations** include:

1) that the strengths of each of the scenarios 2, 4, and 5 should be leveraged and combined in the hybrid governance model;
2) that a new expert group (or sub-group of an existing one) be established;
3) that scenario 2 with an EDIC be leveraged for implementation;
4) that scenario 1 with an EU entity is considered as a contingency if scenario 2 faces delays or challenges;
5) that existing EU regulations serve as the foundation for EMDS;
6) that future regulatory efforts address any gaps or overlaps in existing legislation;[50]
7) that a certification framework is established for sectoral data spaces;
8) that a multifaceted funding model is established; and
9) that alignment and coordination between the EMDS and other European data exchange initiatives is ensured.

We present **our initial reflections** here, and anticipate that our ongoing work in the project will provide additional insights and suggestions:

Preliminary general comments

Firstly, a question arises of whether governance complexities (namely division of competences) of each EU Member State affect the proposed EMDS governance scenarios – and if so, how.

- For example, according to a 2020 report of the Spanish Observatory of Transport and Logistics, in Spain, urban and metropolitan mobility includes administrations from different geographical areas (local, regional, and national) with jurisdiction over transport and traffic, but also other areas of administration that interrelate with the aforementioned (urban planning, environment, energy, economy, health, etc.), which requires intense coordination and cooperation. There are 22 Public Transport Authorities (PTAs) in Spain, which coordinate public transport services for passengers in a metropolitan area. At the same time, the General State Administration (AGE), although it has limited powers in urban and metropolitan mobility, also carries out some functions that impact this area of mobility: planning and development of strategies, provision and operation of infrastructure,

[50] On this topic, see for example Section 2.3.1.2 and Chapter 3 in this report.

provision of transport services (such as the commuter rail services operated by Renfe) regulation, financing, taxation, collaboration, dissemination, promotion of measures, etc.

- In Belgium, competences in the field of transport are distributed between the Federal State (national level), the Flemish Region, the Walloon Region and Brussels-Capital Region. In all regions the municipalities are responsible for the development of integrated local mobility plans. The regions provide a Sustainable Urban Mobility Plan (SUMP) related framework guidance. Some inter-municipal or city region plans have been developed, in order to better tackle common problems and challenges.

These examples reflect a complicated scene, already at national level (other national examples would likely illustrate the same complexity).

Secondly, a related issue concerns the fact that "mobility" covers many different modes of transport, each with their own governance structures. For example, the governance of urban mobility is different than that of rail or aviation. Therefore, how are such divergences reflected in the proposed governance scenarios? How representative of the varied mobility landscape are the scenarios envisaged? How feasible is it to include the mobility governance particularities of each sector under one common umbrella?

A third issue concerns the proposed funding models that include private sector involvement. One key conclusion from deployEMDS so far is the difficulty to engage private stakeholders (and their ensuing data) as urban mobility relies heavily on public sector involvement. Several questions therefore arise:

- Whether private stakeholder engagement can be achieved, and if so, to what degree to support the establishment of the EMDS.
- If private stakeholders engage in the EMDS, what will be their conditions for sharing their data.
- If private sector involvement would de facto steer the EMDS into a more corporate/profit-making avenue and whether there would be conflict of interests.

The proposed timings are also an important variable in the set-up of the EMDS. All scenarios necessitate between 1–3 years to be achieved, if not more, considering the possibility of EU regulation for example. It took approximately four years for the Health Data Space to set up its regulatory framework. A question therefore arises how data spaces should be managed in the meantime until the EMDS governance structure is finalised. Several questions arise in that regard:

- Should data space initiatives – and deployEMDS – set up a temporary governance structure for the local and federated data spaces, or wait until a final decision has been made by the Commission?
- Lacking a determination of the specifications of the common framework under the EMDS, what happens if local data spaces invest in building something that will turn out to not be compatible or even be contradictory to the final governance structure decided?
- When the partition of responsibilities is not yet clearly defined, how can responsibilities and roles be defined at a local level?

Specific comments

Looking at the different scenarios more concretely, as highlighted by the study, all scenarios have their pros and cons. Therefore, combining them in order to leverage the strength of each scenario is an appealing approach. (The combination could also be seen as representing different layers, or functions, of the EMDS.)

Our project focuses primarily on the local level of the EMDS, which, as we have stated above, is crucial for the EMDS. Mobility data sharing predominantly occurs at the local/regional level, where it creates significant value by addressing specific local/regional challenges. (This also helps address broader EU mobility issues.) It is important that the governance of the EMDS, regardless of which scenario or combination of scenarios is taken forward, considers local and regional needs and ensures that Member States and other key

stakeholders are adequately involved. For several scenarios there are some concerns in relation to the local context:

- Regarding scenario 1 (EU entity) there are concerns about the lack of local context sensitivity, and also about limited influence by stakeholders (Member States, data space initiatives, private actors, etc.), which might lead to disengagement from key stakeholders, particularly at the local level.
- About scenario 2 (an EDIC) enhanced local engagement and responsiveness to regional needs are highlighted (as the scenario involves collaboration between Member States, which often are positioned to understand, promote and address local issues), but there are concerns about diverging national priorities, coordination complexity, and slow reactivity to needs and challenges. In addition, there is a lack of clear incentives for Member States to actively engage in supporting local and city-level interests within a European data space framework. Urban and metropolitan mobility challenges are often perceived as local matters, and their relevance may not be directly felt or prioritised at the national ministry level. As a result, even though Member States are formally responsible in an EDIC structure, they may not have the knowledge, political urgency or institutional proximity to act decisively on the needs of cities and regions.
- About scenario 4 (an EU regulatory framework), the potential to balance centralisation with local autonomy is highlighted, but there are concerns that the top-down approach may not account for local specificities and needs and that rules and governance requirements may not fully address local use cases. A principle of "minimum necessary intervention" could ensure that EU-level rules are introduced only where essential for interoperability and ease of access. In practice, this would mean carefully assessing which rules are truly necessary at EU level, and which aspects can (or should) be left to local adaptation. A "local impact assessment" could be a mechanism to ensure that new requirements do not unintentionally hinder innovation or create disproportionate burdens for local actors. This approach would align with Ostrom's principle 8 (nesting) and keeping decision-making at the local level (to the extent possible), as discussed in Section 2.5.
- In scenario 5 (an expert group), there are concerns that it may not fully capture the needs of smaller organisations or less represented regions. This could result in recommendations that are less applicable or feasible for smaller actors, potentially reinforcing existing capacity gaps rather than bridging them, or pushing stakeholders toward high-tech solutions instead of aligning with more frugal, context-appropriate innovations. This risk may already be materialising, as the data space concept is still new to many local/regional stakeholders, who may lack capacity or clarity to meaningfully engage at this early stage. This underscores that ease of use and low-barrier onboarding or integration with existing local digital infrastructure must be a top priority and key criterion for any EMDS components, governance processes, and rules to ensure all stakeholders, especially smaller and less resourced ones, can participate meaningfully from the outset.

Ensuring that local and regional needs are considered in the governance model will be essential for the successful operationalisation of the EMDS framework. For scenarios that are taken forward in a combined model, it is important to find ways to involve national, local, and regional actors in relevant processes, ensuring awareness[51] and participation. We would also like to highlight that, in the context of different scenarios, governance and funding models should actively support less digitally advanced or

[51] On the importance of engaging (at least raising awareness), this example can be provided in relation to scenario 4: In fall 2022, RISE (Lundahl, Sobiech & Thidevall, 2023) surveyed Swedish municipalities on their digitalisation of traffic regulations. One question was about the ongoing revision of the ITS Directive (a proposal for a revised ITS Directive had been released by the Commission in December 2021, and negotiations were ongoing). The survey responses showed that 65 per cent of the municipalities had not heard of it, even though the survey was specifically aimed at the traffic offices in the municipalities (148 out of 290 municipalities responded to the survey).

underrepresented regions and ensure that access to infrastructure, support, and capacity is balanced across Europe.

Aligning local data spaces with the EMDS

And now, some conditions under which multi-level governance could work. As highlighted above, PrepDSpace4Mobility proposed a multi-level governance model for EMDS as part of the requirements for the EMDS governance framework, while acknowledging that data space instances under the EMDS are sovereign in deciding how to tailor their functional requirements and internal governance structure.

While local and regional data spaces in the mobility field will be sovereign and autonomous in their organisational and technical choices, there will be **several advantages** for them to align with the envisaged EMDS:

- to ensure **interoperability** (that the local data spaces are compatible with the EMDS framework, facilitating seamless data sharing and integration between different regions and systems),
- to be able to utilise a **wider range of data sources** (which can facilitate new or improved services but also facilitate policy making through more informed decisions), and
- to **increase cross-border connections and cooperation** (which increases the possibilities for e.g. more efficient transport and seamless travel).

One important aspect of governance for a data space initiative or mobility data ecosystem to consider in order to align with the EMDS is interoperability. One of the objectives of the EMDS is to enable technical, organisational, semantic and legal interoperability for data access, reuse and data sharing between actors (both public and private) (European Commission 2023a).

As stated by the International Data Spaces Association (IDSA), **interoperability** – the ability of different systems and organisations to exchange, understand, and use data – is essential for enabling data sharing and creating value in data ecosystems. As data spaces become more prevalent and diverse, there is also a growing need for intra- and cross-data spaces interoperability. Different data spaces may have different goals, architectures, business models, and governance structures, depending on the authority or community that drives them, but to avoid fragmentation and duplication of efforts, the participants in data spaces need to communicate in an interoperable way with each other and across multiple data spaces, following common standards and principles (IDSA 2024b).

According the IDSA (2024b), there are four main levels of interoperability:

- Technical (transport & syntactic) interoperability refers to the physical and logical connections between systems and data sources, such as protocols, interfaces, and formats. It includes syntactic interoperability, i.e. the structure and syntax of the data exchanged, such as schemas, models, and vocabularies.
- Semantic interoperability refers to the meaning and interpretation of the data, such as concepts, relationships, and ontologies.
- Organisational interoperability refers to the processes, policies, and governance of data sharing, such as roles, responsibilities, and agreements.
- Legal interoperability refers to the acceptance of legal equivalence of contracts and contractual clauses between different data spaces (or data ecosystems).

Given the cross-cutting nature of mobility, there is also a need for mobility data spaces to be interoperable with other sectoral data spaces, so that data can be easily shared and understood across sectors.

Another important consideration for aligning with the EMDS is **data sovereignty**, which allows individuals and organisations to retain control over their data. Data sovereignty implies the possibility for organisations and individuals to control, govern, and ensure the protection of their own data. It involves participating in data

governance and allowing individuals and organisations to decide for themselves how, when, and at what price others can use their data across the entire value chain. This means that data holders can protect user data and ensure it is only used in accordance with defined rules (Farrell et al., 2023).

In **conclusion**, the governance levels for data spaces and ecosystems can be categorised into EU level, Member States level (including NAPs), and local level (where 'local' can refer to collaboration beyond a geographical area). A multi-level governance system for the EMDS with interconnected autonomous data space instances has been proposed. This way local data spaces can operate autonomously (retain their own governance and internal logic, as long as they adopt the interoperability and sovereignty enablers of the EMDS) while benefiting from the advantages of being part of the larger EMDS ecosystem. Aligning local data spaces with the EMDS can enhance interoperability, data sharing, and cross-border cooperation, ultimately fostering innovation and informed decision-making. In subsequent activities, we will evaluate different options for data space governance and develop a multi-level governance framework with business and governance mechanisms to facilitate access to and sharing of mobility data within and across borders.

2.5 Review of governance in the local implementation sites

For this section of the report, we have explored how governance setups in the deployEMDS local implementation sites align with Elinor Ostrom's governance principles (see Section 2.4.2 about the principles and Section 2.4.4 for additional information). While it is beyond the scope of this report to develop recommendations on the governance of data sharing initiatives (that will come in our subsequent activities), this section discusses some suggestions that can inform the discussion on governance principles that could be applied in deployEMDS implementation sites and beyond.

2.5.1 Research questions

We use Elinor Ostrom's design principles for Common Pool Resources (CPR), both as a review lens for examine mobility data-sharing initiatives, and to discuss empirically based recommendations for the deployEMDS implementation sites, and for the further development of EMDS (see section below "Why we use Ostrom's governance principles" below for more details). Ostrom was a Nobel laureate for her analysis of economic governance, particularly the commons. She developed principles for how to design a governance structure in a sustainable and collaborative way.

According to McGinnis and Ostrom (1992), in "(...) the diversity of the settings, one should not expect to be able to discover a single best formulation or set of optimal mechanisms (or rules)". However, design principles are meant as essential elements or conditions that help to sustain common resources. Focusing on underlying principles rather than specific mechanisms, we can learn lessons from a wide diversity of small field settings that have relevance to the design of robust international cooperations.

Our research questions:

- How is governance currently set up in the deployEMDS implementation sites and similar data-sharing initiatives related to mobility?
- How can the governance of data spaces be designed to enable and promote data sharing in the mobility sector?

2.5.2 Why we use Ostrom's governance principles

In this report, we use Ostrom's design principles for Common Pool Resources as a lens to systematically analyse the governance of a number of existing data sharing initiatives. Her eight principles have already served as a basis for determining governance strategies for a number of collectively governed resources, including open-source software and digital public goods (Ruhaak et al., 2021).

Our reasons for using Ostrom's design principles in our analysis are multifold:

- We want to focus on a sustainable use of (digital) resources.
- Given the similarities between overconsumption of physical resources and over-exclusion from data sharing, lessons about institutional design can be drawn from Ostrom's eight principles and help us to unpack ongoing discussions over governance rules and procedures (Simcoe, 2014).
- Ostrom's principles adapt particularly well for examining a diversity of settings, where it will be difficult to find one (or multiple) best governance mechanism(s). Given that European data spaces will probably need to use multiple governance principles, also across different levels of governance (local, national and European), Ostrom's principles are a good fit.
- Ostrom's design principles applied to digital phenomena (i.e. digital commons) have only been examined to a limited extent (with notable exceptions, see Linåker and Runeson 2022, Coyle et al. 2020a, Ruhaak et al., 2021) and not in relation to data spaces (to our knowledge).

2.5.3 Public value and data spaces as commons

Data spaces can be defined as data commons. According to Ruhaak et al. (2021), "when a group of people collectively decide to organize a system to govern a shared data resource and their use of it, a data commons arises." At the core of data commons, is a sustainable and ethical approach to data production, use, reuse, and redistribution, taking place through collaboration among data users and producers (Ruhaak et al. 2021).

Data sharing between businesses and society, and the transformation of data into a common good serve to make better decisions and create public value.[52] If data is understood as a common, governments should be able to access it to ensure the public value of the data use. Society can derive valuable information from data and use it for the public interest to make e.g. mobility cleaner and fairer. This requires more data sharing, with (local) governments – but also with researchers, non-governmental organisations and citizens – who can use data to better shape public spaces according to the needs of citizens.

Data commons is also an alternative way of seeing and imagining data governance. This alternative perspective originates from a critique of the current norms and products where companies assume control over data for commercial benefits. Alternative data governance serves "individual or collective interests grounded in human rights, data rights and consumer rights".[53] Tarkowski et al. (2022) stress that it is important to go beyond the regulation of markets and correction of market failures when it comes to digital transition. The aim should not be to develop another (European) dominant platform, which would rely on the same exploitative business models. Instead, a decentralised architecture of the digital space involving a variety of actors, also public and civic, is possible.

On a practical level, data commons are operated in different ways; some share data openly, while others keep the data private or impose copyleft-like or non-commercial conditions on reuse. Data commons also use different decision-making mechanisms, with some having members who vote on the important questions, and others might elect representatives to do that (Ruhaak et al., 2021). However, there are some key principles that characterise healthy commons, which Elinor Ostrom has developed (Ruhaak et al., 2021). We will examine these principles in the following sections.

[52] Public value – arising when data is used to deliver more effective public services, to improve our environment, and make our lives healthier – stands in contrast to purely monetary value (Coyle et al. 2020b).
[53] https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/data-futures-lab-glossary/.

2.5.4 Governance in deployEMDS implementation cases

In this section, we examine the governance setups for mobility data sharing in the deployEMDS local implementation sites. During workshops with the sites at the Stockholm-conference of deployEMDS in October 2024, it emerged that the development proceeds faster and more value is created at the local level. The actual work will happen there, even if these sites need both skilled persons and guidance from deployEMDS and the EU. According to the workshop participants, the local level approach offers several advantages, including the feeling of autonomy and ownership, as well as responsibility for the data sharing; and allowing for better community management. This approach also offers benefits in terms of cost, time, trust, and flexibility. The participants also stressed that 'local' should not be limited to a specific geographic area but can also refer to a collaboration between multiple cities on specific use cases.

Below, we are summarising the theoretical framework used in this part of the report – the design principles for Common Pool Resources coined by Ostrom (see the list of principles in Section 2.4.2) – and discuss our findings from the literature and from the deployEMDS implementation cases. The aim is to provide examples of how governance of mobility data sharing is set up in different contexts and provide some explorative considerations for how data spaces could be developed further. In addition, we provide questions (in Annex 3) organised by each of Ostrom's principles, that can guide (self-)evaluation of existing data space governance mechanisms and ideas about what to consider when developing these mechanisms further. *Please note* that we have renamed some of Ostrom's principles to adapt to the analysis of digital commons.

Principle 1: Clearly defined boundaries

The first principle is about setting clear boundaries of the resource and the actors who can use the resource, to avoid confusion about what is managed or for whom. This involves specifying the full array of actors who will participate in the governance, management, and use of resources (McGinnis & Ostrom, 1992).

Considering the deployEMDS implementation sites, the geographical boundaries range from municipal to regional. Some of the cases share data only between public sector actors, while others focus on sharing between public and private actors (although the latter is typically limited). None of the cases has a specific focus on involving other types of actors (such as civil society organisations, academics or lay citizens). The virtual boundaries are variably clear across the implementation use cases. Some of them define data-sharing rights and obligations formally (e.g., by legislation such as the ITS Directive), or by the orchestrating body's assignment through public procurement contracts (typically by the local Public Transport Authorities). Others have a more informal approach characterised by collective incentives and visions for a collaboration (e.g., exemplified through the EONA-X initiative in the case of Île-de-France).

Not all deployEMDS cases have articulated and formalised their values but most of them aim at supporting both public and private value creation (e.g. by setting out to improve air quality and by creating new business opportunities). However, some of our interviewees perceive a tension between the private and public value of data sharing. For instance, companies tend to require full control of how their data is accessed and used, given that they associate costs with data sharing, and aspire to get financial returns on investment, while public entities have a mandate to comply with regulation requiring climate-reporting or GDPR-compliance.

While carrying out this work, we realised that **codes of conduct** can be useful as a tool for defining commons' principles. Some prominent codes, which could be used as a starting point, are illustrated in the list below. Moreover, it may be beneficial for the deployEMDS project to consider developing a code of conduct, agreeing and clearly outlining the values of the future EMDS.

Codes/principles	Extracts relevant to boundaries and value definition
The Data Space for Smart and Sustainable Cities and Communities (DS4SSCC) Multi-Stakeholder Governance Scheme (p. 21) contains a prominent code of conduct.	"The sharing and re(use) of data via DS4SSCC should create tangible societal value and public benefits on top of economic value. Local authorities, communities, and citizens should be the main beneficiaries of data sharing and reuse in the context of DS4SSCC."
The Code of Conduct on Data Sharing in Tourism	"In general terms, increased access to data based on fair, reasonable and non-discriminatory conditions may benefit the efficiency and competitiveness of the European tourism sector."
SITRA rulebook for a fair data economy: "5. Ethical principles: Shared values of the Data Network":	"All actors in the data network should promote fairness, justice, and equality among individuals. Fairness means that everyone is treated with respect regardless of their socio-economical background or status. Likewise, the benefits (economical and others) must be balanced between all stakeholders in such a manner that individuals that are the source of data are not seen as mere exploitable resources."

Principle 2: Appropriate rules

The second principle focuses on appropriate rules (technical, legal, economic, and organisational). It underlines that rules affecting the distribution of costs and duties in robust commons should match the distribution of benefits and rights (McGinnis & Ostrom, 1992). Ideally, the rules are deemed fair by most stakeholders (Ruhaak, 2021).[54] Moreover, rules should be tailored to fit particular local circumstances (McGinnis & Ostrom, 1992), which is in line with the current focus on local implementation sites in deployEMDS. Finally, this principle also implies transparency regarding both rights and duties, and regarding how value from data returns to people and organisations (Coyle et al., 2020a).

An example of how rules, and a certain level of transparency, can be implemented in practice is illustrated by the **Rulebook** used by the deployEMDS implementation site in Tampere. In the Tampere case, Fintraffic (steered by the Finnish Ministry of Transport and Communications) coordinates an open-source network of about 200 organisations. Organisations can join the space only if they agree to comply with the Rulebook[55], based on Sitra's "Fair Data Economy Rulebook".[56] The Rulebook – accessible to the general public on the website of Fintraffic – lists the rules for sharing datasets, as well as for providing services and agreeing on cooperation. In the Tampere case, the "terms and conditions of use" for a dataset/service set by the data provider specify how the data/service can be used within the data space.

[54] There are different interpretations of what "fair" entails. Ruhaak (2021) identifies two such areas "Fair use: the rules governing the use of the resource (e.g. data) aim to prevent harm and unwanted exploitation" and "Fair outcomes: over time, the rules put in place ensure that your contribution to the organisation and its resources match the benefits one derives from their participation".
[55] https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy/#preface-and-templates.
[56] https://www.fintraffic.fi/en/rulebook.

There are of course **other ways to build common rules** for a data space. The interviewees from the Île-de-France implementation site mentioned two distinct approaches: by slowly building a trusted community through personal relations, or by smart contracts, where (minimum) conditions are agreed upon automatically (without any personal relation between the data holder and the data user). The latter modality is currently being developed in one of the Île-de-France use cases. Another way for regulating data-exchange, similar to smart contracts, is illustrated by the Flemish Mobilidata case, where the data space participants need to sign collaboration contracts to connect and to provide (real-time) data to the Mobilidata "interchange". These contracts, in combination with data protocols, determine modalities, rights, purpose and duration of the data sharing. However, in practice, Mobilidata finds it difficult to strike the balance between establishing strict rules and duties, and getting third parties interested to connect to the data space in a voluntary (non-funded) setting. Therefore, the contracts are negotiable to some extent, depending on what the connecting party brings to the table (e.g. the larger the existing user base, the more lenient the contract negotiation can be expected). This probably means that big players get better conditions, which could be adverse for fairness and equal access.

Principle 3: Rule-making processes

This principle focuses on the collective element of the commons. Most actors affected by the rules that govern the resources (data) or the community should be able to influence the rules (Ruhaak et al., 2021). Moreover, the interests of all relevant groups must be incorporated in the ultimate agreement to avoid the undermining of the regime's sustainability by those who are excluded (McGinnis & Ostrom, 1992). The Code of Conduct developed by the preparatory action for a Data Space for Sustainable and Smart Cities and Communities (DS4SSCC)[57] exemplifies the latter point by stressing that "(p)articipants, including local governments, communities, and citizens, should have a say in decision-making processes" (of the data space).

The cases reviewed in our study show that often the financing parties are shaping the rules. In government-driven data-sharing initiatives, the governance structure and rules are defined by platform providers and orchestrators in a centralised way. These organisations are often steered by their respective boards of directors, representing their owners, which include stakeholders such as regional public transport authorities, private transport providers, and municipalities. Entities with more resources tend to have greater influence on the direction of these platforms, while those affected by data use (e.g. communities or citizens) cannot influence the data governance structure and rules directly.

In contrast, the OpenStreetMap-community (one of our case surveys) operates with a decentralised governance model, where rules and processes are collectively defined through sub-communities, and local user groups. This model is more open, and allows for greater community participation and influence, while relying on established guidelines for electing decision-makers and on communication facilitated through forums, mailing lists and a common wiki.

When interviewing the deployEMDS implementation sites, several of them highlighted the need for a sustainable orchestrator that can manage and facilitate the data sharing (including maintaining technical platforms, standards, and procurement). However, the set-up and definition of such an orchestrator seems challenging. As a case on point, the Flemish Smart Data Spaces (VSDS), with its 500 actors, is today governed and facilitated by Digital Vlaanderen (the regional Agency for Digital Government). They maintain

[57] This code provides the foundational principles, roles, responsibilities, governance structures and legal frameworks for participants of the data space. It underlines that it is crucial to co-define shared governance principles and ensure buy-in. Source: https://static1.squarespace.com/static/63718ba2d90d0263d7fc1857/t/651ea670a884c256d84f4864/1696507511589/DS4SSCC_D2.2+Multi-stakeholder+governance+scheme.docx.pdf.

the standardisation process, the building blocks for clients and publishers, the data catalogue, and provide hands-on support through its “MacGyver” team. As the current data sharing is centred on open data and only on the region of Flanders, requirements on the governance are considered comparatively limited. However, when integrating with other parts of the country (e.g., the Brussels region) and with the EMDS, the number of actors and requirements may increase significantly. The interview from the Flanders case expressed a need for establishing a new governance system through deployEMDS in order to cater for such growing numbers.

In terms of sharing open versus closed data, the governance of closed data seems particularly challenging. Interviewees from some of the deployEMDS implementation sites emphasised the imminent challenge to onboard private actors, with specific requirements for control, audit, and traceability of non-open data sharing. Private actors are more keen to control not only the data sharing but also data use. Sharing commercial and sensitive data requires capabilities for control and monitoring of who uses the data, when, and how (ID certification and traceability). One of the critical elements is the building of trust among data holders, especially towards competitors or third-party service providers.

These types of control need may be less stringent for open data, although still present. For instance, the more socially oriented wing of the open data movement proposes to retain some rights for the public by the so-called “copyleft” licensing (which is a legal method of granting certain freedoms over of copyrighted works with the requirement that the same rights be preserved in derivative works) (Broumas 2017, in Dulong de Rosnay & Stalder, 2020). This, to avoid private appropriation and commodification without a return to the community, the state or the general public, e.g. by keeping the data closed (by way of public procurement conditions), or require that transport apps, which are reusing these data, be released as free software (Dulong de Rosnay & Stalder, 2020).

Principle 4: Monitoring

This principle sets out that those who monitor (i.e. audit conditions and participant behaviour) should either (i) be the actual participants of the commons or (ii) be accountable to the participants (McGinnis & Ostrom, 1992). In a data common, the monitoring is done not only to ensure compliance with the set values, business rules and rule of law, but also to oversee the security of the architecture, data quality and integrity.

Technical monitoring plays a specific role in data commons, including the respect for rights and duties for access, use and collection/contribution of data (i.e. mode of access, length of access, type of use, purpose of use etc. at specific time intervals, or continuously) (Ruhaak et al., 2021). A specific emphasis is also placed on contractual terms and transparency (Coyle et al., 2020a).

Our examination of cases shows that government-driven ecosystems often use both internal and external monitoring mechanisms, while community-driven ecosystems tend to rely on self-monitoring and community review. When it comes to the deployEMDS implementation sites, our interviewees emphasised that the monitoring of data use (who, when, how) is particularly important when sharing commercial and sensitive data. Several of the surveyed implementation sites, however, highlighted the lack of technical infrastructure and governance that can facilitate this type of monitoring.

In terms of transparency, in community-driven initiatives like the OSM, the monitoring process tends to be transparent and open to the community. Their decentralised approach ensures community oversight and maintains the integrity of the data, with the OSM Data Working Group providing an internal instance for handling serious breaches. In government-driven initiatives that we reviewed, the monitoring mechanisms tend to be less transparent (e.g. the monitoring criteria and results are not published openly).

Principles 5 & 6: Sanctions and conflict-resolution mechanisms

We have merged Principles 5 and 6 in this report given that they touch upon similar issues: conflict, which can potentially lead to sanctions. Principle 6 is mainly about having an effective and accessible (including inexpensive) way to handle conflicts; as well as being explicit about which conflicts will be solved internally or externally (Ruhaak et al., 2021). We did not examine how this principle is applied in the deployEMDS implementation cases. However, other cases from the literature show that conflicts within the government-driven data initiatives (i.e., Samtrafiken, Mobilidata and HSL) are informally managed by the orchestrators, which act as the main facilitators for resolving disputes. However, these three cases do not have any formal conflict resolution-mechanisms in place. Perhaps also because serious conflicts seem to be limited (no conflicts have been reported so far among these cases).

Examining cases outside of the deployEMDS, the community-led case of OpenStreetMap (OSM) shows that issues are usually resolved by discussions and consensus among community members. If the community cannot resolve problems (such as copyright violations, editing the map in a way that doesn't reflect the reality, and inappropriate use of bots), the OSM data working group intervenes to address conflicts. In particular, the working group members make sure that community guidelines are followed. If a map editor does not abide by guidelines, (s)he risks losing the right to participate in OSM.

Principle 5 underlines the importance of graduated and proportional sanctions, which implies that intent and harm are considered when applying sanctions (Ruhaak et al., 2021). In practice, in data commons, the consequences for data misuse can range from notifications to withdrawal of access, fines and other penalties (Coyle et al., 2020a). For instance, first-time offenders might receive warnings, while repeat offenders could be banned. There should also be processes in place that allow those who broke the rules to earn back the trust of the community (Ruhaak, 2021).[58]

The deployEMDS implementation sites have applied serious sanctions to a very limited extent so far. One of the implementation sites, Tampere, foresees the application of sanctions in the event of significant breaches of contract. In that case, the steering group can “terminate the offending party’s agreement with immediate effect, in which case the offending party loses access rights to the data and, if so required by the other parties, must return/delete any data that has already been obtained” (Fintraffic undated). Similarly, in the cases of Samtrafiken and HSL, sanctions include the termination of API access keys if data has been used in an abusive way. In the case of Mobilidata, actors joining their data space are expected to contribute to the Mobilidata mission, which focuses on enhancing road safety, and reduction of throughput and emissions. Not complying with the mission results in disconnection from the data space. However, it could be difficult to establish non-compliance given that the mission is very broadly formulated (the conduct criteria for each of the values are not detailed). It could be argued that the sanctions are not graduated (given that the only sanction, disconnection, is quite serious), and that sanctions could be too arbitrary, considering the lack of clear criteria of mission breach.

Principle 7: Minimal recognition of rights to organise

In the context of data commons, this principle is about the need to align the decisions made about the collection and use of data with formal rules and requirements, e.g. data protection regulations (Ruhaak et al., 2021). Formal recognition stretches beyond regulation and can take different forms, e.g., the

[58] https://www.fintraffic.fi/en/trafficecosystem/rulebook.

OpenStreetMap is globally recognised and used by various government levels and designated as a "Digital Public Good"[59] by the UN-endorsed Digital Public Goods Alliance.

The deployEMDS implementation sites are all affected by formal regulation, including EU legislation mandating data sharing of certain mobility data (see Chapter 3 for more information on legislation affecting mobility data sharing). In some data-sharing initiatives, such as Trafiklab, the orchestrators provide support to public and private actors in complying with EU legislation.

Principle 8. Nested commons

This principle is about appropriation, provision, monitoring, enforcement, conflict resolution, and governance activities being organised in multiple layers of nested entities (McGinnis & Ostrom, 1992). The principle refers to the need for different data commons to interoperate with each other, or to divide one large commons into smaller, nested commons that interact with each other. The aim is to allow smaller commons to make decisions that better reflect their local context (Ruhaak et al., 2021).

Decentralised decision-making has multiple advantages, including access to local knowledge, rules that are better adapted to local context, and simultaneous experimenting with rules in various sites, thereby reducing the probability of failure for a larger endeavour (Ostrom 1999). Nested governance is similar to the 'principle of subsidiarity', i.e. decentralisation of tasks to the lowest level of governance with the capacity to conduct it competently (Marshall, 2008). This is relevant in relation to the envisaged multi-level governance system for the common EMDS, where autonomous data space instances will be interconnected through federation under the governance of an overarching European authority, incorporating the subsidiarity principle by allowing decision-making at the individual data space level, as proposed by the PrepDSpace4Mobility project (see section 2.4.7 for details).

The deployEMDS implementation use cases are nested to different extent, while several lack efficient coordination across the governance levels. For example, the Milan-case expressed the need to develop a structure that can facilitate the coordination of data sharing to guarantee data quality, standards and interoperability, and to reduce effort for actors to share and use data. As a case in point, currently the Milan PTOs have to send their data both to the deployEMDS implementation case and to the regional data ecosystem E015, duplicating their effort. The example highlights the complexity in how data ecosystems on different levels and overlaps within the context of EMDS need to find ways of integrating and collaborating on data sharing, where harmonising governance structures is a key enabler.

On a similar line, Sweden already has potential overlapping resources, such as the national data portal – dataportal.se – where many different organisations provide metadata to open data sources, and National access points (NAPs) that facilitate access to and reuse of transport-related data, in order to help support the provision of EU-wide interoperable travel and traffic services. These examples highlight the potential overlaps and the need of harmonising governance structures between the current deployEMDS data spaces and the future EMDS on the one hand, and other regional, national or international data sharing initiatives on the other hand.

[59] According to the UN Secretary General's Roadmap for Digital Cooperation, digital public goods are open-source software, open standards, open data, open AI systems, and open content collections that adhere to privacy and other applicable laws and best practices, do no harm, and help attain the Sustainable Development Goals (SDGs). This definition is operationalised in the form of nine baseline requirements that must be met to earn recognition as a digital public good. Source: https://www.digitalpublicgoods.net/digital-public-goods.

The OpenStreetMap (OSM) is another example of how nested governance works in practice. The OSM is based on the work of several local user groups and mapping projects, which are collaborating on a common technical platform across various levels. Localised rules in OSM are tailored to specific sub-communities, while overarching principles are applied universally. Issues unresolved at the local level are brought up at another level of governance, allowing an effective monitoring, enforcement, and conflict resolution. The goal is to solve any issues through consensus norms, as decentralised as possible.

However, even if the local perspective is crucial for sustainable data commons, one of our interviewees emphasise that, it is questionable whether municipalities have the resources to take on long-term or skills to shoulder such a responsibility. There is a risk that a lack of national coordination will lead to fragmented solutions and a lack of standardisation, which may hinder effective data sharing on a larger scale. This has already happened with regard to digitalisation and open data in Sweden. The lack of institutional leadership of its digital government agenda, and the absence of the government's political support, has led to a fragmented approach to the promotion of open data across the public sector, at the local, regional and national levels (OECD, 2019).

2.5.5 Conclusions

This work investigated the governance set-ups among deployEMDS implementation sites and similar initiatives. We looked specifically at how governance of the data spaces can be designed to enable and promote data sharing in the mobility sector. To systematically analyse the governance of data sharing initiatives, we used Elinor Ostrom's governance principles, which highlight the importance of clear boundaries, appropriate rules, inclusive rulemaking, robust monitoring, and effective conflict resolution. The principles aim at supporting the design of sustainable governance structures. We had a specific focus on data sharing that promotes public value and collaboration among data users and data holders.

Our examination of deployEMDS implementation sites confirms that the local level is crucial for data sharing (as mentioned in Section 2.4.7), offering advantages like autonomy, community focus, and better alignment with local needs. Challenges include the articulation of the values at the basis of the data space, strategic guidance, and coordination across different governance levels. Our findings are summarised under each of Ostrom's principles below:

- Principle 1: Not all deployEMDS cases have sufficiently defined and transparent articulation of boundaries, which makes it difficult for stakeholders and potential participants to have a clear understanding of the data spaces at hand. Moreover, the local implementation cases have not fully formalised their common values and ethical principles in a way that they can be held accountable by relevant stakeholders and by the communities they ultimately serve.
- Principle 2: Our initial assessment indicates that the technical, legal, economic and organisational rules of the deployEMDS cases could be made more explicit. In particular, the costs and benefits, as well as rights and duties of the data space participants could be made more explicit and publicised in a transparent way.
- Principle 3: There seems to be a lack of mechanisms (such as advisory groups, panels, and surveys) to ensure that those affected by the data sharing can influence the rulemaking. This means that some stakeholder groups (i.e. data holders, data users, and potentially data subjects) are probably not able to articulate their perspectives and have their interests fully represented. This risk is particular significant for the generally under-represented groups that could be impacted by the data sharing and use, but lack information, skills and resources to engage actively. Not all data spaces have developed strategies for how to onboard new stakeholders, while balancing the public and private interests, or how to consider a return of the benefits of data sharing to the community or the general public.
- Principle 4: There is a need to consider more thoroughly both internal and external monitoring mechanisms of the data spaces and take the necessary steps to ensure the transparency of the

monitoring, e.g. clearly documenting both the process and the results, and making them accessible to the general public (to the extent possible).

- Principle 5 & 6: Not all the deployEMDS cases examined have clearly set out how they will solve (potential) conflicts and specified which conflicts will be solved internally or externally, nor considered graduated and proportional sanctions, including sanctions for non-alignment with the values of the data spaces.
- Principles 7: It is important that data governance decisions align with formal rules and requirements (e.g. GDPR or the ITS Directive). There may also be self-imposed requirements (e.g. the Digital Public Goods–label, or the "Principles for digital development",[60] which expect adherence to "do no harm" and "anticipate and mitigate harms" principles). We do not have any specific recommendations in this regard other than to highlight that adapting to mandatory and voluntary requirements can make data spaces more sustainable and responsible.
- Principle 8: The principle of nesting is mainly about keeping the decision-making power at the local level (to the extent possible) to allow smaller commons to make operational and collective choice decisions that better reflect their specific context and local knowledge. At the same time, it is also worth considering what kinds of governance support – in terms of resources, guidance and skills – local data spaces would need to face this type of responsibility, e.g., the responsibility for overarching decisions and mandates, might be better placed at national or regional levels, with the possibilities for local stakeholders to influence these decisions.

As a next step, the project could develop recommendations for sustainable and collaborative data spaces, which align to each of Ostrom's principles, keeping the public interest at core. Developing a code of conduct is also something we can consider moving forward.

In subsequent activities, we will build on this work as we develop a multi-level governance framework with governance mechanisms to facilitate access to and sharing of mobility data within and across borders.

2.6 Summary and conclusions of Chapter 2

Mobility data sharing offers numerous benefits, such as improving urban planning, optimising traffic management, improving public transport systems, and developing new, efficient mobility services. It can also support environmental sustainability, by identifying strategies to reduce emissions or promote sustainable transport options. Access to real-time data helps users make informed travel decisions, avoid congestion, and choose efficient routes and modes of transport. By collaborating on mobility data, authorities, companies, and the public can create smarter, more sustainable mobility systems.

Data products in the project's use cases include road infrastructure, traffic rules, environmental zones, public transport (static and real-time), multimodal data, dynamic incidents, roadworks, mobility services (e.g., micro mobility, car sharing, bike sharing), mobility demand, pedestrian accessibility, electric vehicle charging, multimodal traffic counts, dynamic traffic, meteorological, air quality, and MaaS usage data. This demonstrates the breadth of data considered for mobility use cases.

In the past decade, **data generation and sharing** have surged due to technological advances and the datafication of life. The non-rivalrous nature of data allows it to be reused across applications, prompting efforts to enhance accessibility and sharing. Innovations and regulations are fostering a collaborative data

[60] The principles can be useful in many different ways. They may serve as a design checklist in the early phases of creating a new project, policy, or institution, or they may serve as a way to kick-off critical conversations as to how to maximise impact and minimise risks to people and communities. Source: https://digitalprinciples.org/.

environment, with new platforms and ecosystems emerging. Privacy-preserving technologies and decentralised models aim to balance control and accessibility, though barriers remain.

Mobility is a **complex and evolving field** that overlaps with other areas such as technology, infrastructure, energy, and urban planning. The mobility domain also involves diverse stakeholders, e.g., public transport authorities, urban planners, and private companies, each with different priorities and standards. In addition, different modes of transport often operate under different regulations and technologies. There are also geographical variations as transport systems vary from one location to another, influenced by local policies, infrastructure, and urban planning strategies. Data sharing is crucial in the evolving urban mobility landscape as a means to address mobility challenges. The mobility field's complexity and stakeholder diversity present both challenges and opportunities.

Governance, and data governance, play a central role in data spaces and ecosystems, where data is shared and exchanged among various stakeholders, to help manage data efficiently, ensure compliance, build trust, and drive innovation, while also overseeing the proper functioning of the data space or ecosystem as a whole.

However, defining **terms and concepts** such as 'data', 'governance', and 'data governance' proves difficult due to the many varying definitions that emphasise different aspects and change depending on the context. This means that, depending on the specific context and needs, one definition (or a combination of definitions) may be more appropriate than another.

Governance challenges span organisational, legal, and technical aspects, influenced by power dynamics. Many of the challenges are interconnected and influence several aspects of governance. Addressing more complex and multifaceted challenges might require a holistic approach that considers organisational practices, legal frameworks, technical solutions, and the broader power dynamics at play. Our analysis shows that the challenges frequently mentioned in the literature are largely the same as those faced by our implementation sites in the project. Challenges among the sites include:

- *organisational challenges*, such as how to organise around data sharing, limited capacity, slow digital transformation, trust issues, opaque data contracts, reluctance to share data of public interest, insufficient financial resources;
- *legal challenges*, such as navigating legal frameworks, data sharing obligations in tenders/contracts, legal liabilities for data breaches/misuse;
- *technical challenges*, such as standards harmonisation, integrating legacy systems, ensuring data sovereignty, ensuring data protection, and ensuring data quality; and
- challenges related to *power dynamics and asymmetries*, such as the challenge of clearly explaining purpose of data sharing and demonstrating societal value.

Several **governance principles**, such as participation, accountability, transparency, responsiveness, efficiency, rule of law, fairness, and sustainability, provide overarching guidelines for developing a governance framework that ensures trust and cooperation in data sharing. They can be detailed further in specific governance mechanisms and applied to our project. Additionally, the FAIR principles provide a framework for enhancing data findability, accessibility, interoperability, and reusability, promoting innovation and collaboration.

Regarding **data space governance**, which extends beyond data governance to also include the management of the partnerships and collaborations needed for unlocking the value of data, we consider that **a community-based, purpose-driven approach** that takes into account domain-specific contexts is crucial for ensuring stakeholder buy-in and addressing the diverse technical, social, political, and economic environments in which data is produced and consumed. Evolving frameworks in the data space field emphasises flexibility and adaptability, recognising that there is no one-size-fits-all solution. By focusing on

both **technical and governance building blocks**, these frameworks help ensure that data spaces operate efficiently and securely.

A **multi-level governance system for the EMDS** with interconnected **autonomous data space instances** has been proposed. This way local data spaces can operate autonomously (retain their own governance and internal logic, as long as they adopt the interoperability and sovereignty enablers of the EMDS) while benefiting from the advantages of being part of the larger EMDS ecosystem. Aligning local and regional data spaces with the EMDS enhances interoperability, data sharing, and cross-border cooperation, ultimately fostering innovation and informed decision-making.

Our review of **governance in deployEMDS local implementation sites** using Elinor Ostrom's governance principles, confirms the importance of the local level for mobility data sharing, offering benefits like autonomy, community focus and better alignment with local needs. However, challenges include articulating values, strategic guidance, and coordinating across governance levels. Boundaries are not always clearly defined, values and ethical principles are not fully formalised, and rules need to be more explicit. Mechanisms to influence rulemaking are lacking (for stakeholders affected by the data sharing, e.g., local communities and organisations representing citizens), and onboarding strategies are insufficient. Monitoring mechanisms need to be more transparent, and conflict resolution strategies are unclear. Compliance with formal and voluntary requirements is crucial. Decision-making power should remain local (to the extent possible), with support from higher levels.

In forthcoming project activities, we will build on this work when **developing business and governance mechanisms** to facilitate access to and sharing of mobility data within and across borders. Specific governance and legal challenges are also being addressed in the project's **policy labs**.

3 Legal landscape for mobility data sharing

This chapter of the report results from a preliminary and overview analysis of the legal landscape and the opportunities and limitations the legislation implies regarding mobility data sharing. It starts with an introduction to the legal landscape and then provides more detailed introductions to various laws and regulations relevant. The chapter also explores the intersection of the laws and regulations on data and its use in general, and their impact in relation to sector-specific regulations on mobility. The chapter lays the foundation for understanding the current situation and provisions for mobility data sharing from a legal perspective, as well as possible regulatory gaps and overlaps. This will inform our subsequent project activities, such as the policy labs, where we address specific legal challenges identified in the preliminary analysis and in the use cases of the implementation sites. Legal challenges will also be further analysed in relation to our task of developing legal tools for compliance and interoperability in mobility data spaces.

3.1 An introduction and overview to the legal landscape for mobility data sharing

Legal considerations are central to mobility data sharing as well as to the organisation and governance of mobility data spaces. For instance, several legal frameworks and instruments have an impact on whether and how mobility data can be shared (e.g., legal rights to data access, legal restrictions on sharing certain categories of data).

Most of the data-related legislation applicable in EU Member States is influenced or directly determined by European legislation from the EU. The EU increasingly enacts legislation that affects access to and use of data. Some of these laws apply directly in the EU Member States, without prior sanction by the national legislators, while others must be implemented in national law before they can take effect.[61] For instance, in the area of data protection, the legal situation in the Member States is primarily governed by EU legislation. When the EU's General Data Protection Regulation (GDPR) became applicable on 25 May 2018, it superseded all Member States' data protection laws based on the previous 1995 Data Protection Directive.

Two dimensions are relevant for deployEMDS, as well as future EMDS activities:

- horizontal EU legislation, encompassing legal instruments applicable across different sectors and sectoral data spaces, and
- mobility-specific legislation, specifically on the provision of open data for different purposes.

In terms of **horizontal EU data legislation**, the most prominent piece of legislation in the data domain remains the GDPR. However, since its introduction, the regulatory landscape has evolved. The EU is gradually shifting from a data protection paradigm to facilitating data sharing and reuse under fair conditions,

[61] This is due to the difference between EU regulations and directives. EU regulations become directly applicable in the same way at the same time in all Member States, while EU directives must be implemented in national law in each Member State and they usually have some flexibility in how they implement the rules if they achieve the intended outcome. An EU regulation thus is a binding legislative act that must be applied in its entirety across the EU and each Member State must ensure their domestic laws do not conflict with the regulation. However, certain national regulations that supplement the EU regulation are sometimes needed, e.g. to designate which authority should have a certain task. Once an EU law (regulation or directive) is passed, it can be necessary to update it to reflect developments in a particular sector or to ensure that it is implemented properly. The Parliament and Council can authorise the Commission to adopt delegated or implementing acts. While these acts are of a non-legislative nature, they are still legally binding. Delegated acts amend or supplement existing laws, notably in order to add new non-essential rules. Implementing acts introduce measures to ensure laws are implemented in the same way throughout the EU.

aiming to exploit data potential for socio-economic purposes. Data is at the heart of the EU's digital transformation, and this change is facilitated by new horizontal legal instruments in the data domain. According to the EU's data strategy, these instruments will address identified challenges such as the lack of trust and fairness in the data economy. Therefore, while the GDPR remains an important piece of legislation, it is now part of a broader and evolving framework for data in Europe.

Several of EU's horizontal legal instruments in the data domain are summarised in the table below. Additionally, other legal regimes that serve wider purposes, such as competition law, contract law, and IP rights, must also be considered when sharing data.

Table 2 – Key EU horizontal legal instruments in the data domain

Legal instrument	Description (what, why, when)
Artificial Intelligence Act (AI Act)	A legal framework for the development and use of AI in the EU, addressing risks to health, safety, and fundamental rights. This is to balance safety and fundamental rights while strengthening AI uptake. It entered into force on 1 August 2024 and the application will be staged over two years.
Data Governance Act (DGA)	This act aims to facilitate data sharing across the EU by regulating the reuse of public sector data, data intermediation services, and data altruism. It establishes the European Data Innovation Board (EDIB) to steer data governance and prioritise standards. It entered into force on 23 June 2022 and has been applicable since 24 September 2023.
Data Act (DA)	This act aims to ensure fair access to and use of data, particularly data generated by connected devices, and to enhance data sharing between businesses and public bodies. It entered into force on 11 January 2024 and will be applicable from 12 September 2025.
Digital Markets Act (DMA)	This act aims to ensure fair and contestable digital markets. It targets large online platforms (gatekeepers) to ensure fair competition and prevent unfair practices. It entered into force on 1 November 2022 and has been applicable since 2 May 2023.
Digital Services Act (DSA)	This act aims to create a safer online environment for consumers and companies in the EU, addressing illegal content and protecting users' rights. It introduces responsibilities and a system of accountability and transparency for providers of online intermediary services (online platforms). The main goal is to prevent illegal and harmful activities online and the spread of disinformation. It entered into force on 16 November 2022 and has been applicable since 17 February 2024 (some provisions began to apply earlier).

General Data Protection Regulation (GDPR)	This regulation regulates the processing of personal data within the EU, enhancing privacy rights and data protection. It entered into force on 24 May 2016 and has been applicable since 25 May 2018.
Free Flow of Non-Personal Data Regulation	This regulation aims to ensure that non-personal data can be processed and stored anywhere in the EU without unjustified restrictions, promoting a single market for data services. It entered into force on 18 December 2018 and has been applicable since 28 May 2019.
Open Data Directive	This directive promotes the reuse of public sector information by setting standards for open data and transparency. The directive entered into force on 16 July 2019, replacing the Public Sector Information (PSI) Directive, and had to be transposed into national law by 17 July 2021.
Implementing Act High-Value Datasets (under the Open Data Directive)	This act regulates that public sector organisations must make specified high-value datasets available free of charge in machine-readable formats. It entered into force on 9 February 2023 and has been applicable since 9 June 2024.

There is also **mobility-specific EU data legislation** that aim to support digitalisation and data sharing in the mobility sector, such as the Intelligent Transport Systems (ITS) Directive and its delegated acts on real-time traffic information services (RTTI), multimodal travel information services (MMTIS), etc. The ITS Directive was established to facilitate the coordinated and coherent deployment and use of ITS in road transport and its connections to other modes of transportation. The delegated regulations provide detailed requirements for the availability and accessibility of data for specific purposes. Some of the use cases implemented under deployEMDS focus particularly on the availability of data for RTTI and MMTIS, hence the relevance of the two delegated regulations mentioned.

Below, we give an overview of European legislation relevant to the project. This overview does, however, not cover all the legislation that impacts data handling, access, and use in Europe. Each section concludes with a brief comment on the relevance of each piece of legislation to our project. These comments are concise, as the report aims to only provide an overview, and our analysis will continue.

3.2 Legislation for personal versus non-personal data

3.2.1 General Data Protection Regulation

This section delves into privacy and protection of personal data within the EU. The right to privacy and the right to protection of personal data are both enshrined in the Charter of Fundamental Rights of the EU (EU, 2000) and in the EU Treaties. The entry into force of the Lisbon Treaty in 2009 gave the Charter the same legal value as the Treaties and abolished the pillar structure, providing a stronger basis for a more effective and comprehensive EU data protection regime (Mildebrath, 2023).

Regulation (EU) 2016/679 – the **General Data Protection Regulation** (GDPR) (EU, 2016) – regulates the processing of personal data. The objectives of the GDPR are to strengthen the protection of the individual's right to personal data protection and to guarantee the free movement of such data within the EU (Article 1). It applies to EU organisations that collect, store or otherwise process personal data of individuals in the EU,

but also to organisations based outside the EU that offer goods or services to EU residents, monitor their behavior, or process their personal data. It is a single set of EU wide rules for data protection which protects individuals when their data is being processed by the private sector and most of the public sector.

The scope of the GDPR is **personal data**, which means any information that refers to an identified or identifiable natural person (Article 4). What is crucial is that the information on its own or in combination with other information can be linked to a living person. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. However, personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. But for data to be truly anonymised, the anonymisation must be irreversible. Typical personal data is a person's name, and address. However, the term is much wider and includes more types of data. Images and sound recordings of individuals that are processed by a computer can constitute personal data, even if no names are mentioned, if they relate to an identified or identifiable person. Various kinds of electronic identities, for example IP addresses and cookies, are also considered personal data if they can be linked to a natural person. The GDPR also applies in the case of mixed datasets comprised of both non-personal and personal data, even if personal data represents only a small part of the dataset.

All organisations that process personal data are either a data controller or a data processor. A **data controller** is any person or entity that determines the purposes and means of the processing. A data controller must ensure that the processing is carried out in accordance with all the provisions of GDPR. Where two or more controllers jointly determine the purposes and means of the processing, they are joint controllers and must decide together their respective responsibilities for compliance with the different obligations. A **data processor** is any person or entity that processes personal data on behalf of a data controller. Many of the obligations that apply to the data controller also apply to the data processor.

The GDPR states several fundamental **principles** that are at the core of the regulation, and which apply in the case of all processing of personal data (Article 5): Lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

These principles in brief mean that data controllers must have a lawful basis under the GDPR to process personal data; may only collect personal data for specific, explicitly stated, and legitimate purposes; and must not process more data than necessary for those purposes. They are responsible for ensuring the accuracy of the data, erasing it when no longer needed, and protecting it from unauthorised access, loss, or destruction. Additionally, they must be able to demonstrate how they live up to the GDPR.

Processing of personal data must be based on one of the six **lawful grounds**:

- Consent[62]: The data subject has consented to the personal data processing. Since consent is often not appropriate or feasible, there may be reasons to consider other lawful grounds for processing personal data first.
- Contract: The data subject has a contract or is to enter into a contract with the data controller.
- Weighing of interests: The data controller may process personal data if the data controller's interests outweigh those of the data subject and if the processing is necessary for the purpose in question.
- Legal obligation: There are laws and rules that oblige the data controller to process certain personal data in its activities.

[62] As set out in Article 4(11) of the GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

- Exercise of official authority or task in the public interest: The data controller must process personal data to carry out its duties as an authority or to carry out a task in the public interest.
- Fundamental interest: The data controller must process personal data to protect a data subject who cannot give their consent, for example if they are unconscious.

Companies, associations, and other organisations in the private sector will mainly use consent, contract, legal obligation, or weighing of interests as lawful grounds for processing of personal data. Authorities and others in the public sector will mainly use legal obligation, task in the public interest or exercise of official authority, or contract as lawful grounds for processing of personal data. Authorities may not use weighing of interests when they carry out their tasks.[63]

The principles and lawful grounds that apply to the primary use of data are **equally applicable to its reuse**.

Individuals' rights under the GDPR include:

- The right to be informed about the collection and use of their personal data.
- The right to data portability, allowing them to obtain and reuse their personal data for their own purposes across different services.
- The right to rectification of inaccurate or incomplete personal data.
- The right to erasure (right to be forgotten), allowing them to request deletion or removal of their personal data where there is no legitimate reason for its continued processing.
- The right to object to processing of their personal data in certain cases.
- The right to limitation of processing in certain cases.
- Rights related to automated decision-making and profiling.

Data protection by design and by default is a requirement for data controllers under the GDPR. In brief, data protection by design means that the data protection rules are already considered when designing IT systems and processes, and data protection by default that personal data is not processed unnecessarily as standard. Privacy-friendly techniques are encouraged, for example pseudonymisation and encryption. However, the implementation may vary depending on the individual case.

A **data protection officer** (a person responsible for data protection) must be designated by public authorities and by businesses that process data on a large scale, or whose core activity is the processing of special categories of data, such as health-related data.

The GDPR establishes a system of **independent supervisory authorities** in charge of monitoring and enforcing compliance. The EU countries have set up **national bodies** responsible for protecting personal data in accordance with Article 8(3) of the Charter of Fundamental Rights of the EU. In addition, the GDPR has established the European Data Protection Board (**EDPB**) as an independent European body which shall ensure the consistent application of data protection rules throughout the EU. The EDPB adopts guidelines covering key aspects of the GDPR. The EDPB is composed of the representatives of the national data protection authorities of the EU/EEA countries and of the European Data Protection Supervisor (**EDPS**). The European Commission participates in the activities and meetings of the Board without voting right.

Comments on the relevance of this legislation to the project:

- GDPR is perhaps the most fundamental regulatory framework to consider when sharing data because it sets strict rules for data protection within the EU. These rules apply to all organisations

[63] IMY (Swedish Authority for Privacy Protection), www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/lawful-grounds-for-personal-data-processing/.

that process 'personal data', which is broadly defined. Special categories of personal data are subject to stricter rules. The data subjects have various rights that must be ensured.

- In our project, urban mobility data is in focus. Mobility data are highly unique and regular. Unicity refers to the data of different individuals to be easily differentiable, particularly at some specific locations. The starting and ending locations of users' trajectories are often their home and work locations which are highly unique and can lead to reidentification. Studies show that user full trajectories can be uniquely recovered with the knowledge of only two locations. The regularity of trajectories means that for single individuals, their data follows periodic patterns. Namely, individuals tend to follow the same trajectories during workdays – home to work and back to home. Systematic mobility data of the Milan use case (home-to-work, home-to-school), for example, falls into this category. Ticket validation data that the Barcelona use case requires, could fall into this category.
- Mobility data can therefore contain elements that make it possible to directly or indirectly identify a person. For example, information about the time and location of a vehicle/object (which can be linked to a certain individual) – which the Milan use case includes – or even direct information about a traveller's identity. Mobility data may also contain other elements such as speed of travel. Speed of travel can, if it indicates a speeding violation (which is a criminal offence in several countries) and can be linked to a certain individual (for example, through a vehicle's registration number or other identifying information), be considered sensitive personal data and require special protection measures.
- The multimodality use cases in the project require careful consideration as even if the individual data does not lead to an identification of a person, the combination of data from multiple sources and their collective reading could entail such risk.
- The EDPB has noted that geolocation data warrant special attention as they are particularly revealing of one's life habits. The journeys carried out are very characteristic and can reveal private details about a person's life (e.g. residence, places of leisure, places of worship etc.). The relevant stakeholders therefore need to be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purposes of processing. The EDPB further mentions a number of principles that need to be complied with when collecting geolocation data. The Sofia use case, for example, requires GPS data of e-scooters, e-bikes, e-cars and public transport vehicles. The same applies for the Budapest use case.
- Real-time traffic data, including disruptions and alerts and planned events could also be personal data. This information is also typically provided by public authorities in real time, although it is common for service providers to offer real-time or aggregated traffic information obtained through crowdsourcing. Service providers that continuously monitor the location of their users (e.g., Google via Android phones), can obtain traffic information aggregating the speed, location, and density of their users, and enriching this data with publicly available information.
- In some instances, the use cases of the local implementation sites involve personal data (some examples mentioned above), which means that the rules and principles of the GDPR must be adhered to. Additionally, new use cases that potentially involve personal data may be introduced.
- Several examples of challenges related to data protection under GDPR are mentioned in Section 2.3.1.2 and Section 2.3.2.2. For example, the implementation sites have mentioned challenges in fulfilling certain requirements such as the right to data portability and the right to be informed.
- From a GDPR perspective an important part of the governance structure of a data space is the clear establishment of the roles of controllers/joint controllers and processors/sub-processors when processing personal data. But other aspects also need to be guaranteed, e.g., data subjects' rights.
- Another key consideration concerns to what extent consent can validly be used as a basis for data transactions in a data space, primarily regarding secondary uses of the data. For example, a passenger validating their ticket on the bus would have to be informed by the transport operator acting as controller for the purposes of processing their data. If that data is then used by a third party for their own purposes, the original consent cannot validly be relied upon for further processing.

- Enforcement issues also arise if the data space operates in more than one jurisdiction (such as the common EMDS), namely who will be the competent authority to monitor GDPR enforcement. The same applies for enforcement within the data space. The governance structure of the data space and the ensuing allocation of roles and responsibilities will also impact the body responsible for ensuring internal GDPR compliance.
- In a data spaces context, data is primarily meant to be used as a basis for commercial transactions. However, the EDPS has stressed that personal data cannot be considered a commodity subject to such transactions. The EDPB expressed similar considerations in light of the EC's Data Governance Act proposal, the first legislative instrument under the EC's 2020 European Data Strategy to epitomise the EC's vision for creating a single market for data. The Board stated that: "[..] considering that data protection is a fundamental right guaranteed by Article 8 of the Charter, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over personal data relating to them, the EDPB reiterates that personal data cannot be considered as a 'tradeable commodity'. An important consequence of this is that, even if the data subject can agree to the processing of his or her personal data, he or she cannot waive his or her fundamental rights. As a further consequence, the controller to whom consent has been provided by the data subject to the processing of her or his personal data is not entitled to 'exchange' or 'trade' personal data (as a so-called 'commodity') in a way that would result as not being in accordance with all applicable data protection principles and rules".
- In conclusion, rights and obligations relating to the processing of personal data can function both as an enabler and a barrier to data transactions. On the one hand, the general principles (e.g. transparency, data integrity, accountability) and the legal grounds for processing (e.g. consent), provided in the GDPR restrict data transactions involving personal data in the sense that they create a burden of compliance for the entity mainly responsible for data processing which they might not be able to adhere to. This could certainly be the case for data spaces, considering the EDPB comments, as participants are faced with a high threshold that must be attained when it comes to GDPR compliance. Public authorities that lack the private sector experience on navigating the GDPR and that are risk adverse may find that a deterring factor to joining a data space.
- On the other hand, certain individual rights in the GDPR could facilitate data transactions as they allow data subjects to retain some control over their data, thereby providing an incentive to enter into the transaction in the first place. But guaranteeing such rights in the data space context – when original data subjects may not be even aware of the secondary use of their data for the purposes of the data space, is an issue that requires further analysis and consideration.

3.2.2 Free Flow of Non-Personal Data Regulation

Regulation (EU) 2018/1807 (EU, 2018) – the **Free Flow of Non-Personal Data Regulation** – aims to ensure the free flow of non-personal data across the EU, meaning that such data can be stored and processed anywhere within the EU, regardless of where it was collected. This makes it easier for businesses to operate across the EU, as they can store and process their data wherever it is most convenient or cost-effective for them. So this regulation aims to ensure the free flow of non-personal data (Article 1). Data shall move freely, just like goods, capital, services, and labour.

The regulation applies to **non-personal data**, which is any information not linked to an identified or identifiable individual, i.e. any data other than personal data as defined in the GDPR (see Section 3.2). This can be, for example, data on weather conditions. It can also be data which was initially personal data but later anonymised. If datasets contain both personal and non-personal data and are inextricably linked, the GDPR applies to the entire set even if personal data is only a small part of the dataset. Also worth mentioning is that the distinction between personal data and non-personal data tends to become increasingly blurred with the widespread mixing and processing of different data sources using sophisticated algorithms that can make non-personal data personally identifiable or at least make it possible to identify specific social groups.

The regulation bans 'localisation requirements', which restrict data processing to specific EU territories, except for public security reasons. Previously, different EU countries had their own data storage and processing rules, sometimes requiring data to be stored and processed where it was collected. This made it difficult for businesses to operate across the EU, as they had to comply with different rules in each country.

The regulation entered into force on 18 December 2018 and applies from 28 May 2019. According to the regulation, EU countries must inform the Commission of any new data localisation requirements and by 30 May 2021, repeal any unjustified localisation requirements or notify the Commission if they consider them to be justified. EU countries must also establish a national online single information point containing all up-to-date localisation requirements and appoint a single contact point to liaise and cooperate with counterparts in other EU countries and the Commission, especially regarding assistance requests. Public authorities may request access to data located in another EU country, or stored or processed in the cloud, and required for their official duties.

The regulation also deals with supplier lock-in practices, ensuring that data can be easily transferred between cloud service providers or back to the company's IT system. Several providers have signed a code of conduct to ensure this.

Comments on the relevance of this legislation to the project:

- This regulation ensures that non-personal data can flow freely across borders within the EU, facilitating when mobility data needs to be shared and processed in different regions to optimise transport systems and mobility services.
- That this regulation allows non-personal data to be stored and processed anywhere within the EU, regardless of where it was collected, can make it easier and more cost-effective to manage data.
- The regulation also facilitates easier switching between cloud service providers, which can be beneficial for mobility data initiatives that rely on cloud infrastructure for data storage and processing.
- The regulation applies to non-personal data only, as personal data is governed by the GDPR. However, the GDPR also ensures free movement of personal data within the EU. Under the GDPR, EU Member States may neither restrict nor prohibit the free movement of personal data within the EU for reasons connected with the protection of natural persons with regard to the processing of personal data. The regulation for free flow of non-personal data establishes the same principle of free movement within the EU for non-personal data except when a restriction or a prohibition is justified by public security reasons. The regulations thus provide a coherent set of rules that cater for free movement of different types of data, and there is no obligation to store the different types of data separately. Thus, both non-personal data and personal data fall under the principle of free flow within the EU, promoting digital innovation and cross-border collaboration.
- Another thing is that different rules apply to personal data vs. non-personal data, and as already mentioned, the GDPR also applies to mixed datasets if these are inextricably linked. The distinction between "personal" and "non-personal" can have a negative impact when it comes to such datasets. Businesses may have difficulty categorising data as non-personal, thereby obliged to consider data as personal – even though they might not be – and apply the GDPR out of fear of non-compliance (given the threat of hefty fines) with all the obligations that flow from the GDPR for controllers and processors. In addition, the GDPR's definition of personal data is very broad and almost any data can potentially become personal data. This limits the application of the regulation on free flow. However, the application depends on the type of data involved in each case.
- Where the use cases of the local implementation sites in the project involve non-personal data, the Free Flow of Non-Personal Data Regulation can facilitate them in the above-mentioned ways.

3.3 Legislation on open data, INSPIRE data, ITS data and UMI data

This section explores the INSPIRE (Infrastructure for Spatial Information in the European Community), an infrastructure for spatial data in the EU, with the purpose of providing better access to public spatial data. It also explores the Open Data Directive and the specific high-value datasets that organisations within its scope must make available for free reuse in machine-readable formats and via APIs. Moreover, it describes the Intelligent Transport Systems (ITS) Directive, which promotes data availability of data types relevant to ITS services in road transport, e.g. travel planning and real-time traffic information services. Additionally, it includes a section on the TEN-T Regulation, which is the legal basis for Urban Mobility Indicators (UMI) and mandates the collection of UMI data covering each urban node.

3.3.1 INSPIRE Directive

Directive 2007/2/EC – the **INSPIRE Directive** (EU, 2007) – establishes an infrastructure for **spatial information** in Europe to support EU environmental policies and activities which may have an impact on the environment. Environmental issues require cooperation between countries, which is more successful when it is easy to share data across borders and organisations. Sharing spatial information can also lead to the development of new products and services. Each Member State has had to translate the directive into national legislation by 15 May 2009. Previously, spatial data was difficult to find online, poorly documented, and often incompatible. Many public authorities lacked online services for discovering, accessing, using and sharing spatial data (European Commission, 2016).

The directive aims to remove obstacles to the sharing of spatial data between all levels of government within and across EU countries. It applies to spatial data that cover areas where EU countries have jurisdictional rights, exist in electronic format, are held by or on behalf of a public authority or another body using the network, and relate to environmental information. EU countries are responsible for ensuring that metadata[64] are created for environmental spatial datasets and services listed in the legislation. It specifies common data models, code lists, map layers and metadata for 34 spatial data themes across three annexes. One of the data themes is **transport networks** (including road, rail, air and water transport networks and related infrastructure, links between different networks, and the trans-European transport network). The directive also defines implementing rules and technical guidelines for interoperability and accessibility of spatial datasets and services. It does not require the collection of new spatial data but seeks to harmonise existing data across Member States via internet services.

The European **INSPIRE Geoportal** is the central European access point to the data provided by EU member states and several EFTA countries under the INSPIRE Directive.

Comments on the relevance of this legislation to the project:

- The INSPIRE Directive facilitates public access to standardised spatial data throughout Europe. This increases the availability of such data, which can benefit various applications and services in the mobility field. In particular, data on transport networks, which are in the scope of this directive, could be useful for such applications and services.
- Datasets by theme ‘transport networks’ on the INSPIRE Geoportal include, for example, in the case of the road transport network, road network characteristic information such as the road’s functional

[64] Metadata usually refers to information that describes the content, availability and quality of datasets and services. In other words, metadata is data about data. It can help you understand if a dataset is what you are looking for and want to use.

class, road width, pavement information, level crossings, direction of traffic flow, road name and address information, road network usage restrictions (e.g., closed connection, turning restriction, weight, height, length and width restriction), and speed limits. Some deployEMDS implementation sites focus their use cases on similar data products (e.g., road infrastructure data and traffic rule data).

- The implementing act on high-value datasets (see Section 3.3.2) relies on the INSPIRE Directive in terms of the actual datasets and their modes of provision (data formats, metadata information, licensing, etc.) for the definition of high-value datasets in for instance the thematic category mobility.
- Kotsev et al. (2021) define a vision for the future development of INSPIRE as the public contribution to the emerging European common data spaces. (They mention especially the Green Deal Data Space, but the same holds for the EMDS. The Green Deal Data Space is one of the other sectoral data spaces relevant to the EMDS, as joint use cases can be searched for shared needs, datasets, key stakeholders, and ecosystems.) Kotsev et al. also highlight that spatial analyses can be used to support policy making in domains such as environment and transport.

3.3.2 Open Data Directive and High-Value Datasets

Directive (EU) 2019/1024 – the **Open Data Directive** (EU, 2019) – promotes reuse[65] of open data from public sector. The directive is based on the principle that public and publicly funded data should be reusable for commercial or non-commercial purposes. It entered into force on 16 July 2019, replacing the Public Sector Information (PSI) Directive (EU, 2003). It had to be transposed into national law by 17 July 2021.

This directive involves minimum harmonisation[66] and does not affect stricter regulations, which place higher demands on how the data must be made available (e.g. data format requirements). Such provisions can be found in the Commission's delegated regulations adopted within the framework of the ITS Directive (see Section 3.3.3). When implementing the directive, EU Member States may have chosen different approaches. Some may have reflected the requirements of the directive without going beyond it, while others may have introduced additional obligations for making data available for reuse. For example, Sweden has chosen the former approach (Swedish Government, 2021), whereas other countries may have opted for a different one.

Under this directive public-sector bodies[67] and public undertakings[68] must make their documents available in any pre-existing format or language and, where appropriate, by electronic means in formats that are open, machine readable, accessible, findable and reusable, complete with their metadata.

There are practical arrangements for reuse: Public-sector bodies must process requests for document reuse, electronically where appropriate, and make them available within a reasonable time. They must also facilitate online search and discovery of their documents. EU Member States must facilitate the effective reuse of documents, in particular by providing information on rights and offering assistance and guidance.

Dynamic and real-time data must be made available for reuse immediately on collection via an application programming interface (API) and, where relevant, as a bulk download.

---

[65] The term 'reuse' in this directive refers to the use, by individuals or legal bodies, of documents held by public-sector bodies or public undertakings.
[66] This means that EU Member States can impose stricter rules than required by the directive.
[67] Public-sector body: The state, regional or local authorities, bodies governed by public law or associations formed by such authorities, or bodies governed by public law.
[68] Public undertaking: Any undertaking over which public-sector bodies have a dominant influence through ownership, financial participation or the rules which govern it; these include those acting as public passenger road or rail transport operators, air carriers and EU shipowners fulfilling public-service obligations.

EU Member States must adopt policies and take action to make publicly funded research data openly available by default and support the dissemination of research data that are findable, accessible, interoperable and reusable (FAIR principles). They must consider intellectual property rights, personal data protection, confidentiality, security, and commercial interests, following the principle of 'as open as possible, as closed as necessary'. Publicly funded research data available via repositories can be reused for commercial and non-commercial purposes. Reuse conditions must be non-discriminatory. Reuse conditions must be non-discriminatory, and exclusive rights arrangements are generally prohibited. In specific cases where such arrangements are allowed, they are subject to regular review and transparency requirements.

There are datasets whose reuse are associated with significant socioeconomic benefits and should be made available under particularly friendly reuse conditions. The Open Data Directive therefore introduces the concept of **High-Value Datasets (HVDs)** and sets out six thematic categories of HVDs: geospatial, earth observation and environment, meteorological, statistics, companies and company ownership, and mobility (Article 13.1). New thematic categories may be added by the Commission by way of a delegated act.

As a result, the Commission Implementing Regulation (EU) 2023/138 of 21 December 2022 (European Commission, 2022c) lists specific HDVs and their publication and reuse arrangements, such as mobility (transport network). Public sector bodies must these HDVs available for reuse, free of charge, in machine-readable formats (via APIs and, where relevant, as bulk download). The regulation applies from 9 June 2024.

The mobility category includes datasets within the scope of the INSPIRE data theme "Transport networks" (as outlined in Annex I of Directive 2007/2/EC) and for some Member States (to which Directive 2005/44/EC applies) additional datasets related to inland waterways.

The directive does not apply to:

- documents for which third parties hold intellectual property rights;
- documents to which access is excluded or restricted by a national access regime, or on the grounds of sensitive critical infrastructure protection;
- documents whose supply falls outside the scope of the public task of a public-sector body or outside the scope of provision of services in the general interest of a public undertaking;
- documents held by public undertakings that are related to activities directly exposed to competition and therefore not subject to procurement rules under Article 34 of Directive 2014/25/EU;
- other documents referred to in Article 1(2) of the directive.

The above vacuum of applicability was remedied by the DGA (see Section 3.4.1), which mandates the reuse of certain categories of protected data held by public sector bodies.

Public authorities are only required to make existing data available, with no obligation to produce new data.

Comments on the relevance of this legislation to the project:

- In accordance with the Open Data Directive, publicly accessible data funded by the public sector should be reusable for commercial or non-commercial purposes. The Implementing Regulation on HVDs lists certain datasets that the public sector must make reusable as open data and free of charge, for instance data on transport networks. This increases the availability of such data for different applications in the mobility field.
- One key question, however, is how the ODD has been applied across Member States and whether there is a sufficient degree of harmonisation to allow consistent data sharing (as already mentioned in Section 2.3.1.2). How to deal with documents that contain personal data, IPRs or other confidential information is a key consideration for the public sector.
- Public undertakings were outside the scope of the PSI Directive but were included in the 2019 update. This change meant to capture undertakings in the utility sectors, including transport, as the Commission argued that data generated by these sectors have tremendous reuse potential. However, the Directive

does not contain a general obligation to allow the reuse of documents produced by public undertakings. The decision whether or not to authorise reuse should remain with the public undertaking concerned, except where otherwise required by the directive or by EU or national law (e.g., the ITS Directive). Only after the public undertaking has made a document available for reuse, should it observe the relevant obligations laid down in the Open Data Directive, in particular as regards format, charging, transparency, licences, non-discrimination and prohibition of exclusive arrangements. In the Impact Assessment accompanying the Open Data proposal, the Commission suggested that giving the freedom to public undertakings on whether they want to open up their data or not, would minimise the effect of imbalance (in terms of openness requirements) between the private companies and public undertakings in transport and utility domains active in the same markets.

- Although the directive applies only to reuse and in principle not the production and original use of the data, it lays down the obligation for Member States to encourage public sector bodies and public undertakings to produce and make available documents in accordance with the principle of 'open by design and by default', namely introducing the 'taste' of reuse as from the earliest stages of the production and first use of the data.
- The practical significance of this legislation for stakeholders included in this project requires further analysis as in principle, the ITS Directive has a broader scope than the Open Data Directive as it mandates accessibility of several travel and traffic data categories. It could also be considered as overriding the Open Data Directive as *lex specialis*. However, at the same time, it must be acknowledged that the Open Data Directive and the ITS Directive have different scopes: the former concerning open data and reuse while the latter targets accessibility of data. Therefore, the relationship between the two laws is not entirely clear. The terms used such as 'availability', 'accessibility' and 're-use' – that may seem like similar or complementary notions, but each have their own distinct meaning – may contribute to the confusion about what is in fact required under each legislation.

3.3.3 Intelligent Transport Systems (ITS) Directive

In this section, we delve into the legal framework for deploying intelligent transport systems (ITS) in road transport and their interfaces with other modes of transport.

Directive 2010/40/EU – the **ITS Directive** (EU, 2010) – was adopted on 7 July 2010 to accelerate the deployment of ITS services across Europe. The directive aims to establish interoperable and seamless ITS services while leaving Member States the freedom to decide which systems to invest in. The directive also aims to contribute to sustainable mobility. The aim is for users to become better informed and thus be able to use the transport network in a safer, more coordinated, and more efficient way.

Under the directive the Commission has adopted common European specifications (i.e. functional, technical, organisational or services provisions) to address the compatibility, interoperability, and continuity of ITS solutions across the EU. The first priorities were traffic and travel information, the eCall emergency system and intelligent truck parking, followed by real-time traffic information and multimodal travel information.

The directive promotes data availability of data types relevant to ITS services in road transport, e.g. travel planning and real-time traffic information services. EU Member States shall ensure that certain data is accessible via a National Access Point (**NAP**). NAPs must be established in all EU Member States.[69] These NAPs are a mechanism for accessing, exchanging, and reusing transport related data under the delegated

[69] This list shows the state of the art deployment of the NAPs across Europe, within the scope of the implementation of the delegated acts adopted under the ITS Directive (2010/40/EU): https://transport.ec.europa.eu/document/download/963c997d-efd9-40ae-a38b-5d4b935bdfcf_en?filename=its-national-access-points.pdf.

acts of the ITS Directive, in order to help support the provision of EU-wide interoperable travel and traffic services to end users.

A NAP can take various implementation forms, such as a database, data warehouse, data marketplace, repository, and register, web portal or similar depending on the data type concerned and provide discovery services, making it easier to fuse, crunch or analyse the requested datasets. For these purposes, data is accessible on a non-discriminatory basis, following necessary standards for exchange and reuse.

In 2021, a project started to work on a better adaptation of the implementation of EU specifications in the Member States – the NAPCORE project[70]. NAPCORE acts as a coordination mechanism to improve the interoperability of NAPs in Europe through harmonisation and alignment of mobility data standards. Also, NAPCORE aims at increasing access to and expanding availability of mobility related data by coordinated data access and better harmonisation of the European NAPs.

However, the ITS Directive from 2010 and the delegated acts only require actors to share and exchange data to the extent that they have these in machine-readable format. The requirements have not included that data must be produced if it does not already exist. This is about to change.

Directive (EU) 2023/2661 (EU, 2023a), amending the ITS Directive, was adopted on 22 November 2023, with the aim to adapt to new road mobility options, mobility apps and connected and automated mobility. The new directive mandates that certain crucial road, travel and traffic data, such as speed limits, traffic circulation plans, and roadworks, be available in digital format. It also ensures that essential safety-related services are made available for drivers along the TEN-T network. Additionally, it also strengthens cooperation between Member States in implementing ITS.

The directive also imposes authorities to align with relevant stakeholders. These stakeholders can be identified as partners of union supported projects.

The Commission has adopted **delegated acts** to further detail the provisions of the directive:

- Commission Delegated Regulation (EU) No 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an **interoperable EU-wide eCall**. (This regulation is currently under review.)
- Commission Delegated Regulation (EU) No 885/2013 of 15 May 2013 supplementing ITS Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of **information services for safe and secure parking places for trucks and commercial vehicles**.
- Commission Delegated Regulation (EU) No 886/2013 of 15 May 2013 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to data and procedures for the provision, where possible, of **road safety-related minimum universal traffic information free of charge to users**.
- Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 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**. (This regulation is repealed from 1 January 2025.)
- 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**.

[70] NAPCORE is a Programme Support Action co-funded by the EU under the Connecting Europe Facility. More information about NAPCORE can be found at its website: https://napcore.eu/ and at the European Commission's website https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/road/action-plan-and-directive/national-access-points_e.

- 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**. (This regulation applies from 1 January 2025.)

We describe some of these regulations below. For the deployEMDS use cases, the regulations on real-time traffic information services (RTTI) and multimodal travel information services (MMTIS) are most relevant.

Regulation (EU) 2022/670 is a new regulation on RTTI replacing the old regulation (EU) 2015/962 from 1 January 2025. The difference is mainly that new data types, more actors, and a larger road network is covered by the new regulation. Conditions for access, exchange, update, and reuse of data have also been modified. In addition to this, there are also requirements for the Member States to cooperate on additional or alternative standards and minimum requirements for quality.

The new regulation applies to the entire road network that is publicly accessible to motorised traffic. By way of exception, it shall not apply to private roads, unless they are part of the comprehensive TEN-T network or designated as a motorway or as a primary road. However, for a transitional period ending on 31 December 2027, obligations regarding some of the data types shall not apply with respect to roads other than the comprehensive trans-European road network, motorways, and primary roads.

The requirements to provide data and services under the regulation apply to various actors as follows:

- Road authorities, road operators, tolling operators and recharging and refuelling-related stakeholders shall provide data on infrastructure.
- Road authorities, road operators and tolling operators shall provide data on regulations and restrictions.
- Road authorities, road operators, holders of in-vehicle generated data and service providers shall provide data on the state of the network.
- Road authorities, road operators, service providers, holders of in-vehicle generated data, and recharging and refuelling-related stakeholders shall provide data on the real-time use of the network.

The data types set out in the Annex of the new RTTI regulation include, for instance, data on the infrastructure (e.g., data on road network links and their physical attributes, and data on road classification), static and dynamic traffic regulations (e.g., speed limits), data on the state of the network (e.g., roadworks, accidents and incidents, and weather conditions affecting road surface and visibility), data on the real-time use of the network (e.g., traffic volume, traffic speed, location and length of traffic queues, and travel times).

The regulation sets out a number of reference data exchange standards like DATEX II and TN-ITS. Other machine-readable formats are acceptable if compatible with the refence data exchanges standards.

Regulation (EU) 2017/1926 on MMTIS has been in place since 2017, but it has been recently revised. The regulation establishes the necessary specifications to ensure that EU-wide multimodal travel information services are accurate and available across borders to ITS users. It is applicable to the entire transport network of the EU and requires that data holders, such as transport operators, transport authorities, infrastructure managers and transport-on-demand service providers, make information (such as timetables, bike-sharing stations, stations and bus stops) accessible via NAPs in each Member State. The purpose is to enable data users, such as providers of multimodal travel information services, to make accurate information available to passengers, enabling smoother multimodal travel. The obligation to make data available only applies when it is already available in a digital, machine-readable format. On 29 November 2023, the Commission adopted a new delegated regulation – (EU) 2024/490 – amending the delegated regulation 2017/1926. The revised delegated regulation makes it mandatory for data holders to make dynamic information (real-time data such as disruptions) available through the NAPs. Previously, only certain static data had to be accessible. The obligation also extends to new data, for example on whether bicycles can be taken onto a train, and on accessibility, including for passengers with disabilities or reduced mobility (this aligns the delegated regulation with the regulations on EU passenger rights). Passengers will also be able

to find, through travel information services, real-time information on delays or cancellation of planes, ferries, or transport-on-demand, and where to park their bike, scooter or car (European Commission 2023b).

Regulation (EU) 886/2013 is a regulation on road safety-related minimum universal traffic information (SRTI) that was enacted in May 2013 to supplement the ITS Directive and has been in force since then. The regulation establishes the specifications necessary to ensure compatibility, interoperability and continuity for the deployment and operational use of data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users. The geographical scope of the regulation is the trans-European road network. Public and private road operators and/or service providers shall set up or use the means to detect events or identify conditions and shall collect the relevant road safety-related traffic data. The deployment of these means shall comply with the conditions and requirements set out in national law. Public and/or private road operators and/or service providers shall share and exchange the data they collect in certain format via a NAP. The data shall be accessible for exchange and reuse by any user on a non-discriminatory basis, within the EU, in accordance with certain access rights and procedures, within a timeframe that ensures the timely provision of the information service, through the NAP. Public and private road operators and service providers shall ensure the timely renewal and quality of data made available through their access point.

The list of road safety-related events or conditions and information content covered by the regulation include, for instance, data on temporary slippery road; data on animal, people, obstacles, or debris on the road; data on unprotected accident areas; data on short-term road works; and data on exceptional weather conditions.

The delegated regulations are binding in their entirety and directly applicable in all Member States from their date of application, without the need for implementation in national legislation. However, national legislation may still be required to supplement the regulations and support their effective application. For instance, national legislation can designate responsible authorities (a national body or competent authority that assesses whether the requirements of the delegated regulations are fulfilled), establish necessary administrative structures, and define enforcement procedures. Additionally, national legislation can create incentives for stakeholders to adhere to the delegated regulations.

Comments on the relevance of this legislation to the project:

- The ITS Directive, and its delegated acts, are highly relevant to mobility data spaces, particularly because they require certain road, travel, and traffic data to be made available in digital format. This enhances the accessibility and shareability of such data, supporting better decision-making and innovation in the mobility sector. The data can be utilised by various applications, such as multimodal travel planners and navigation services.
- For our project, the delegated acts on RTTI and MMTIS are especially relevant, as some of the implementation use cases focus specifically on the availability of such data. For example, some use cases involve RTTI-related data, such as data on road infrastructure, traffic regulations, incidents, and roadworks. Some use cases involve MMTIS-related data, such as public transport data regarding timetables, stops, occupancy, etc., and mobility services data, such as data on car or bike sharing stations.
- The recent revision of the MMTIS steps in the right direction towards increasing the availability of dynamic data. But it remains to be seen whether its mandates will be sufficient to enable the deployment of multimodal services, or additional datasets must be included in its scope in the future.
- Moreover, by establishing common European specifications to ensure that ITS data is accessible, standardised, and shareable across different platforms, interoperability between systems is ensured, which also benefits mobility data spaces.
- Additionally, the NAPs will be an important component of the future EMDS, ensuring that transport-related data are accessible and can be shared effectively. Several of the deployEMDS use cases focus on making data sources needed to meet the requirements of the updated ITS Directive

available to NAPs. Actors responsible for three NAPs are involved in the project: Fintraffic (responsible for the Finnish NAP), Trafikverket (responsible for the Swedish NAP), and BASt (responsible for the German NAP). Fintraffic and Trafikverket are actively engaged in the local implementations in Tampere and Stockholm, respectively. BASt follows the progress of the project as an associated partner to ensure the connection to NAPCORE and co-organises workshops on European governance of mobility data. This active engagement not only demonstrates the initiative that NAPs can take in the digital transformation towards data spaces but also highlights the convergence of different mobility stakeholders within these data spaces.

3.3.4 TEN-T Regulation and UMI data

Regulation (EU) 2024/1679 – the **TEN-T Regulation** (EU, 2024b), revised in 2024, defines the trans-European transport network (TEN-T) and sets out the requirements for the infrastructure to ensure a coherent quality throughout the EU. The infrastructure of the trans-European transport network consists of infrastructure for railway transport, inland waterway transport, maritime transport, road transport, air transport and multimodal transport, including in urban nodes. The network consists of three layers: the core network (the most important connections between mayor cities and nodes), the extended core network, and the comprehensive network. There are different deadlines for completing the different layers: the core network by 2030, the extended core network by 2040, and the comprehensive network by 2050.

The purpose of the infrastructure requirements is twofold: to ensure that transport infrastructure users can count on an efficient, reliable and high-performing infrastructure, and to ensure the development of more sustainable forms of transport.

The revised TEN-T Regulation emphasises the importance of urban nodes[71], which are key urban areas along the TEN-T network. By 31 December 2027, all 431 urban nodes must adopt and monitor Sustainable Urban Mobility Plans (SUMPs)[72]. These plans should include measures to integrate different transport modes and shift towards sustainable mobility, promote efficient zero or low-emission mobility, reduce air and noise pollution, and assess transport accessibility. Member States will be required to collect urban mobility data per urban node in the fields of sustainability, safety and accessibility, with a view to improve the performance of the trans-European transport network (Article 41, paragraph 1 b).

The Commission shall adopt an implementing act by 19 July 2025 to define the indicators to be used for data collection and to establish a methodology for the collection and submission of data, as well as to set deadlines (between three and five years) for the submission of such data. The implementing act shall be prepared in close cooperation with the Member States and their regional and local authorities. In doing so, the availability and accessibility of data at local level, as well as existing urban mobility plans, shall be taken into consideration (Article 41, paragraph 2).

Comments on the relevance of this legislation to the project:

- The TEN-T Regulation requires that major cities along the TEN-T network develop SUMPs to promote zero and low-emission mobility and that Urban Mobility Indicators (UMI), formerly known as

[71] An ‘urban node’ is an urban area where elements of the transport infrastructure of the trans-European transport network for passengers and freight, such as ports, including passenger terminals, airports, railway stations, bus terminals and multimodal freight terminals, located in and around the urban area are connected with other elements of that infrastructure and with the infrastructure for regional and local traffic, including infrastructure for active modes (Article 3).

[72] A ‘SUMP’ is a document for strategic mobility planning, aiming at improving, in a sustainable way, accessibility to and mobility within the functional urban area, including commuting zones in that urban area or in its vicinity), for people, businesses and goods in view in particular of a better quality of life (Article 3).

Sustainable Urban Mobility Indicators (SUMI), are collected per urban node. These indicators are used to assess and improve urban transportation systems (evaluate mobility performance and identify areas for improvement).

- Effective governance will be crucial for successful UMI collection (EGUM, 2024). Member States are the primary recipients of the collection requirement, but they need to engage in dialogues with local and regional authorities to define responsibilities for data collection and aggregation. In turn local and regional authorities may need to involve private stakeholders on data transmission and collaboration. Member States can also make use of existing structures such as the NAPs under the ITS Directive (EGUM, 2024).
- The cities involved in the project are urban nodes, and within the regions involved there are also urban nodes. Several of the deployEMDS use cases focus on facilitating the availability, sharing and reuse of data for UMI indicators.

3.4 Legislation promoting data sharing: Data Governance Act and Data Act

This section covers two legal instruments that encourage data sharing within the EU: the Data Governance Act and the Data Act. While the former regulates processes and structures to facilitate voluntary data sharing, the latter clarifies who can create value from data and under which conditions. Together, these two acts aim to facilitate reliable and secure access to data, fostering its use in key economic sectors and areas of public interest.

3.4.1 Data Governance Act

Regulation (EU) 2022/868 – the **Data Governance Act** (DGA) (EU, 2022a) – creates processes and structures to facilitate data sharing between companies, individuals, and the public sector, across sectors and Member States. It entered into force on 23 June 2022 and applies from 24 September 2023.

The DGA **aims to** make more data available for reuse and facilitate data sharing across areas such as health, environment, energy, mobility, manufacturing, and public administration for the benefit of EU citizens and businesses. Moreover, the DGA aims to increase trust in voluntary data sharing, improve data availability, and address technical barriers. It regulates neutral data intermediaries, which can facilitate data exchanges, and mandates the Commission to establish the European Data Innovation Board (EDIB), which will develop guidelines and identify standards for cross-sectoral data sharing.

The DGA contains conditions for **reusing certain protected data held by public sector bodies**. They hold vast amounts of data protected by third-party rights (such as trade secrets, personal data, or intellectual property) that cannot be used as open data but that could be reused under specific EU or national rules. Whenever such reuse is allowed, public sector bodies must comply with the reuse conditions laid down by the DGA. Notably, the reuse conditions should be non-discriminatory, transparent, proportionate, justified and made publicly available. A reuser intending to **transfer protected, non-personal data to a non-EU country** must comply with specific rules in the DGA. **Fees** for reuse should be transparent, proportionate, non-discriminatory, and objectively justified. Public sector bodies granting reuse permits can apply reduced or zero fees, for example, for SMEs, start-ups, civil society organisations and educational establishments. To ensure that **data can be found** ('findability'), the Member States must ensure that all relevant information

on conditions for reuse and on charges is available and easily accessible through a **single information point**. The Commission will, in turn, collate this information at the official portal for European data[73].

The DGA regulates providers of **data intermediation services**. These are neutral third parties that connect individuals and companies that hold data with others that want to use data. The requirements for such services aim to ensure that such data intermediaries will function as trustworthy organisers of data sharing. To increase trust in data sharing, this approach lays down a model based on the neutrality and transparency of data intermediaries while putting individuals and companies in control of their data. Entities wishing to provide data intermediation services must: comply with strict requirements to ensure neutrality and avoid conflicts of interest; have structural separation from any other value-added services provided; have price terms independent of whether a potential data holder or data user is using other services; and register with a competent authority. Once registered, the data intermediary can legally start to operate and use the label "data intermediation services provider recognised in the Union" in its communication, as well as a common logo. The Commission keeps a central register of recognised data intermediaries.

The DGA also has a framework for **data altruism** (the sharing of data voluntarily and for no reward). Data altruism is when individuals and companies give their consent or permission to make data that they generate available for use in the public interest, voluntarily and without reward. Such data have the potential to advance research and develop better products and services. EU Member States may develop national policies to encourage data altruism and an entity engaged in data altruism can apply to be registered as a "data altruism organisation recognised in the Union" and use a common logo designed for this purpose. These entities must have a not-for-profit character and meet transparency requirements as well as offer specific safeguards to protect the rights and interests of citizens and companies who share their data. The Commission maintains an EU-level register of these organisations, for information purposes.

As provided in the DGA, the Commission has established the **European Data Innovation Board (EDIB)** to facilitate the sharing of best practices, in particular on data intermediation, data altruism and the use of public data that cannot be made available as open data, as well as on the prioritisation of cross-sectoral interoperability standards. The EDIB includes representatives of national authorities designated under the DGA (Member State competent authorities for data intermediation and for data altruism), the European Commission, the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the European Union Agency for Cybersecurity (ENISA), the EU SME Envoy, and other relevant bodies with specific expertise. According to Article 30, the EDIB is tasked with **developing guidelines** to support the consistent application of the DGA across the EU. These guidelines should cover several key areas, for example guidelines for common European data spaces. The guidelines shall address, among other things: (i) cross-sectoral standards for data sharing; (ii) requirements to counter barriers to market entry and avoiding lock-in effects for the purpose of ensuring fair competition and interoperability; (iii) adequate protection for lawful data transfers to third countries; (iv) adequate and non-discriminatory representation of relevant stakeholders in the governance of common European data spaces; and (v) adherence to cybersecurity requirements in accordance with Union law.

Regarding **international data flows**, the DGA introduces safeguards to protect such data from unlawful access by non-EU countries' authorities.

Comments on the relevance of this legislation to the project:

- The DGA is a piece of legislation that is relevant for our project since it aims to make more data available and facilitate data sharing across sectors and EU countries. The DGA brings several innovations to facilitate sharing and reuse of data:

[73] The official portal for European data: https://data.europa.eu/.

- It expands the legal framework for the reuse of certain public sector data, allowing sensitive data like personal and commercially confidential information, excluded from the scope of the Open Data Directive, to be made available with specific safeguards (Graux, 2024a).
- Moreover, the DGA establishes a legal framework for data intermediation services, enabling specialised service providers to facilitate controlled data sharing (which can help gain access to data that data holders might be less willing or interested in sharing directly).
- It also introduces the notion of data altruism, which allows data sharing decisions to be made by the data subjects.

- All this creates new opportunities for different actors interested in accessing, sharing and reusing data. This increased availability of data can benefit many data spaces and ecosystems.
- However, there is still some uncertainty about the precise implementation of data intermediation services with regard to their application in data spaces, but the DSSC is developing a building block which may clarify this (PrepDSpace4Mobility, 2023).
- Furthermore, the DGA supports the establishment of common European data spaces. It establishes the EDIB and tasks the EDIB with developing guidelines for such data spaces.

3.4.2 Data Act

Regulation (EU) 2023/2854 – the **Data Act** (DA) (EU, 2023b) – is the second main legislative initiative resulting from the European Strategy for Data (the DGA was the first). It entered into force on 11 January 2024 and will be applicable from 12 September 2025, except for certain provisions that will be implemented at a later date. The DA is a cross-sectoral piece of legislation, i.e., it lays out principles and guidelines that apply to all sectors. It does not change existing data access obligations, however any forthcoming legislation should align with its principles.

The DA **aims to** ensure a fair distribution of the value of data among actors in the data economy, stimulate a competitive data market, create opportunities for data-driven innovation and make data more accessible to all. It is a regulation on harmonised rules on fair access to and use of data. Through the DA, the EU seeks to remove barriers to access data, for both private and public sector bodies, while preserving incentives to invest in data generation by ensuring a balanced control over the data for its creators.

Notably, the DA sets out rules that **enable users of connected products to access the data generated** by these devices and also to share such data with third parties. These rules provide individuals and businesses with the right to access the data produced through their utilisation of smart objects, machines, and devices (whether they own, lease or rent such a product). They may choose to share this data with third parties. This will enable aftermarket (e.g. repair) service providers to enhance and innovate their services, fostering fair competition with similar services provided by manufacturers. Consequently, users of connected products have the option to choose more cost-effective repair and maintenance providers (or undertake these tasks themselves), leading to potentially lower prices in the market. This can also extend the lifespan of connected products, thus contributing to the European Green Deal[74] objectives.

This does not mean that companies lose control over the data generated by their products. The ability of manufacturers to use data of objects they manufacture is not affected. Furthermore, the third party selected by the user compensates the manufacturer for the costs of granting access, i.e., of technical arrangements to make the data available (such as APIs). Safeguards provided for in the regulation prevent situations where the data is used in any manner that would have a negative impact on the manufacturer's business opportunities. This includes using it to develop a product or related service that would compete with the

[74] The European Green Deal is a package of policy initiatives, which aims to set the EU on the path to a green transition, with the goal of reaching climate neutrality by 2050.

original data-generating product, or where the data is used by parties without an appropriate basis for the use, through the appropriate technical protection measures.

How does the **DA relate to the GDPR**? Unlike the GDPR, which is limited to personal data, the DA applies to both personal and non-personal data, which means that its scope is broader. However, the DA clarifies that it is "without prejudice" to the GDPR, which include the powers and competences of supervisory authorities and the rights of data subjects. Therefore, when personal data is generated from connected products or related services, the requirements of both the DA and the GDPR must be met. In case of conflicts the GDPR will take precedence over the DA, see Article 1 (5), recital 7 sentence 5 of the DA. In fact, much of the data generated by individual users is personal data. For example, the data generated by smart vehicles, IoT devices and other consumer goods can usually be attributed to an identifiable person, making them personal data. They are therefore subject to the GDPR. Where the user is not the data subject whose data is being requested, personal data can only be made available if there is a valid legal basis (e.g. consent). The data generated may also consist of both personal and non-personal data which may be difficult to separate. Furthermore, the DA builds on GDPR, in particular concerning the right to data portability. Under the GDPR, this right, which allows data subjects to move their data between controllers offering competing services, is limited to personal data processed on certain legal bases and where technically feasible, but the DA enhances this right for connected products so that consumers can access and port any data generated by the product, both personal and non-personal data.

The DA also sets out general rules relating to the obligations to make data available which either stem from horizontal regulations or vertical interventions. Under the DA, any data made available must abide by the following **obligations**: (i) share data under fair, reasonable and non-discriminatory ('FRAND') terms and (ii) provide for reasonable compensation. These obligations apply only to legally mandated data access or sharing requirements in B2B relationships.

Furthermore, the DA establishes rules **enabling public sector bodies to access and use data held by the private sector** in situations where there is an exceptional need for data, such as floods or wildfires. Private companies are obliged to provide certain data under key conditions (which businesses can enforce in case of abuse). If the data is necessary to address a public emergency, it must be provided for free. In other situations – to prevent or recover from a public emergency, or to fulfil a public-interest mandate imposed by law – the data holder may request compensation.

Additionally, the DA protects businesses from **unfair contractual terms** in data sharing agreements, ensuring a level playing field for SMEs in the data market. These rules cover all data, both personal and non-personal, held by a private entity that is accessed and used based on a contract between businesses. The DA establishes a non-exhaustive list of terms that are always considered unfair as well as terms that are presumed to be unfair. If a contract term is considered unfair, it is no longer valid. If possible, it is simply removed from the contract. If it is presumed to be unfair, the company that imposed the term can try to show that the term is not unfair.

The DA contains essential **interoperability requirements** to allow data to flow within and between data spaces. It also includes rules to ensure interoperability between data processing services. The inter-operability requirements for data space participants (that offer data or data services to other participants) includes making descriptions of data structures, data formats, and vocabularies publicly accessible and ensuring the interoperability of data-sharing agreements, such as through smart contracts. The DA promotes the interoperability of data processing services via harmonised standards and open specifications. It also sets requirements for vendors of smart contracts to ensure that automated data-sharing agreements are executed correctly and resist third-party manipulation. The Commission will identify interoperability barriers and prioritise standardisation needs, potentially requesting European standardisation organisations to draft harmonised standards. If these efforts fall short, the Commission can adopt common specifications, developed in an open and inclusive way, considering feedback from the EDIB (recital 103 of the DA).

The DA also reviews certain aspects of the Database Directive, which was created in the 1990s to protect investments in the structured presentation of data. It clarifies that the directive cannot be used to prevent access to data generated by a connected product or related service. Otherwise, data holders could in practice claim exclusivity over data generated by connected products, which, if left unaddressed, would hinder the effective application of data access and portability rights under the DA.

Comments on the relevance of this legislation to the project:

- The DA will contribute to more data being available, especially data collected or produced from connected devices. It allows users of these devices to access and even forward data that was previously usually only available to the manufacturer. Thus, the DA increases the possibility for different stakeholders in the mobility sector to access relevant mobility data generated by connected products and related services, such as connected vehicles or connected traffic infrastructure, and use it to develop applications and services. The DA also enables public sector bodies to access and use data held by the private sector in certain situations. In these ways, the DA can foster innovation in the mobility sector. Sharing data with public authorities in cases of public interest (based on an exceptional need) can impact traffic management, urban planning, and environmental regulations, enabling more informed decision-making based on accurate, real-time mobility data (PrepDSpace4-Mobility, 2023).
- The DA further specifies the essential requirements for interoperability of data, mechanisms, and services for data sharing and for common European data spaces to ensure that (mobility) data can be shared between different systems and platforms, which is relevant for the integration of data from different stakeholders in the mobility sector.
- As a result of the DA's provisions on data access, use, and interoperability, it is expected to contribute to more data being available, also for and within data spaces and ecosystems.
- Nevertheless, many of its provisions rely on being implemented by contractual negotiations, so the ongoing Commission work to provide model contractual terms is crucial in this regard.

3.5 Platform regulations: Digital Markets Act and Digital Services Act

The EU has introduced the Digital Markets Act (DMA) and the Digital Services Act (DSA) to address specific players in the digital economy. The DMA focuses on regulating dominant players, particularly those designated as 'gatekeepers' (large online platforms). The DSA addresses online services' transparency, accountability, and regulatory oversight. These acts are part of the EU's broader effort to create a safer digital environment where the fundamental rights of users are protected and to establish a level playing field for businesses.

3.5.1 Digital Markets Act

Regulation (EU) 2022/1925 – the **Digital Markets Act** (DMA) (EU, 2022b) – aims at ensuring fair competition and market access in the digital economy. It establishes rules for large online platforms, designated as 'gatekeepers', to cultivate fairer and more competitive digital markets in the EU. The goal is to create a more level playing field for SMEs and start-ups, support innovation, and protect users' interests.

The DMA came into force on 1 November 2022. Gatekeepers have six months from their designation to comply with the obligations.

Under the DMA, a 'gatekeeper' is a large digital platform providing any of a pre-defined set of digital services ('core platform services'), such as online search engines, app stores, and messenger services, which have a significant impact on the internal market, act as an important gateway for a large number of businesses to

reach large user base, and hold an entrenched position in the market. Platforms meeting specific size and influence thresholds may be designated as gatekeepers.

Gatekeepers must comply with obligations to maintain a fair and open digital market, including preventing self-preferencing practices (where a gatekeeper unfairly prioritises its own services to the detriment of competitors), providing data portability, and ensuring interoperability functions, particularly for messaging services, to reduce dependency on gatekeepers. The DMA also prohibits unfair practices, such as blocking users from uninstalling pre-installed software or applications, or restricting businesses from offering their goods and services through alternative platforms at different prices or conditions. The DMA aims to limit the ability of gatekeepers to exploit their dominant market position at the expense of competitors, users, or business partners.

The Commission oversees compliance with the DMA and can impose significant fines for non-compliance. In severe cases, non-financial remedies, such as divestiture, may be imposed.

The DMA represents a shift from reactive competition enforcement to proactive regulation of influential players in the digital economy, aiming to foster innovation, improve consumer choice, and create a fairer and more open digital environment in the EU.

Comments on the relevance of this legislation to the project: The DMA can indirectly influence mobility data spaces by regulating gatekeepers and preventing anti-competitive behaviour that might otherwise hinder data sharing in the mobility sector. The DMA's focus on data portability and interoperability, alongside its obligations for gatekeepers to grant business users access to the data they generate through their use of the gatekeeper's platform, can enhance companies' access to data, to the extent these are held by gatekeepers. This improved access has the potential to support data-sharing practices within a mobility data space, namely when it comes to important datasets held by such important actors, facilitating innovation and collaboration in the mobility sector.

3.5.2 Digital Services Act

Regulation (EU) 2022/2065 – the **Digital Services Act** (DSA) (EU, 2022c) – aims to create a safer and more transparent online environment in the EU. It sets comprehensive rules for online intermediaries and platforms, for example, online marketplaces, social networks, content sharing platforms, app stores, and online travel and accommodation platforms, to address illegal content, enhance accountability, and protect users' fundamental rights. The goal is to foster a safer and innovative digital space.

The DSA entered into force in November 2022. Platforms designated as very large online platforms and search engines (VLOPs and VLOSEs) have 4 months from designation to comply with DSA rules, which includes the publication of a risk assessment. All regulated entities must comply with the DSA by 17 February 2024.

Under DSA, different types of digital service providers are subject to specific obligations depending on their role, size, and impact on the digital ecosystem. These include Intermediary services, Hosting services, Online platforms, and very large online platforms and search engines (VLOPs and VLOSEs). The obligations vary based on the scale and nature of the service, with stricter requirements applying to VLOPs and VLOSEs due to their significant impact on public discourse and the online economy. Key obligations include countering illegal goods, services or content online, enhanced transparency, and safeguarding users' rights. Platforms must implement mechanisms to put in place measures to counter the spreading of illegal goods, services or content online, such as mechanisms for users to flag such content and for platforms to cooperate with "trusted flaggers", and to provide clear and transparent information on content moderation and personalised content.

The Commission and Member states will oversee compliance with the DSA. The Commission can impose significant fines for non-compliance, with penalties of up to 6 per cent of the company's total worldwide turnover. Severe cases may lead to temporary suspension of the service.

Comments on the relevance of this legislation to the project: The DSA can indirectly influence mobility data spaces by enhancing transparency and accountability for the platforms within scope that may be used in mobility services. It establishes rules for online platforms aimed at creating a safer and more trustworthy digital environment, which is crucial for mobility solutions where digital interaction and data sharing are central.

3.6 Interoperable Europe Act

Regulation (EU) 2024/903 – the **Interoperable Europe Act** (EU, 2024a) – aims to enhance the interoperability of public services across EU Member States, facilitating cross-border data exchange and accelerating public sector digital transformation. It supports the objectives of the Digital Decade, such as having 100 per cent of key public services available online by 2030. This includes services that require cross-border exchange of data, such as:

- mutual recognition of academic diplomas or professional qualifications;
- digital driving licenses and exchanges of vehicle data for road safety;
- access to social security and health data;
- the exchange of information related to taxation and customs;
- public tender accreditation; and
- commercial registers.

The act establishes a governance framework led by the **Interoperable Europe Board** and mandates interoperability assessments for public sector bodies. It introduces the **Interoperable Europe Portal** for related information and support. The Commission provides tools and trainings, such as the EIF toolbox, the SEMIC Support Centre, the JoinUp platform, and the Interoperable Europe Academy. The GovTech Incubator initiative helps governments adopt solutions developed by startups and other governments.

The act affects public authorities as well as businesses and citizens using trans-European digital public services. It entered into force on 12 July 2024. Mandatory interoperability assessments and measures by national authorities had to be implemented by 12 January 2025. Non-compliance may result in administrative sanctions and corrective actions.

Comments on the relevance of this legislation to the project: The Interoperable Europe Act promotes data sharing and collaboration across borders. It provides increased opportunities for open data initiatives and is likely to facilitate data spaces as well. The act creates a framework to facilitate interoperability between Member States' public administrations and promotes the development of digital public services across borders through common rules and governance. It enables easier access to and sharing of public sector data across borders. This act and the EMDS share a common vision of promoting interoperability, cooperation and innovation in order to avoid fragmentation and break down data silos (PrepDSpace4Mobility, 2023). In Section 3.9.3, we discuss the intersection between this act and the ITS Directive, a directive very relevant to our project and the EMDS, concluding that the Interoperable Europe Act can support the implementation of the objectives of the ITS Directive and contribute to the deployment and use of EU-wide ITS.

3.7 Artificial Intelligence Act

Regulation (EU) 2024/1689 – the **Artificial Intelligence Act** (AI Act) (EU, 2024c) – establishes a legal framework for the development and use of AI in the EU. This law defines what constitutes an AI system and which risk category it belongs to, along with the requirements that must be met before the system can be

placed on the market in Europe. The aim is to ensure a high level of protection from harmful effects of AI systems in the EU, while supporting innovation and improving the functioning of the internal market.

The AI Act was proposed by the Commission[75] in April 2021 and agreed by the European Parliament and the Council in December 2023. It was formally adopted by Parliament in its March 2024 plenary session (with a corrigendum issued in April 2024) and the Council endorsed the final text in May 2024. It entered into force on 1 August 2024. The application of the AI Act will be staged over two years, starting with the phasing out of the prohibited systems within six months after the act enters into force, and will require the European Commission to issue implementing and delegated acts and guidelines.

The AI Act assigns applications of AI to different **risk categories**, with different degrees of regulation applying. Risk is defined as "the combination of the probability of an occurrence of harm and the severity of that harm". AI systems that create an unacceptable risk are banned. These include manipulative AI, social scoring systems, biometric identification systems (limited exemptions for law enforcement purposes may apply under strict conditions) and emotion recognition in workplace and educational institutions (other than for medical or safety reasons). High-risk applications (applications that can have a detrimental impact on people's health, safety or on their fundamental rights)[76] are subject to specific requirements, including implementation of appropriate technical and organisational measures, human oversight, exercise of control, monitoring, keeping automatically generated logs and assessing impact on fundamental rights. Applications not explicitly banned or listed as high-risk are largely left unregulated. AI systems posing limited risks because of their lack of transparency will be subject to information and transparency requirements.

Under the AI Act, general purpose AI (GPAI) models are regulated separately from AI systems. GPAI models are also classified depending on their risk.

The AI Act imposes obligations throughout the entire value chain – from providers, importers and distributors to deployers of AI solutions within the EU, as well as persons adversely impacted by the use of an AI system placed on the market or put into service in the EU. A deployer is "any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity".

Before placing a **high-risk AI system** on the EU market or otherwise putting it into service, providers must subject it to a conformity assessment and demonstrate that their system complies with the mandatory requirements for trustworthy AI (e.g., data quality, documentation and traceability, transparency, human oversight, accuracy, cybersecurity and robustness). The assessment must be repeated if the system or its purpose are substantially modified. Providers of high-risk AI systems will also have to implement quality and risk management systems to ensure their compliance with the new requirements and minimise risks for users and affected persons, even after a product is placed on the market.

Under the AI Act, the European Commission will establish the **European AI Office** to develop EU expertise and capabilities in the field of AI. The AI Act also establishes a European Artificial Intelligence Board (**EAIB**)

[75] Proposal for a Regulation laying down harmonised rules on AI (AI Act) (COM(2021) 206 final.
[76] Together with a definition of "high-risk", the AI Act sets out a methodology to help identifying high-risk AI systems. The risk classification is based on the intended purpose of the AI system, in line with the existing EU product safety legislation. This means that the classification of the risk depends on the function performed by the AI system and on the specific purpose and modalities for which the system is used. Annexed to the act is also list of use cases which are considered to be high-risk, which the Commission will update over time. One example on this list, which might be relevant for our project, is critical infrastructure in the field of road traffic. Systems on the high-risk list, that perform narrow procedural tasks, improve the result of previous human activities, do not influence human decisions or do purely preparatory tasks are not considered high-risk. However, an AI system shall always be considered high-risk if it performs profiling of natural persons.

composed of one representative per Member State. The European Data Protection Supervisor (EDPS) will participate as observer and the AI Office will also attend without taking part in the votes. The EAIB will advise and assist the Commission and the Member States to facilitate the consistent and effective application of the AI Act. Moreover, the AI Act establishes an **advisory forum** to advise and provide technical expertise to the EAIB and the Commission to contribute to their tasks under the AI Act. The membership of the advisory forum shall represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society, and academia. The Commission will also establish a **scientific panel** of independent experts to support the enforcement activities under the AI Act. Each Member State must establish or designate at least one notifying authority and one market surveillance authority. In addition, the Commission will set up an **EU database** for certain high-risk AI systems.

The AI Act is a horizontal legal framework, which means that its requirements should apply across all sectors. However, the **horizontal nature** of the act requires full consistency with existing EU legislation applicable to sectors where high-risk AI systems are already used or likely to be used in the near future. As regards high-risk AI systems which are safety components of products, the rules will be integrated into the existing sectoral safety legislation to ensure consistency, avoid duplications, and minimise additional burdens. As regards high-risk AI systems related to products covered by the New Legislative Framework (NLF) legislation (e.g. machinery, medical devices, toys), the requirements for AI systems will be checked as part of the existing conformity assessment procedures under the relevant NLF legislation. The applicability of the requirements of the AI Act should thus not affect the specific logic, methodology or general structure of conformity assessment under the relevant specific NLF legislation. As regards high-risk AI systems related to products covered by relevant Old Approach legislation (e.g. aviation, cars), the AI Act will not directly apply. However, the ex-ante essential requirements for high-risk AI systems set out in the regulation will have to be considered when adopting relevant implementing or delegated legislation under those acts.

Under the AI Act, an '**AI system**' means "a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". This definition determines if a system is within the scope of the AI Act. The definition is not intended to cover simpler traditional software systems or programming approaches, and the Commission has been tasked to develop guidelines on its application.

The AI Act applies primarily to providers and deployers putting AI systems into service or placing on the EU market and who have their place of establishment or who are located in the EU, as well as to deployers or providers of AI systems established in a third country when the output produced by their systems is used in the EU.

The AI Act asks EU Member States to set up **regulatory sandboxes** and allows testing high-risk AI systems in real-world to facilitate the development, training, testing and validation of innovative AI systems.

Comments on the relevance of this legislation to the project:

- The AI Act deals with AI systems but is relevant to mobility data spaces in several ways:
    - AI enhances the accessibility and reuse of mobility data, creating new information and services when trained with representative, non-biased datasets. The EMDS and AI reinforce each other, with the EMDS facilitating data sharing and AI enabling effective data utilisation (European Commission, 2023a).
    - To the extent that AI is developed or used within a mobility data space, the AI Act provides a framework that needs to be followed, especially for high-risk AI systems, to ensure that AI is trustworthy, safe, and developed and used in accordance with fundamental rights obligations.

- In addition, regulatory sandboxes create opportunities to test and validate AI applications in real-world scenarios, supporting innovation while aligning with the broader goals of efficiency and sustainability for data spaces.
- Developers of AI applications can benefit from data spaces, as data spaces can make more data available for access and reuse, providing AI applications with datasets they need in order to learn and make accurate predictions. Interoperable data spaces will also make it easier to integrate and analyse data from different sources in AI applications. AI-based solutions in the mobility sector, such as AI for predictive awareness in road traffic safety contexts, need access to various types of mobility data, which mobility data spaces and the EMDS can facilitate.

- The AI Act sets out certain requirements, such as specific data quality requirements for high-risk AI systems in Article 10, which data spaces must ensure their datasets meet if they are to be used in such systems. Training, validation and testing datasets for such systems shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete "in view of the intended purpose". In policy lab workshops in the project, we have discussed the emphasis on the intended purpose and the challenges around it. Assessing whether a dataset is fit for one's own intended purpose is one thing; assessing the level required for external purposes can be much more challenging. Two relevant questions are: How do we ensure that data from an external source is fit for an internal purpose? And how do we ensure that data from an internal source is fit for an external purpose? We discussed how standards might help us (see Section 2.4.5 for more on this in relation to the data life cycle, but the discussion will continue in upcoming workshops). One question, however, is to what extent actors will be willing to make extra efforts to ensure data quality for an external purpose with the data. Ensuring data quality for external purposes (beyond the actor's immediate scope or organisation) can enhance collaboration and benefit the broader community, but may require additional resources and effort, which could be challenging without clear incentives. As mentioned in Section 2.3, many organisations struggle with capacity limitations for data management.
- It is currently unclear to us to what extent data in deployEMDS will be used for AI systems where the AI Act places specific requirements, e.g., on data quality.

3.8 Additional relevant legislation

In addition to the above-mentioned laws and regulations and how they affect access to and sharing of data, some additional areas of legislation that may need to be considered are also briefly mentioned below (without providing an exhaustive list of relevant laws and regulations). We place less focus on this legislation in this report, as we will analyse it in more detail within the framework of later project activities.

3.8.1 Competition law

A relevant area of law is EU **competition law** and its application to data management practices. The unique nature of the data market presents new challenges (data.europa, 2023).

Information exchange is a common feature of many competitive markets and can bring efficiencies by addressing information asymmetries, informing decisions, benchmarking against best practices, and developing improved products or services, ultimately benefiting consumers. However, a key principle of competition law is that businesses must act independently in the market to ensure better outcomes for consumers, typically resulting in greater choice and lower prices. While this does not prevent companies from adapting to the behaviour of their competitors, it does prevent direct or indirect contact between them (through agreement, concerted practice, or decision by an association of companies) that affects the commercial strategy of companies (Herbert Smith Freehills, 2024).

EU competition law has been used to tackle anti-competitive data management practices. Two provisions have been particularly important for tackling anti-competitive practices in the data market. The first bans anti-competitive agreements that could affect trade between Member States and "which have as their object or effect the prevention, restriction or distortion of competition within the internal market" (Article 101 of the Treaty on the Functioning of the European Union, TFEU). The second prohibits any abuse of dominant position within the internal market (Article 102 TFEU). Also relevant to consider are the European Commission's guidelines on the applicability of Article 101 TFEU on horizontal cooperation agreements (European Commission, 2023c). These guidelines contain a chapter on information exchange that provides guidance on key concepts and the assessment of commercially sensitive information. Additionally, the horizontal block exemption regulations exempt certain research and development and specialisation agreements that meet the conditions of these regulations from Article 101(1) of the TFEU.

The EU competition law has been developed with case law. However, the unique nature of the data market presents new challenges, and case law on competition in the data economy is limited. Based on previous cases like Microsoft (T-201/04) and Huawei (C-170/13), Article 102 TFEU is interpreted on a case-by-case basis for questions including, for example, recognition of a dominant position or market distortion in a non-traditional marketplace such as the data economy (data.europa, 2023; Graux, 2022). How to define dominance (including the determination of relevant markets) in data sharing contexts is still an open question (PrepDSpace4Mobility, 2023; Bayamlioğlu et al., 2022).

Comments on the relevance of this legislation to the project: Data sharing arrangements can often be pro-competitive, but in some cases they may be anti-competitive (Lundqvist, 2018). This would be particularly the case when data sharing results in situations that infringe Article 101 TFEU, namely information exchange or anticompetitive agreements, including through the use of an intermediary/third party. Competition law may also be relevant in data sharing where exclusive data control may give rise to significant market power for a limited number of market participants. It is also relevant if a dominant company only allows data sharing under unequal or discriminatory conditions, or if it abuses its dominant position to ensure its control over potential competitors. Mobility data spaces, as well as the future EMDS, aims to bring together mobility actors to share data, but their competitive relationships may raise questions about appropriate governance structures for cooperation, and competition law may prohibit the sharing of certain data with specific entities or mandate cooperation and data sharing, depending on the circumstances (PrepDSpace4Mobility, 2023). In that respect, competition law compliance must be a key aspect for data space participants. For deployEMDS, participants should particularly be aware of whether there are actual or potential competitors who will take part in their data space and whether any data exchange will involve data that are considered highly risky to induce competition law implications.

3.8.2 Intellectual property law

Another relevant area of law to consider in relation to data is **intellectual property (IP) law**. IP law can confer rights over data, often through copyright and the sui generis database right. Data may also be protected by trade secrets (confidential business information), which constitute a separate legal regime (often referred to as quasi-IP).

Copyright law protects creative works such as text, images, video and sound. It also protects software (e.g. source code) and databases (e.g. a collection of independent data that is protected). Databases can also be protected by the sui generis database right in addition to copyright.

Directive 96/9/EC – the EU's **Database Directive** (EU, 1996) – seeks to provide legal protection for databases, regardless of whether they reach the level of originality or not. The directive has two main aspects of protection:

- copyright protection for the intellectual creation involved in the selection and arrangement of materials;

- sui generis protection for a substantial investment (financial and in terms of human resources, effort and energy) in obtaining, verifying or presenting the contents of a database.

A database[77] will be protected by copyright if the selection or arrangement of its contents constitute the creator's own intellectual creation. The creator enjoys a group of exclusive rights (restricted acts), such as reproduction, alteration, distribution, etc. The legitimate user of a database may carry out the restricted acts that are necessary for using the database, subject to certain restrictions. The sui generis right is a property right similar to but distinct from copyright. It exists to recognise the substantial investment that is made in obtaining, verification or presentation of the contents of a database, even when this does not involve the creative aspect that is reflected by copyright. It allows the database maker to prevent unauthorised extraction and/or reuse of substantial parts of those contents. The duration of copyright protection is usually the lifetime of the author plus 70 years, while the duration of sui generis protection is shorter and lasts 15 years from the completion of the creation of the database.

However, the creation of a database from data that falls within the scope of the Data Act (described in Section 3.4.2) cannot be protected by the sui generis right under the Database Directive. This is clarified in the Data Act (Article 43). Thus, the Database Directive cannot be used to prevent access to data obtained from or generated by a connected product or related service falling within the scope of the Data Act.

Trade secret protection coexists with IP rights for confidentiality and competitive advantage. The EU rules on protecting trade secrets can be found in the Trade Secrets Directive, Directive (EU) 2016/943[78], which aims to harmonise national laws in EU countries on the protection against the unlawful acquisition, disclosure and use of trade secrets. It is intended to have a deterrent effect against the illegal acquisition, use and disclosure of trade secrets, without undermining fundamental rights and freedoms.

Hence, this directive is relevant for various data types that require confidentiality and commercial value. It provides protection against certain unlawful conduct and helps support the development of secure data sharing practices.

Comments on the relevance of this legislation to the project: Data spaces must consider IP rights to address various issues such as rights allocation (who "owns" the data and how are rights distributed among participants), protection (safeguards against unauthorised use or breaches), licensing (terms under which the data can be used by other participants), and commercialisation (how data can be monetised or used for economic gain). Understanding and respecting IP rights in data spaces is important because it creates a trusted environment that encourages parties to share their privately owned data. When participants are confident that their IP rights will be respected and protected, they are more likely to share their data. Additionally, the protection of trade secrets plays a role in safeguarding confidential business information. By maintaining the confidentiality of valuable information, companies can preserve their competitive advantage.

3.8.3 Contract law

Contract law deals with the interpretation and enforcement of agreements between two or more parties, such agreements for the exchange of goods or services. It is essential in business transactions and other agreements to ensure that promises made are legally enforceable.

[77] Database is defined as a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.
[78] DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

There is no harmonised contract law at the EU level, so national contract law must be considered for agreements within the EU. Contracts are typically subject to the laws of the country in which they were created, and many contracts contain a governing law clause to specify which laws will apply in the event of a dispute.

There is ongoing work by the Commission to develop model contractual terms and standard contractual terms for B2B data sharing contracts. This can facilitate for data spaces by providing a common legal framework that parties can adopt.

The Data Space Support Centre's (DSSC) blueprint for data spaces contains a contractual framework building block, which provides an overview of the most common agreements that support the establishment and functioning of a data space (e.g., a constitutive agreement and general terms and conditions, as well as agreements related to data transactions), see Section 2.4.6.

Comments on the relevance of this legislation to the project: Contract law is an important area of law for the governance of data spaces. It provides the framework for creating legally binding agreements between the dataspace participants, defining the terms under which data is shared and used within a dataspace, determining the rights and obligations of the participants, the parties' responsibilities in the event of a breach of contract, and the remedies available to the injured party. Contracts can thus foster a secure and collaborative environment for data sharing and innovation by establishing rights and responsibilities among the participants, promoting accountability and trust. The agreements may also contain clauses to ensure that shared data is handled in accordance with applicable laws and regulations. Contract law also contains mechanisms for resolving disputes that may arise between parties. Therefore, contract law plays a significant role in the functioning of data spaces.

3.8.4 The ePrivacy Directive

Directive 2002/58/EC – the **ePrivacy Directive** (EU, 2002) – focuses on ensuring the privacy in the electronic communication sector across the EU. The ePrivacy Directive was first adopted in 2002 and has since been updated to reflect changes in technology and communication practices.

The directive covers for example confidentiality of communications, processing of traffic and location data, unsolicited commercial communications and the use of cookies and similar technologies for storing information, and accessing information stored, on a user's equipment such as their computer or mobile, requiring clear user information and consent before deployment, except when strictly necessary for the service. Providers of publicly available electronic communications services are also obliged to provide security of services, and to inform the subscribers whenever there is a particular risk, such as a virus or other malware attack.

Enforcement is carried out at the national level by Data Protection Authorities and telecommunications regulators in each Member State, resulting in penalties that vary across countries.

Efforts are underway to replace the directive with an ePrivacy Regulation, aiming to harmonise rules across Member States further and align with technological developments. A proposal was published by the Commission in 2017, but it is still under negotiation. The proposal aims to ensure a level playing field for companies and its purposes include enhancing security and confidentiality of communications (including content and metadata), and defining clearer rules on tracking technologies such as cookies as well as on spam. This proposed regulation seeks to expand and modernise privacy protections, ensuring consistency with GDPR while addressing emerging privacy challenges.

Comments on the relevance of this legislation to the project: The ePrivacy Directive is relevant for mobility data spaces as it regulates privacy within electronic communications services. It ensures the confidentiality of communications and requires clear user information and consent before deployment of

cookies. By governing cookies and tracking technologies, it influences how user data can be collected and utilised in a data space. These rules could enhance trust in data-sharing practices by safeguarding user privacy and ensuring transparency. Together with GDPR, the ePrivacy Directive provides a robust legal framework for secure and privacy-compliant data sharing in a data space.

3.8.5 The eIDAS Regulation

Regulation (EU) 910/2014 – the **Electronic Identification and Trust Services (eIDAS) Regulation** (EU, 2014) – provides a framework for secure and trustworthy digital identity and authentication. It targets electronic identification (eID) and trust service providers. First adopted in 2014 and effective since 2016, it supports cross-border eID recognition. The eIDAS Regulation provides for the interoperability of national eID schemes among the Member States. With eIDAS, the aim is to lay down a foundation and a legal framework for people, companies and public administrations to safely access services and carry out transactions online. The regulation also sets requirements for so-called Qualified Trust Service Providers (QTSPs).

In 2021, the Commission proposed a new regulation establishing a framework for a European Digital Identity, amending the eIDAS regulation, which addresses the shortcomings of eIDAS by improving the effectiveness of the current framework for digital Identity and extending its benefits to the private sector. The aim is to promote acceptance of digital identities throughout the EU. Therefore, the Member States shall provide European Digital Identity Wallets (EU DI Wallets) to citizens by 24 December 2026. Five Implementing Acts laying down the rules for the core functionalities and certification of EU DI Wallets entered into force on 24 December 2024.

Comments on the relevance of this legislation to the project: The regulation is relevant for mobility data spaces as it sets up a framework for secure and trusted electronic identification and data exchanges across borders. By providing a legal framework for digital identity, the regulation facilitates interoperability and legal certainty for digital transactions within a data space. It also supports seamless cross-border interactions by enabling recognition of national eIDs, fostering trust and collaboration among stakeholders.

3.8.6 NIS2 Directive

Directive 2022/2555, also known as **NIS2** (EU, 2022d), replaced its predecessor, Directive 2016/1148 or NIS1, in January 2023. The NIS2 Directive is the EU's comprehensive legislation on cybersecurity. NIS2 updates and strengthens the 2016 rules to address the challenges of increased digitisation and evolving cyber threats. By broadening the scope to include more sectors and entities, NIS2 enhances the resilience and incident response capacities of both public and private entities across the EU.

NIS2 requires the EU Member States to strengthen their cybersecurity preparedness by establishing a competent authority, and a national Computer Security Incident Response Team (CSIRT). It also fosters cooperation by creating a Cooperation Group to facilitate the strategic exchange of information and collaboration among Member States, enhancing the EU's collective security posture.

The directive promotes a culture of security across critical sectors and that heavily depend on ICT systems, including energy, transport, water, banking, healthcare, and digital infrastructure. Businesses classified as operators of essential services in these sectors must adopt appropriate security measures and notify serious incidents to relevant authorities. Key digital service providers, such as cloud computing services, search engines, and online marketplaces, are also subject to security and reporting requirements.

Comments on the relevance of this legislation to the project: By providing legal measures to boost the overall level of cybersecurity in the EU the directive is relevant for mobility data spaces. The directive's emphasis on cooperation among Member States enhances the security of cross-border data exchanges within mobility data spaces. Businesses classified as operators of essential services within the relevant sectors, including transport (air, rail, water and road), must comply with the requirements in the directive.

3.9 Intersection between cross-sectoral and sector-specific data legislation

This section explores the intersection between cross-sectoral data legislation, such as the Data Governance Act (DGA), the Data Act (DA), the Interoperable Europe Act, and the Artificial Intelligence Act (AI Act), and its impact on sector-specific legislation on mobility data, mainly the Intelligent Transport Systems (ITS) Directive and its delegated acts. As we will demonstrate, the cross-sectoral data legislation can have various impacts on the sector-specific legislation on mobility.

3.9.1 The Data Governance Act and the ITS Directive

The ITS Directive (see Section 3.3.3 for details) is intended to promote the use of intelligent transport systems (ITS) in road transport and for interfaces with other modes of transport. It establishes the framework for the coordinated and coherent introduction and use of ITS and lays down the conditions for their implementation. The ITS Directive provides for the availability and accessibility of e.g. travel and traffic data as well as real-time traffic information at National Access Points (NAPs).

The DGA (see Section 3.4.1 for details) sets out the legal framework for the reuse of certain categories of protected data held by public bodies. However, it is not intended to create an obligation to allow the reuse of data held by public sector bodies, but only to regulate the conditions for the reuse of the data. Moreover, this regulation should complement and be without prejudice to more specific obligations on public sector bodies to allow reuse of data laid down in sector-specific Union or national law. The data in certain categories of data, such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data, in public databases are insufficiently used and often not even made available, although such availability is possible under the applicable Union law, in particular Regulation (EU) 2016/679, Directive 2002/58/EC and Directive (EU) 2016/680. The reason for this is extensive technical and legal procedural requirements that must be met to protect the data. The DGA now provides a legal framework for this, setting out standardised conditions for access to and use of this data throughout the EU.

The DGA thus provides improved conditions for the access to new categories of data that were previously unavailable. This can increase the amount of data available and promotes the development of innovative services and applications in the field of ITS based on this data by facilitating data access. Improved conditions for access to public data can enable companies and research institutions to develop new mobility services and transport solutions. This could promote the use of ITS by supporting innovative services such as improved traffic management systems, real-time information services for drivers or traffic management solutions.

The DGA facilitates the provision of certain categories of protected data by setting out the conditions for their reuse and thus facilitates the implementation of the ITS Directive. The DGA does not overrule the applicable reuse conditions under the delegated regulations of the ITS Directive, but complements them with regard to certain categories of protected data held by public sector bodies. The DGA thus supports the provision and use of further data necessary for the deployment and use of ITS.

Furthermore, the provisions of the DGA for data intermediation services facilitate the implementation of the ITS Directive and the delegated regulations. Data intermediation services act as trusted intermediaries that can assist data holders in fulfilling their obligation to provide data under the ITS Directive and its delegated regulations. This is particularly useful for the provision of personal data. If data holders provide personal data, personal data is processed and the GDPR is applicable (Article 2(a) GDPR). This means that the requirements of the GDPR apply to the processing. In order to avoid these requirements, it seems useful in practice to exclude personal reference from the beginning by anonymising the data. Anonymisation can

change data in such a way that the identification of persons is excluded and the data does not show any personal reference. Without personal reference, the data is not personal, so the GDPR does not apply. The data is anonymised when the content of a dataset is retained, but the statement can no longer be assigned to a specific or identifiable person (Ernst, 2021). The requirements for anonymising data are therefore high and require specific technical knowledge and infrastructure (Martini & Roeingh, 2024). In addition, there is the problem that the data formats differ due to the large number of different data types to be provided that require different anonymisation procedures to maintain the specific characteristics of the data and can lead to inconsistencies in the data and thus complicate data analysis (Martini & Roeingh, 2024). The DGA provides a solution to this with its requirements for data intermediation services (Martini & Roeingh, 2024). Under Article 12(e) DGA, data intermediation services may include offering additional specific tools and services for data holders or data subjects that are specifically designed to facilitate data sharing. This includes the anonymisation of data, but also other services.

3.9.2 The Data Act and the ITS Directive

The DA (see Section 3.4.2 for details) is intended to create a harmonised legal framework for the use of product data and data from connected services in order to reduce barriers to data sharing and data reuse (European Commission, 2024). Therefore, the DA regulates the access and use of data from connected products or related services and contains data access rights for various parties. It also provides a horizontal framework for B2B relationships, setting out requirements concerning the contractual content of data sharing agreements when EU or national law imposes data sharing obligations.

The ITS Directive aims to promote the deployment and use of ITS in the EU. An essential prerequisite for ITS is data. The ITS Directive and its delegated regulations require the availability and accessibility of a wide range of different mobility data, such as multimodal travel information and real-time traffic information, provided through a NAP.

The DA and the ITS Directive thus both aim to promote data access and data sharing and contain data provision obligations in order to achieve this. This leads to the question of the relation between the data provision obligations of the legal acts. According to Article 44(1) DA the specific obligations for the making available of data between businesses, between businesses and consumers, and on exceptional basis between businesses and public bodies, in Union legal acts that entered into force on or before 11 January 2024, and delegated or implementing acts pursuant thereto, shall remain unaffected. Thus, the data provision obligations under the delegated regulations of the ITS Directive remain unaffected.

The DA applies to data generated by connected products[79] or related services. Connected vehicles use their extensive sensor technology to generate a wide range of data about their surroundings, as well as data about the driving process and the vehicle itself. The vehicle also exchanges information with other vehicles (V2V) and the infrastructure (V2X) via interfaces in the vehicle. Connected vehicles can therefore be considered connected products under the DA. Also connected infrastructure applications, such as dynamic traffic lights or dynamic road signs that generate data and exchange it with connected vehicles, can be considered connected products. In the context of the revised ITS Directive, the data generated by connected vehicles and infrastructure can form an interface between the DA and the ITS Directive and its delegated regulations. The revised ITS Directive now also covers connected vehicles and infrastructure and provides for the deployment and use of ITS services for cooperative, connected and automated mobility. Therefore,

[79] A connected product is an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user (Article 2, point 5, of the DA).

specifications and standards for linking vehicles with the transport infrastructure, raising awareness and enabling highly automated mobility services shall be adopted (Annex I 4.). This involves the definition of necessary measures to further progress the development and implementation of cooperative (vehicle-vehicle, vehicle-infrastructure, infrastructure-infrastructure) intelligent transport systems (Annex I 4.1). These measures should promote the availability of the relevant data or information to be exchanged to the respective vehicle or road infrastructure parties (Annex I 4.1.2.).

The DA gives users of connected products access rights to the data generated by the connected product (Article 3(1) DA, Article 4(1) DA). In addition, the user may request that the data holder makes the data accessible to a third party (Article 5(1) DA). The DA could under certain circumstances provide the right to access vehicle data and data from connected infrastructure for NAPs as third parties. In principle, NAPs could be considered as third parties within the meaning of Article 5(1) DA (Martini & Roeingh, 2024). However, this would require an agreement with the user for each dataset and a request from the user to the data holder to provide the data to the NAPs, which is challenging to implement in practice (Martini & Roeingh, 2024). In some cases, the NAPs are operated by public sector bodies. The DA also gives public sector bodies a right of access to the data if there is an exceptional need. However, this is only to be assumed in certain situations defined in the DA and will rarely be the case. Regardless of whether the NAPs have a right of access to data, the DA can expand the amount of available data that can be used for the development and use of ITS services for cooperative, connected and automated mobility in the EU.

In addition, the essential requirements for the interoperability of data, mechanisms and services for data sharing, as well as common European data spaces, impact the implementation of the ITS Directive. The DA defines essential requirements that must be met by participants in data spaces that offer data or data services to other participants. Compliance with these requirements should ensure the interoperability of data, of mechanisms and services for data sharing and of common European data spaces. NAPs can under certain circumstances be such data sharing services. By defining the essential requirements, the DA would promote the interoperability of the NAPs and facilitate their integration into the EMDS.

Finally, a question could arise whether the rules imposed for B2B data sharing when prescribed by EU or national law, i.e. the requirement to share data under FRAND terms and provide reasonable compensation contradicts the existing regime of data sharing through the NAPs under the ITS Directive. Nevertheless, Art. 50(4) clarifies that these requirements for data sharing only apply to provision obligations in law that enters into force after the date of application of the DA (12 September 2015). Data provision obligations that arise before this date are therefore in principle not covered. Both the ITS Directive and the updated MMTIS Regulation are already in force and thus fall outside the scope of these provisions.

Even if the ITS Directive must be transposed by 21 December 2025 and some of the MMTIS Regulation obligations have different timeframes, ranging from 1 December 2025 to December 2028 – thus after the date of application of the DA – this is irrelevant. Art. 50(4) clearly refers to the entry into force of the law mandating to make data available as the test for the obligations to apply.

But even if that was not the case, there are good arguments suggesting that the obligations under the ITS Directive and the delegated acts fall outside the scope of this DA provision. Article 8 refers explicitly to business-to-business relations, suggesting this covers direct relationships. Furthermore, it necessitates a ‘data holder’ being obliged to make data available to a ‘data recipient’. A ‘data recipient’ is defined as “a natural or legal person, acting for purposes which are related to that person’s trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law”. Even if the NAP could lato sensu be considered a ‘data recipient’, the ITS Directive and the delegated acts do not mandate data availability, but data accessibility.

3.9.3 The Interoperable Europe Act and the ITS Directive

The Interoperable Europe Act (see Section 3.6 for details) aims to promote the cross-border interoperability of trans-European digital public services. This is intended to facilitate the cross-border flow of data for trans-European digital public services, with the intention of strengthening the internal market (recital 1 of the Act). With regard to the mobility sector, the Interoperable Europe Act can particularly support the implementation of the objectives of the ITS Directive. The ITS Directive was introduced to promote the coordinated and coherent introduction and use of intelligent transport systems. To this end, the delegated regulations under the ITS Directive set out obligations to provide various data required for the development and operation of ITS. The provision of ITS applications often does not stop at national borders. Especially in border regions, the use of data from different Member States is needed for the optimal development and use of ITS applications. Through various tools, the Interoperable Europe Act promotes the cross-border interoperability of trans-European digital services and facilitates the cross-border exchange of data. The Interoperable Europe Act can thus make a significant contribution to the deployment and use of EU-wide ITS.

3.9.4 The AI Act and the ITS Directive

The development of AI systems requires larges amount of data, especially AI systems that use techniques in which models are trained with data. In addition to the DGA and the DA as cross-sectoral legislation on data, the ITS Directive also promotes data access and data sharing in the mobility sector. If this data is used as training, validation and testing datasets for the development of high-risk AI systems, it must meet the quality criteria of Article 10(2)-(5) of the AI Act to ensure that the high-risk AI system functions as intended and safely and does not become a cause of discrimination. (See Section 3.7 for details on the AI Act.)

The use of AI in ITS forms an interface between the AI Act and the ITS Directive. One example of the use of AI in intelligent transport systems is AI-based functions in traffic information services. Traffic information services use information and communication technology to provide users with real-time traffic information. Traffic information services thus use information and communication technologies in road traffic, making them intelligent transport systems as defined in Article 4, point 1, of the ITS Directive. Google Maps is an online mapping website that, in addition to navigation functions, also contains traffic information. Google Maps provides AI-based information on speed limits (Shashidharan, 2023). The AI system is trained with various data. One important source of this data is data on speed limits provided by public authorities (Shashidharan, 2023). According to the Delegated Regulation (EU) 2022/670, data on speed limits must be provided pursuant to Annex 2 (a) (iv) of the Delegated Regulation (EU) 2022/670. If the AI system used in the ITS is considered a high-risk AI system, it must meet the requirements for such systems.

3.10 Summary and conclusions of Chapter 3

In this chapter, we have examined the legal landscape and the opportunities and limitations of legislation on data access and sharing in the mobility sector.

Most of the data-related legislation applicable in EU Member States is influenced or directly determined by European legislation from the EU. For instance, in the area of data protection, the legal situation in the Member States is primarily governed by EU legislation. When the EU's **General Data Protection Regulation** (GDPR) became applicable on 25 May 2018, it superseded all EU Member States' data protection laws based on the previous 1995 Data Protection Directive. The GDPR is still the most prominent piece of legislation in the data domain, setting strict rules for data protection in the EU, but the regulatory focus is shifting towards facilitating data sharing and reuse for socio-economic benefits, making the GDPR part of a broader, evolving framework for data in Europe. The GDPR also ensures free movement of personal data within the EU. The **Free Flow of Non-Personal Data Regulation** establishes the same principle of free movement within the EU for non-personal data, promoting digital innovation and cross-border collaboration. There are instances in the use cases of the local implementation sites where personal data is involved.

Challenges that the sites are experiencing include ensuring data subjects rights under GDPR. For data spaces handling personal data, establishing clear roles for GDPR roles is important.

With a view to creating a solid data-driven economy, the EU has enacted several legal acts in recent years as part of the establishment of a genuine single EU market for data, where data can flow across countries and sectors and be easily accessed and used, while respecting European values and rules. For instance, the **Data Governance Act** (DGA) and the **Data Act** (DA) have been introduced to promote access and trust in data sharing. The DGA regulates processes and structures to facilitate voluntary data sharing, while the DA clarifies who can create value from data and under which conditions. The increased data availability and facilitation of data sharing benefits data spaces and ecosystems. The DGA also supports the creation of common European data spaces and establishes the European Data Innovation Board (EDIB) to develop guidelines. The DGA extends the legal framework for the reuse of sensitive public sector information with safeguards. It also establishes a framework for data intermediation services to facilitate controlled data sharing, and introduces data altruism, which allows data subjects to decide whether to share their data. These measures create new opportunities for stakeholders interested in accessing, sharing and reusing data. The DA is important for mobility data spaces and ecosystems in several ways. It improves access to mobility data from connected vehicles and infrastructure, fostering innovation in the mobility sector. It also enables public authorities to access and use private sector data in certain situations. It further specifies requirements for data interoperability and sharing mechanisms, ensuring that (mobility) data can be integrated across systems and platforms.

The EU has also introduced the **Digital Markets Act** (DMA) and the **Digital Services Act** (DSA) to address specific players in the digital economy with the aim to create a safer digital environment, protect users' rights, and establish a level playing field for businesses. These laws can indirectly impact mobility data spaces: DMA by regulating large digital platforms and preventing anti-competitive behaviour that might otherwise hinder data sharing in the mobility sector; DSA by improving transparency and accountability of platforms within scope that may be used in mobility services.

The **Interoperable Europe Act** is another piece of legislation that has been introduced by the EU to enhance the interoperability of public services across the Member States and facilitate access to and sharing of public sector data across borders. Of particular relevance to the mobility sector, this act can support the implementation of the objectives of the ITS Directive. In particular in border regions, the use of data from different Member States may be needed for development and use of ITS applications. The Interoperable Europe Act promotes cross-border interoperability of trans-European digital services and facilitates the cross-border exchange of data. It can thus contribute to the deployment and use of EU-wide ITS.

Moreover, the EU has introduced the world's first comprehensive AI law – the **AI Act** – to ensure a high level of protection from harmful effects of AI systems in the EU, while supporting innovation and improving the functioning of the internal market. Even though it deals with AI-systems, the AI Act is relevant to mobility data spaces, providing a framework for developing and using AI, especially high-risk systems, to ensure trustworthiness and safety. Data spaces can offer AI developers access to more data for learning and predictions. Interoperable data spaces facilitate data integration and analysis. The AI Act also sets data quality requirements for high-risk AI systems, which data spaces must ensure their datasets meet if they are to be used in such systems.

Moreover, the **INSPIRE Directive**, with the purpose of providing better access to standardised spatial data, such as data on transport networks, is of relevance for mobility data spaces. Some of the project's use cases focus on such data. (The implementing act on high-value datasets, see below, relies on the INSPIRE Directive in terms of actual datasets and their modes of provision for the definition of high-value datasets in the category mobility.)

Moreover, the **Open Data Directive** and the **High Value Datasets Implementing Act** enhance the accessibility and reusability of public sector information. The directive sets out the general framework for making such information available for reuse across the EU and the implementing act specifies specific datasets with high socio-economic potential that the public sector must make reusable as open data and free of charge, such as data on transport networks. This increases the accessibility of such data for various applications in the field of mobility.

Relevant to our project is also the **Intelligent Transport Systems (ITS) Directive**, which promotes data availability of data types relevant to ITS services in road transport, such as travel planning and real-time traffic information services. This directive and its delegated regulations require certain road, travel, and traffic data to be available in digital format. Several of the project's use cases focus on ITS data. Moreover, by establishing common European specifications to ensure that ITS data is accessible, standardised, and shareable across different platforms, interoperability between systems is ensured, which also benefits mobility data spaces. Additionally, the National Access Points (NAPs), where ITS data should be exchanged in all the Member States, will be an important part of the future EMDS, ensuring that transport-related data is accessible and can be shared effectively.

The **TEN-T Regulation**, revised in 2024, is the legal basis for the Urban Mobility Indicators (UMI), which are used to assess and improve urban transportation systems. The Commission will adopt an implementing act setting out indicators in certain areas. The Member States will have to provide to the Commission urban mobility data for these indicators covering each urban node. The cities involved in the project are urban nodes, and within the regions involved there are also urban nodes. Several of the deployEMDS use cases focus on facilitating the availability, sharing and reuse of data for UMI indicators.

We also **examined how cross-sectoral data legislation** (the DGA, DA, Interoperable Europe Act, and AI Act) **impacts sector-specific mobility data legislation** (particularly the ITS Directive and its delegated acts). The analysis highlights the importance of the various cross-sector and sector-specific legislation on data for the EMDS. The cross-sectoral legislation on data collectively establishes a legal framework that facilitates secure and trusted access to data, promotes data sharing and ensures interoperability, thereby enabling data spaces in the EU. This framework also impacts sector-specific legislation such as the ITS Directive and its delegated regulations. By facilitating data access, promoting the secure and trusted data handling, and ensuring common standards and interoperability, the cross-sectoral legislation can support the implementation of the ITS Directive and its delegated regulations. The interaction between cross-sectoral and sector-specific regulations contributes to a European market for data in the mobility sector and the creation of the EMDS.

We will continue to analyse the legal frameworks and **develop legal tools** in forthcoming project activities.

4 Conclusions

By **collaborating on mobility data**, authorities, companies, and the public can create smarter, more sustainable mobility systems. Technological advances have surged data generation and sharing, fostering a collaborative data environment with new platforms and ecosystems. Privacy-preserving technologies and decentralised models aim to balance control and accessibility, though barriers remain.

Data sharing is crucial in the evolving urban mobility landscape to address mobility challenges, improve transport systems, traffic management, and urban planning. **Mobility** is a complex and evolving field with diverse stakeholders with different priorities and standards. In addition, different modes of transport operate under different regulations and technologies. There are also geographical variations as transport systems vary from one location to another, influenced by local policies, infrastructure, and strategies. The field's complexity and stakeholder diversity present both challenges and opportunities.

In this context, governance and legal challenges become central. **Defining terms and concepts** such as 'data', 'governance', and 'data governance' proves to be quite difficult. Uniform definitions are rare, and the definitions available often vary in detail, emphasise different aspects, and change depending on the context. It is **important to know which policies are applicable** for the activities and organisations under consideration, as this impacts what data refers to and what that implies in terms of rights and responsibilities.

Governance challenges span organisational, legal, and technical aspects, influenced by power dynamics. Many of the challenges are interconnected and influence several aspects of governance. Addressing more complex and multifaceted challenges might require a holistic approach that considers organisational practices, legal frameworks, technical solutions, and the broader power dynamics at play. Challenges include, for example, ensuring data integrity and security; navigating legal frameworks and enforcing compliance; ensuring data interoperability; data ownership (control) interests and reluctance to share data; and ensuring data quality.

Governance principles, such as participation, accountability, transparency, responsiveness, efficiency, rule of law, fairness, and sustainability, can guide trust and cooperation in data sharing, and they can be detailed further in specific governance mechanisms in our project. Additionally, the FAIR principles provide a framework for enhancing data findability, accessibility, interoperability, and reusability.

Data space governance extends beyond data governance to also include the management of the partnerships and collaborations needed to unlock the value of data. A community-based, purpose-driven approach is crucial for ensuring stakeholder buy-in and addressing diverse environments in which the data is produced and consumed. Flexible frameworks and a focus on both technical and governance building blocks help ensure efficient and secure data spaces.

A **multi-level governance system** for the EMDS with interconnected autonomous data space instances has been proposed. Aligning local and regional data spaces with the EMDS enhances interoperability, data sharing, and cross-border cooperation, fostering innovation and informed decision-making.

The review of **governance in the local implementation sites** underscores the importance of the local level in mobility data sharing, for autonomy, community focus and better alignment with local needs. However, it also highlights challenges such as articulating values, strategic guidance, and coordinating across governance levels. Based on the analysis, boundaries are not always clearly defined, values and ethical principles are not fully formalised, and rules need to be more explicit. Mechanisms to influence rulemaking are lacking, and onboarding strategies are insufficient. Monitoring mechanisms need to be more transparent, and conflict resolution strategies are unclear. We also highlight adapting to mandatory and voluntary

requirements to make data spaces more sustainable and responsible. Decision-making power should remain local (to the extent possible), with support from higher levels.

Looking at **legal considerations**, several legal frameworks and instruments impact whether and how mobility data can be shared (e.g., legal rights to data access, legal restrictions on sharing certain data categories). This includes legal frameworks that target data “as such”, but also traditional frameworks that were already in place and can equally directly or indirectly apply to data. On top of this complexity, there are also mobility specific laws that apply to certain data categories. The key challenge going forward is to decode the application of these laws with concrete use cases in mind but also try to understand potential interactions and incompatibilities. Laws such as the Data Governance Act and the Data Act – introduced to facilitate the data-driven economy – are still in their infancy and it remains to be seen how they will be applied and to what extent they can facilitate data sharing in the mobility sector.

In **forthcoming project activities**, we will continue to analyse the legal frameworks and develop legal tools, address specifically selected governance and legal challenges within policy labs, and develop business and governance mechanisms to facilitate access to and sharing of mobility data within and across borders.

5 References

AI Aware Scale Up (2023). AI Powered Awareness for Increased Traffic Safety – Final Report, V1.0. Retrieved from www.drivesweden.net/sites/default/files/2024-02/ai-aware-scale-up-final-report-v1.0-1.pdf.

Abraham, R., Schneider, J., vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, Volume 49, 2019, pages 424-438, ISSN 0268-4012. Doi: https://doi.org/10.1016/j.ijinfomgt.2019.07.008.

Anderson, J., Sarkar, D., & Palen, L. (2019). Corporate editors in the evolving landscape of OpenStreetMap. ISPRS International Journal of Geo-Information, 8(5), 232.

Arnaut, C., Pont, M., Scaria, E., Berghmans, A., Leconte, S. (2018). Study on data sharing between companies in Europe – Final report. Publications Office. Doi: https://data.europa.eu/doi/10.2759/354943.

Bayamlıoğlu, E. (2021). EUHubs4Data Deliverable D3.6 Evaluation and recommendations on the legal conditions for trading data in a complete ecosystem I 1.0. Retrieved from https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e18183a1&appId=PPGMS.

Bayamlioğlu, E., Benmayor, A., Blanco justicia, A., & de Ryck, D. (2022). MobiDataLab Deliverable D2.1 Legal and Regulatory Data Sharing Gap Analysis. Retrieved from https://mobidatalab.eu/wp-content/uploads/2023/01/MobiDataLab-D2.1-LegalRegulatoryDataSharingGapAnalysis-v1.1.pdf.

Bayamlioğlu, E., & Benmayor, A. (2023). MobiDataLab Deliverable D2.7 Data Governance Assessment. Retrieved from https://mobidatalab.eu/wp-content/uploads/2023/01/MobiDataLab-D2.7-DataGovernanceAssessment-v1.1.pdf.

Benfeldt, O., Persson, J.S. & Madsen, S. (2020). Data Governance as a Collective Action Problem. Inf Syst Front 22, 299–313 (2020). Doi: https://doi.org/10.1007/s10796-019-09923-z.

Benmayor, A., Blanco Justicia, A., Plot B., Mechyakha H. (2024). MobiDataLab Deliverable D2.2 Recommendations on data sharing legal frameworks. Retrieved from https://mobidatalab.eu/wp-content/uploads/2024/02/MobiDataLab-D2.2-RecommendationsOnDataSharingLegalFrameworks_v1.0_DRAFT.pdf.

Bria, F. Blankertz, A., Fernández-Monge, F., Gelhaar, J., Grafenstein, M. v., Haase, A., Kattel, R., Otto, B., Sagarra Pascual, O., & Rackow, L. (2023). Governing urban data for the public interest. The New Institute. Retrieved from https://thenew.institute/media/pages/documents/529e984d02-1698245881/the-new-hanse_blueprint_governing-urban-data-for-the-public-interest.pdf.

Burden, H., Stenberg, S., & Olsson, M. (2023). Proposed EU Regulations' Impact on Data Utilisation – A Multi-Case Study within Public Transport. RISE Report 2023:47. Retrieved from https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Ari%3Adiva-64372.

Burden, H., & Stenberg, S. (2024). Fit for purpose – Data quality for Artificial Intelligence. RISE Report 2024: 57. Retrieved from https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Ari%3Adiva-74929.

Cazacu S., Chandrasekhar, R., Dulong de Rosnay M., and Vancauwenberghe, G. (2024). Towards a sustainable Open Data ECOsystem D2.3: User needs from a governance perspective. D2.3, ODECO project. 2024, 103 p.

Commission on Global Governance (1995). Our Global Neighbourhood: The Report of the Commission on Global Governance. Oxford: Oxford University Press.

Coyle, D., Kay, L., Diepeveen, S., Tennison, J. & Wdowin, J. (2020a). The Value of Data – Policy Implications. Bennett Institute for Public Policy, Cambridge in partnership with the Open Data Institute. Retrieved from www.bennettinstitute.cam.ac.uk/publications/value-data-policy-implications/.

Coyle, D; Diepeveen, S. Wdowin, J., Kay, L. & Tennison, J. (2020b): The Value of Data: Summary report 2020. Cambridge: The Bennett Institute for Public Policy. Retrieved from www.bennettinstitute.cam.ac.uk/wpcontent/uploads/2020/12/Value_of_data_summary_report_26_Feb.pdf.

Curry, E., Tuikka, T., Metzger, A., Zillner, S., Bertels, N., Ducuing, C., Dalle Carbonare, D., Gusmeroli, S., Scerri, S., López de Vallejo, I. & García Robles, A. (2022). Data Sharing Spaces: The BDVA Perspective. In: Otto, B., ten Hompel, M., Wrobel, S. (eds) Designing Data Spaces. Springer, Cham. Doi: https://doi.org/10.1007/978-3-030-93975-5_22.

data.europa academy (2023, May 12). Data spaces: Introducing the concept and relevance in today's world. [Video]. YouTube. Retrieved from www.youtube.com/watch?v=L9U-eKVtspA.

data.europa.eu (2023, 5 May). Data sharing and competition law. Retrieved on 13 May 2024 from https://data.europa.eu/en/publications/datastories/data-sharing-and-competition-law.

Davies, T. (2022) Data Governance and the Datasphere Literature Review. Datasphere Initiative. Retrieved from https://www.thedatasphere.org/wp-content/uploads/2022/11/Data-governance-and-the-Datasphere-Literature-Review-2022.-Tim-Davies.pdf.

Davis, J. (2018, 28 June). The Big Data Question: To Share or Not To Share. InformationWeek. Retrieved on 29 September 2024 from www.informationweek.com/data-management/the-big-data-question-to-share-or-not-to-share#close-modal.

Deloitte (2017). Assessing the value of TfL's open data and digital partnerships. Retrieved from http://content.tfl.gov.uk/deloitte-report-tfl-open-data.pdf.

Deloitte (2018), 'Study to support the review of Directive 2003/98/EC on the re-use of public sector information', published 24 April 2018, https://op.europa.eu/en/publication-detail/-/publication/45328d2e-4834-11e8-be1d-01aa75ed71a1/language-en.

Determann, L. (2018). No One Owns Data. UC Hastings Research Paper No. 265. Doi: http://dx.doi.org/10.2139/ssrn.3123957.

DIGG (2020). Sveriges digitala förvaltning 2020 – En samlad analys och bedömning av digitaliseringen av den offentliga förvaltningen.

DIGG (2022). Uppföljning av statliga myndigheters digitalisering 2021 – En enkätundersökning. Dnr 2021-2731.

DIGG (2023). Digitala Sverige 2022 – En samlad analys av samhällets digitalisering. Dnr 2023–0715.

DSBA (2023). Technical Convergence – Discussion Document, Version 2.0. Retrieved from https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.

DSSC (2023, 27 September). DSSC Glossary – Version 2.0. Retrieved on 13 May 2024 from https://dataspacessupportcentre.refined.site/space/Glossary/176553985/DSSC+Glossary+%7C+Version+2.0+%7C+September+2023.

DSSC (2024). DSSC Insight Series 6 June 2024 – The free flow of data from source to fruition. [Video]. YouTube. https://www.youtube.com/watch?v=fQ2_nWSsvZU.

DSSC (2024). Data Spaces Blueprint v1.0. Retrieved from https://dssc.eu/space/BVE/357073006/Data+Spaces+Blueprint+v1.0.

Dutkiewicz, L., Miadzvetskaya, Y., Ofe, H., Barnett, A., Helminger, L., Lindstaedt, S., & Trügler, A. (2022). Privacy-Preserving Techniques for Trustworthy Data Sharing: Opportunities and Challenges for Future Research. In: Curry, E., Scerri, S., Tuikka, T. (eds) Data Spaces. Springer, Cham. Doi: https://doi.org/10.1007/978-3-030-98636-0_15.

EGUM (2024). EGUM OPINION ON THE SUSTAINABLE URBAN MOBILITY INDICATORS – Best practice on monitoring SUMP implementation, especially on defining and applying sustainable urban mobility indicators and data collection. Retrieved from https://transport.ec.europa.eu/document/download/cb890007-af95-46e8-8f9c-1a29c1efefac_en?filename=EGUM_SUMP_subgroup_SUMI_opinion.pdf.

Eisenträger, M., Seifert, I., Fotakidis, D., Firogenis, G., Lindner, M., Rohde, M., Simon-Lehmstedt, J., Straub, S., Wenzel, B., Atik, C., Bogaardt, M-J., Gomez, T. (2024). Deliverable D2.1: Multi-stakeholder Governance Scheme and Business Models for Agricultural Data Spaces. Retrieved from https://agridataspace-csa.eu/wp-content/uploads/2024/04/D2.1_ADS_Governance-and-Business-Models.pdf.

ENISA (2024). Engineering personal data protection in EU data spaces. Retrieved from www.enisa.europa.eu/sites/default/files/publications/Data%20Spaces%20Report.pdf.

Ernst, S. (2021). Anonymisierung. In: Paal, B. /Pauly, D. (Ed.). Datenschutz-Grundverordnung (3. Edition, p. 49). Munich: C.H.Beck.

Estrada, J., Rouquette, S., & Babío, L. (2022). MOBI-MIX Insight Report: Shared Mobility Data for Policy Making. Bax & Company and POLIS. Retrieved from www.polisnetwork.eu/wp-content/uploads/2022/12/MOBI-MIX-insight-report-4-Shared-mobility-data-for-policy-making.pdf.

EU EIP - Annual NAP Report 2020, 26 February 2021, https://its-platform.eu/wp-content/uploads/ITS-Platform/AchievementsDocuments/NAP/EU%20EIP%20-%20National%20Access%20Points%20-%20annual%20report%202020.pdf.

EU (1996). DIRECTIVE 96/9/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 1996 on the legal protection of databases.

EU (2000). Charter of Fundamental Rights of the European Union, www.europarl.europa.eu/charter/pdf/text_en.pdf.

EU (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201, 31.7.2002, p. 37–47. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058.

EU (2003). Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

EU (2007). Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).

EU (2010). Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

EU (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal L 257, 28.8.2014, p. 73–114.

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

EU (2018). Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

EU (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.

EU (2022a). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

EU (2022b). REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

EU (2022c). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

EU (2022d). 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).

EU (2023a). Directive (EU) 2023/2661 of the European Parliament and of the Council of 22 November 2023 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.

EU (2023b). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

EU (2024a). Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act).

EU (2024b) Regulation (EU) 2024/1679 of the European Parliament and of the Council of 13 June 2024 on Union guidelines for the development of the trans-European transport network, amending Regulations (EU) 2021/1153 and (EU) No 913/2010 and repealing Regulation (EU) No 1315/2013.

EU (2024c). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU)

No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

European Commission (2016). REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT on the implementation of Directive 2007/2/EC of March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) pursuant to article 23. COM(2016) 478 final/2.

European Commission (2020a). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data, COM/2020/66 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

European Commission (2020b). 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 – putting European transport on track for the future, COM/2020/789 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0789.

European Commission (2020c). Berlin Declaration on Digital Society and Value-based Digital Government. News article. Published 8 December 2020. Retrieved on 25 October 2024 from https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government.

European Commission (2020d). Towards a European strategy on business-to-government data sharing for the public interest – Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing. Publications Office. Retrieved from https://data.europa.eu/doi/10.2759/731415.

European Commission (2021). Report – Workshop on the common European mobility data space. Retrieved from https://digital-strategy.ec.europa.eu/en/events/workshop-common-european-mobility-data-space.

European Commission (2022a). COMMISSION STAFF WORKING DOCUMENT on Common European Data Spaces. SWD(2022) 45 final. Retrieved from https://data.consilium.europa.eu/doc/document/ST-6532-2022-INIT/en/pdf.

European Commission (2022b). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Digitalising the energy system – EU action plan. COM/2022/552 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0552&qid=1666369684560.

European Commission (2022c). Commission Implementing Regulation (EU) 2023/138 of 21 December 2022 laying down a list of specific high-value datasets and the arrangements for their publication and re-use.

European Commission (2023a). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Creation of a common European mobility data space, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Transport-data-creating-a-common-European-mobility-data-space-communication-_en.

European Commission (2023b). Questions and Answers on the revision of the Delegated Regulation on multimodal travel information services and on the Communication on the creation of a common European

mobility data space (EMDS). Retrieved on 25 October 2024 from https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_6112.

European Commission (2023c). COMMUNICATION FROM THE COMMISSION – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements. Official Journal C 259, 21.7.2023, p. 1–125. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2023.259.01.0001.01.ENG&toc=OJ%3AC%3A2023%3A259%3ATOC.

European Commission (2024). COMMISSION STAFF WORKING DOCUMENT on Common European Data Spaces. SWD(2024) 21 final. Retrieved from https://ec.europa.eu/newsroom/dae/redirection/document/101623.

European Parliament (2023, 9 November). Boosting data sharing in the EU: what are the benefits? Retrieved on 25 October 2024 from www.europarl.europa.eu/pdfs/news/expert/2022/4/story/20220331STO26411/20220331STO26411_en.pdf.

Eurostat (2024). Digitalisation in Europe – 2024 edition. Retrieved on 26 November 2024 from https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024#about-this-publication.

EU Urban Mobility Observatory, Belgian profile, https://urban-mobility-observatory.transport.ec.europa.eu/sustainable-urban-mobility-plans/member-state-profiles_en.

Farrell, E., Minghini, M., Kotsev, A., Soler-Garrido, J., Tapsall, B., Micheli, M., Posada, M., Signorelli, S., Tartaro, A., Bernal, J., Vespe, M., Di Leo, M., Carballa-Smichowski, B., Smith, R., Schade, S., Pogorzelska K., Gabrielli, L., & De Marchi, D. (2023). European Data Spaces: Scientific insights into data sharing and utilisation at scale. Publications Office of the European Union, Luxembourg, 2023, JRC129900. Doi: https://dx.doi.org/10.2760/400188.

Fischli R, Muldoon J. (2024). Empowering Digital Democracy. Perspectives on Politics. Published online 2024:1-17.

Fritzenkötter, J., Hohoff, L., Pierri, P., Verhulst, S.G., Young, A., & Zacharzewski, A. (2022). Governing the Environment-Related Data Space. TheGovLab. Retrieved from https://files.thegovlab.org/erdgovernance.pdf.

Gabelica, M., Bojčić, R., & Puljak L. (2022). Many researchers were not compliant with their published data sharing statement: a mixed-methods study. Journal of clinical epidemiology, 150, 33–41. Doi: https://doi.org/10.1016/j.jclinepi.2022.05.019.

Gangneux (2023). DS4SSCC Deliverable D2.2 Multi-Stakeholder Governance Scheme. Retrieved from https://static1.squarespace.com/static/63718ba2d90d0263d7fc1857/t/6557179174ea0873bd612813/1700206503021/DS4SSCC_D2.2+Mulkti+stakeholder+governance+scheme_FINAL.pdf.

Global Data Barometer (2021). Global Data Barometer Handbook – Governance: Data sharing frameworks. Retrieved on 25 October 2024 from https://handbook.globaldatabarometer.org/2021/indicators/G.GOVERNANCE.DATASHARING/.

Graux, H. (2022). Sharing Data (Anti-)Competitively – Will European data holders need to change their ways under the proposed new data legislation? Publications Office of the European Union, 2022. Retrieved from https://data.europa.eu/doi/10.2830/913446.

Graux, H. (2024a). Granular Data Governance Systems for Open Data – A primer on the impact of the Data Governance Act on open data ecosystems. data.europa.eu. Publications Office of the European

Union. Retrieved from https://data.europa.eu/sites/default/files/report/Granular%20Data%20Governance%20Systems%20for%20Open%20Data.pdf.

Graux, H. (2024b). What is data ownership, and does it still matter under EU data law? An exploration of traditional concepts of data ownership, and of the expected impact of the Data Act. data.europa.eu. Publications Office of the European Union. Retrieved from https://data.europa.eu/sites/default/files/report/What%20is%20data%20ownership%2C%20and%20does%20it%20still%20matter%20under%20EU%20data%20law.pdf.

Herbert Smith Freehills (2024). Overview of the EU Commission's guidance on information exchange. Published on 21 November 2023. Retrieved on 7 November 2024 from www.herbertsmithfreehills.com/insights/2023-11/overview-of-the-eu-commission%E2%80%99s-guidance-on-information-exchange.

Huyer, E., & Cecconi, G. (2020). Analytical Report n 12: Business-to-Government Data Sharing. Luxemburg: Publications Office of the European Union, Capgemini Invent, European Data Portal, 2020. Doi: https://data.europa.eu/doi/10.2830/078126.

IDSA (n.d.). How to Build Dataspaces? Retrieved on 29 September 2024 from https://docs.internationaldataspaces.org/ids-knowledgebase/how-to-build-data-spaces.

IDSA (2024a, 5 September). IDSA Q&A Session: Your essential guide to data spaces. [Video]. YouTube. Retrieved on 29 September 2024 from www.youtube.com/watch?v=ZzAvC54RdqM.

IDSA (2024b). Interoperability in Data Spaces. Retrieved on 29 September 2024 from https://docs.internationaldataspaces.org/ids-knowledgebase/v/idsa-rulebook/idsa-rulebook/3_interoperability.

ITF (2021). Reporting Mobility Data: Good Governance Principles and Practices. International Transport Forum Policy Papers, No. 101, OECD Publishing, Paris. Doi: https://doi.org/10.1787/b988f411-en.

Jacobsen, A., de Miranda Azevedo, R., Juty, N., et al. (2020). FAIR Principles: Interpretations and Implementation Considerations. Data Intelligence. 2020;2 (1-2) :10-29. Doi: https://doi.org/10.1162/dint_r_00024.

Janssen, M., Brous, P., Estevez, E., S. Barbosa, L., Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. Government Information Quarterly, Volume 37, Issue 3. Doi: https://doi.org/10.1016/j.giq.2020.101493.

Keping, Y. (2018). Governance and Good Governance: A New Framework for Political Analysis. Fudan J. Hum. Soc. Sci. 11, 1–8 (2018). Doi: https://doi.org/10.1007/s40647-017-0197-4.

Kotsev A., Minghini M., Cetl V., Penninga F., Robbrecht J., Lutz M. (2021). INSPIRE – A Public Sector Contribution to the European Green Deal Data Space: A vision for the technological evolution of Europe's Spatial Data Infrastructures for 2030. JRC126319. Publications Office of the European Union, Luxembourg. Doi: https://dx.doi.org/10.2760/8563

Linåker, J. and Runeson, P. (2021). How to Enable Collaboration in Open Government Data Ecosystems: A Public Platform Provider's Perspective. JeDEM: EJournal of EDemocracy and Open Government, 13(1), 1-30.

Linåker, J., & Runeson, P. (2022). Sustaining open data as a digital common–design principles for common pool resources applied to open data ecosystems. In Proceedings of the 18th international symposium on open collaboration (pp. 1-11).

Lundahl, J., Sobiech, C., & Thidevall, N. (2023). Framtidens trafikregler – Hur når vi dit? RISE Rapport 2023:6. Retrieved from https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Ari%3Adiva-64042.

Lundahl, J., Stenberg, S., & Faxer, A. (2023). Elsparkcyklar från ett policyperspektiv. Retrieved from https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Ari%3Adiva-67424.

Lundahl, J. (2024a). Steering the Future: An Overview of Current and Upcoming Regulations in Automated Driving, Version 1.0. RISE Report 2024:63. Retrieved from https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Ari%3Adiva-75672.

Lundahl, J. (2024b). One Year of Automated Driving Roundtables: Key Takeaways. Retrieved from https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Ari%3Adiva-76333.

Lundqvist, B. (2018). Data Collaboration, Pooling and Hoarding under Competition Law. Faculty of Law, Stockholm University Research Paper No. 61. Doi: http://dx.doi.org/10.2139/ssrn.3278578.

MaaS Alliance (2021). Interoperability for Mobility, Data Models, and API - Building a common, connected, and interoperable ground for the future of mobility. Working Group 3 - Position paper. Retrieved from https://maas-alliance.eu/wp-content/uploads/2021/11/20211120-Def-Version-Interoperaability-for-Mobility.-Data-Models-and-API-_-FINAL.pdf.

Madrigal, A. C. (2012, 1 March). Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days. Atlantic. Retrieved on 13 May 2024 from www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/?ref=cyberlaw.stanford.edu.

Marshall G. R. (2008). Nesting, subsidiarity, and community-based environmental governance beyond the local level. International Journal of the Commons, 2(1), 75–97. Retrieved from https://www.jstor.org/stable/26522991.

Martini, M. & Roeingh, N. (2024). Freie Fahrt für freie Daten? Das Mobilitätsdatengesetz im Spannungsfeld zwischen Datenschutz und Datennutzung. In Neue Juristische Wiochenzeitschrift: NJW, Volume 33, 2379–2384.

Meinzen-Dick R. (2012). Elinor Ostrom's trailblazing commons research can inspire Rio+20. The Guardian. Retrieved from www.theguardian.com/global-development/poverty-matters/2012/jun/14/elinor-ostrom-commons-rio20.

McGinnis, M. & Ostrom, E. (1992). Design Principles for Local and Global Commons. Paper presented at the Linking Local and Global Commons, Cambridge, MA. Retrieved from https://dlc.dlib.indiana.edu/dlcrest/api/core/bitstreams/28e75858-baf3-4cf8-917b-da51a1053b11/content.

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. Big Data & Society, 7(2). Doi: https://doi.org/10.1177/2053951720948087.

Mildebrath, H. (2023). Understanding EU data protection policy. Retrieved from www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI%282022%29698898_EN.pdf.

Müller, J.-H., Andersson, K., Fjällström, A., & Lundahl, J. (2024). Navigating the Future: Enhancing E-Scooter Traffic Management through Governance and Regulation. Retrieved from https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Ari%3Adiva-74584.

Nagel L., Lycklama D. (2021): Design Principles for Data Spaces. Position Paper. Version 1.0. Berlin. Doi: http://doi.org/10.5281/zenodo.5105744.

Nagel, L., & Lycklama, D. (2022). How to Build, Run, and Govern Data Spaces. In: Otto, B., ten Hompel, M., Wrobel, S. (eds) Designing Data Spaces. Springer, Cham. Doi: https://doi.org/10.1007/978-3-030-93975-5_2.

Nationell dataverkstad (2022, 24 Nov). Dataverkstaden arrangerar: Informationssäkerhet och öppna data. Retrieved on 13 May 2024 from https://player.vgregion.se/s/KiMFjjDb6VqhTiG48EDYWN/GJgQfWVd5Tpq9BiZEsWbDZ.

Neumaier, S., Thurnay, L., Lampoltshammer, T. J., & Knap, T. (2018). Search, filter, fork, and link open data: The ADEQUATe platform: Data- and community-driven quality improvements. WWW '18: Companion Proceedings of the Web Conference 2018. April 2018. Pages 1523–1526. Doi: https://doi.org/10.1145/3184558.3191602.

Observatory of Transport and Logistics in Spain, Report: Urban and metropolitan mobility: A major challenge for cities in the 21st century (January 2020). Retrieved from https://cdn.mitma.gob.es/portal-web-drupal/OTLE/elementos_otle/monografico_otle_2019_movilidad_urbana_y_metropolitana_1.pdf.

ODI (2020, 26 September). The Data Spectrum. Retrieved on 7 November 2024 from https://theodi.org/insights/tools/the-data-spectrum/.

OECD (2015). Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing, Paris. Doi: https://doi.org/10.1787/9789264229358-en.

OECD (2019). Enhancing Access to and Sharing of Data – Reconciling Risks and Benefits for Data Re-use across Societies. Doi: https://doi.org/10.1787/276aaca8-en.

OECD (2020). OECD Digital Economy Outlook 2020, OECD Publishing, Paris. Doi: https://doi.org/10.1787/bb167041-en.

OECD (2021). Recommendation of the Council on Enhancing Access to and Sharing of Data. OECD Legal Instruments, OECD/LEGAL/0463, adopted on 06/10/2021. Retrieved from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463.

OECD (2022a). Going Digital to Advance Data Governance for Growth and Well-being. OECD Publishing, Paris. Doi: https://doi.org/10.1787/e3d783b0-en.

OECD (2022b). Responding to societal challenges with data: Access, sharing, stewardship and control. OECD Digital Economy Papers, No. 342, OECD Publishing, Paris. Doi: https://doi.org/10.1787/2182ce9f-en.

OECD (2022c). Measuring the value of data and data flows. OECD Digital Economy Papers, No. 345, OECD Publishing, Paris. Doi: https://doi.org/10.1787/923230a6-en.

OECD (2023). Smart City Data Governance: Challenges and the Way Forward, OECD Urban Studies, OECD Publishing, Paris. Doi: https://doi.org/10.1787/e57ce301-en.

Ostrom, E. (1990). Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge University Press, Cambridge, UK (1990).

Ostrom E. (1999). Coping with tragedies of the commons, Annual Review of Political Science, 2:493- 535.

Otto, B. (2011). Data governance. Business and Information Systems Engineering, 3(4), 241–244. Doi: https://doi.org/10.1007/s12599-011-0162-8.

Palen, L., Soden, R., Anderson, T. J., & Barrenechea, M. (2015, April). Success & scale in a data-producing organization: The socio-technical evolution of OpenStreetMap in response to humanitarian events. In Proceedings of the 33rd annual ACM conference on human factors in computing systems (pp. 4113-4122).

Park, C. H., Longo, J., & Johnston, E. W. (2020). Exploring non-state stakeholder and community-led open governance: Beyond the three pillars of open government. Public Performance & Management Review, 43(3), 587-612.

Pavel, V., Kind, C., Strait, A., Reeve, O., Peppin, A., Szymielewicz, K., Veale, M., MacDonald, R., Lynskey, O., Coyle, D., & Nemitz, P. (2022). Rethinking data and rebalancing digital power. Ada Lovelace Institute: London, UK. Retrieved from www.adalovelaceinstitute.org/report/rethinking-data/#fnref-1.

PrepDSpace4Mobility (2023). Deliverable D3.1 – Towards a common European mobility data space: Perspectives, recommendations and building blocks. Retrieved from https://mobilitydataspace-csa.eu/wpcontent/uploads/2023/10/deliverable-3.1.pdf.

Pretzsch, S., Drees, H., & Rittershaus, L. (2022). Mobility Data Space: A Secure Data Space for the Sovereign and Cross-Platform Utilization of Mobility Data. In: Otto, B., ten Hompel, M., Wrobel, S. (eds) Designing Data Spaces. Springer, Cham. Doi: https://doi.org/10.1007/978-3-030-93975-5_21.

Pursiainen, H. (2020) 'When the going gets easier', Permanent Secretary, Ministry of Transport and Communications of Finland, 2 March 2020.

Reiberg, A., Niebel, C., & Kraemer, P. (2022). What is a Data Space? Definition of the concept Data Space. Gaia-X Hub Germany, White Paper 1/2022.

Ruhaak, A., Bloom, G., Motz, G., Raymond, A., Siddarth, D., Tavernier, W., Dulong de Rosnay, M. (2021, 6 December). A Practical Framework for Applying Ostrom's Principles to Data Commons Governance. Retrieved on 7 November 2024 from https://foundation.mozilla.org/en/blog/a-practical-framework-for-applying-ostroms-principles-to-data-commons-governance/.

Ruhaak A. (2021). The *governance* in data governance. Blog post. Retrieved from https://foundation.mozilla.org/en/blog/the-governance-in-data-governance/.

S. Oliveira, M.I., Barros Lima, G.d.F., & Farias Lóscio, B. (2019). Investigations into Data Ecosystems: a systematic mapping study. Knowledge and Information Systems, 61(2), 589–630. Retrieved from https://doi.org/10.1007/s10115-018-1323-6.

Shashidharan, S. (2023). Google Maps 101: Welche Rolle KI für stets aktuelle Geschwindigkeitsbegrenzungen in Google Maps spielt. Google. Blog post. Retrieved on 7 November 2024 from https://blog.google/intl/de-de/produkte/suchen-entdecken/google-maps-101-geschwindigkeitsbegrenzungen-ki/.

Sheombar, H., van Oosterhout, M., Diran D., Bagheri, S., & Popp Larsen, C. (2020). RUGGEDISED D6.6: Governance, Trust and Smart City Business Models: the Path to Maturity for Urban Data Platforms. Retrieved from https://ruggedised.eu/fileadmin/repository/Publications/RUGGEDISED-D6.6-Governance-Trust-SmartCity_business_Models-EUR-FINAL-2020.11.13.pdf.

Simcoe, T. (2014). Governing the Anticommons: Institutional Design for Standard-Setting Organizations. NBER Chapters. In: Innovation Policy and the Economy, Volume 14, pages 99-128, National Bureau of Economic Research, Inc. https://www.journals.uchicago.edu/doi/10.1086/674022#.

Sitra (2022). Rulebook for a Fair Data Economy – Version 2.0. Retrieved from https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy.

Smith, G. (2020). Making Mobility-as-a-Service: Towards Governance Principles and Pathways. Retrieved from https://research.chalmers.se/publication/516812.

Snaith, B. (2020). What mobility data has been collected and published during Covid-19? The Open Data Institute, ODI. Retrieved on 13 September 2024 from https://theodi.org/news-and-events/blog/what-mobility-data-has-been-collected-and-published-during-covid-19/.

Swedish Government (2021). Regeringens proposition 2021/22:225 Den offentliga sektorns tillgängliggörande av data. Prop. 2021/22:225. Retrieved from https://data.riksdagen.se/fil/AE688353-E486-4E6D-A757-5B78F6A18F0A.

Tarkowski A., Bloemen S., Keller P., and de Groot T. (2022) Generative Interoperability: Building Online Public and Civic Spaces. Retrieved from https://openfuture.eu/publication/generative-interoperability/.

Tenopir, C., Allard, S., Douglass, K., Aydinoglu, A. U., Wu, L., Read, E., Manoff, M., & Frame, M. (2011). Data sharing by scientists: practices and perceptions. PLoS ONE 6(6), e21101. Doi: https://doi.org/10.1371/journal.pone.0021101.

Torre-Bastida, A.I., Gil, G., Miñón, R., & Díaz-de-Arcaya, J. (2022). Technological Perspective of Data Governance in Data Space Ecosystems. In: Curry, E., Scerri, S., Tuikka, T. (eds) Data Spaces. Springer, Cham. Doi: https://doi.org/10.1007/978-3-030-98636-0_4.

UNESCAP (n.d.). What is Good Governance? Retrieved from www.unescap.org/sites/default/files/good-governance.pdf.

van der Waal, S., Stikker, M., Kortlander, M., van Eeden, Q., Demeyer, T., & Bocconi, S. (2020). Digital European Public Spaces. Waag Futurelab for technology and society. Retrieved from https://waag.org/sites/waag/files/2021-04/Waag%20Report%20on%20Digital%20European%20Public%20Spaces.pdf.

Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. Journal of Management Information Systems, 12(4), 5–33. Doi: https://doi.org/10.1080/07421222.1996.11518099.

Watson C. (2022). Many researchers say they'll share data – but don't. Nature, 606(7916), 853. Doi: https://doi.org/10.1038/d41586-022-01692-1.

Verhulst, SG and Saxena, S (2022) The need for new methods to establish the social license for data reuse. Data & Policy Blog (blog), 20 May 2022. Available at https://medium.com/data-policy/the-need-for-new-methods-to-establish-the-social-license-for-data-reuse-e7c67bdc4aff (Accessed 9 Jan. 2025).

Weill, P., & Ross, J. W. (2004). IT Governance on One Page. CISR Working Paper, (349). Doi: http://dx.doi.org/10.2139/ssrn.664612.

Wieringa, R. J. (2014). Design science methodology for information systems and software engineering. Springer.

Wilkinson, M., Dumontier, M., Aalbersberg, I., & et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018. Doi: https://doi.org/10.1038/sdata.2016.18.

World Economic Forum (2019). Global Technology Governance – A Multi-stakeholder Approach. Whitepaper. Retrieved from www3.weforum.org/docs/WEF_Global_Technology_Governance.pdf.

World Bank (2021). Data for better lives. World Development Report 2021. Retrieved from https://wdr2021.worldbank.org/the-report/.

Wu, J., & Thomann, E. (2023). Governance in Public Policy. In: van Gerven, M., Rothmayr Allison, C., Schubert, K. (eds) Encyclopedia of Public Policy. Springer, Cham. Doi: https://doi.org/10.1007/978-3-030-90434-0_66-1.

Yin, R. K. (2012). Applications of case study research (Vol. 34). Sage.

& Fika (2022). 48 | Samtal med DIGG om digitalisering av offentlig sektor. [Video]. YouTube. Retrieved on 23 April 2024 from https://www.youtube.com/watch?v=Y9huwfi5-jI.

Annex 1. Questions in the survey with deployEMDS local implementation sites

This annex contains the questions used in the survey sent to the local implementation sites (see Section 2.3.2). The survey aimed to explore governance challenges related to mobility data sharing as perceived by the sites. The set of questions was based on challenges repeatedly mentioned in the literature (see Section 2.3). A brief summary of the responses can be found in Section 2.3.2, while a more detailed summary of the responses can be found in Annex 2.

Organisational governance

1) Please select all the organisational governance challenges from the list below that you experience or are affected by:

1. Slow digital transformation.
2. Absence of a formal data strategy.
3. Lack of data sharing culture.
4. Trust issues (incl. understanding how to build trust and mitigate trust issues among actors involved in data cooperation).
5. Opacity on data contracts.
6. Challenges related to defining common purpose and scope for data cooperation (potential challenges related to aligning different visions and priorities).
7. How to organise around data sharing (decide on legal form, governance authority, assign roles and responsibilities, develop an effective governance framework, etc.).
8. How to ensure fair representation of participants in data governance bodies (and the ability of participants to contribute to the decision-making processes on an equal basis).
9. How to ensure transparency in data cooperation (challenges might revolve around inadequate information on what data is provided or received, for what purpose and for what duration, etc.; policies, rules and standards not clearly defined).
10. Accountability in data cooperation (e.g. how to adopt suitable accountability measures).
11. How to ensure effective oversight/monitoring and enforcement of rules and policies in data cooperation.
12. Consensus process & reciprocity in data cooperation.
13. Insufficient stakeholder participation and/or low engagement.
14. How to ensure effective onboarding/offboarding of participants.
15. How to consider different needs and interests of stakeholders actively involved.
16. How to deal with external stakeholders and consider their needs.
17. Lack of mandate to distribute and share data.
18. Unwillingness (by other actors) to share data of public interest.
19. How to adopt approaches to citizen-centricity / public interest.
20. How to leverage voluntary data sharing.
21. Insufficient financial resources (e.g. due to high costs related to collecting and processing or distributing and sharing data).
22. Limited capacity for data management (lack of human resources, skills or technical solutions).
23. Limited cross-silo collaboration.
24. A challenging political ambience when it comes to data sharing (e.g. lack of political interest in the issue).
25. Other: …

2) Please specify/elaborate on one or more of the challenges related to organisational governance that you have ticked in the list (for instance, describe an issue you have experienced in detail).

3) What type of key challenge do you see related to organisational governance regarding data sharing across borders (if any)?

Technical governance

4) Please select all the technical governance challenges from the list below that you experience or are affected by:

1. How to implement the FAIR principles.
2. Standards harmonisation.
3. How to ensure data sovereignty (i.e. the possibility for individuals and organisations to control, govern, and ensure the protection of their own data).
4. How to ensure technological sovereignty.
5. How to ensure (and understand) data quality.
6. How to ensure data security.
7. How to ensure data privacy and data protection (e.g. how to implement privacy-preserving mechanisms and privacy by design).
8. How to set and implement usage control policies.
9. How to set and implement measures for identity, authentication and access control.
10. How to ensure data interoperability (decide on common standards, specifications, formats, languages etc.).
11. Discovery of data (finding other relevant data sources and also enhancing data discovery of your own datasets).
12. Identifying shareable data that the city/region holds and define scope and conditions for access and reuse (and knowing others' need of data, i.e. what data would be valuable to others if distributed/shared).
13. Choice of licensing.
14. Challenges related to linked data.
15. Challenges related to open-source software.
16. Integrating legacy systems with new data sharing technologies.
17. Managing data storage and scalability issues.
18. Other: …

5) Please specify/elaborate on one or more of the challenges related to technical governance that you have ticked in the list (for instance, describe an issue you have experienced in detail).

6) What type of key challenge do you see related to technical governance regarding data sharing across borders (if any)?

Legal governance

7) Please select all the legal governance challenges from the list below that you experience or are affected by:

1. Lack of clarity on the laws applicable to data.
2. Navigating and dealing with a complex and fragmented legal framework around accessing and sharing data.
3. Mapping roles and responsibilities under different legal regimes, for instance between the General Data Protection Regulation (GDPR) and the Data Governance Act (DGA).
4. Difficulty to understand how the new regulations impact or change the existing obligations under the Open Data Directive and the ITS Directive.

5. Legal uncertainties on how to respect the rights of individuals and the rights of companies (e.g. trade secrets) under protection laws when sharing data.
6. Challenges related to the application of intellectual property rights.
7. Challenges related to including data sharing obligations in tenders and contracts with suppliers of products and services.
8. Challenges related to entering into data contracts with private companies (for instance voluntary data agreements with private companies).
9. Understand how to benefit from data intermediary services and what the potential implications might be.
10. Understand how to benefit from data altruism organisations and what the potential implications might be.
11. Lack of legislation mandating the sharing of private sector data deemed to be in the public interest.
12. Understanding the legal implications of using emerging technologies (e.g. AI, blockchain) in data sharing.
13. Addressing legal liabilities in case of data breaches or misuse.
14. Other: …

8) Please specify/elaborate on one or more of the challenges related to legal governance that you have ticked in the list (for instance, describe an issue you have experienced in detail).

9) What are the main legal frameworks that you are having difficulty with when it comes to data sharing (e.g. data protection, procurement)?

10) Could you please share an example where legislation (or legal uncertainty) was a barrier to data access or sharing in your city/region?

11) What do you consider as the biggest obstacle from a legal perspective to sharing data (e.g. lack of certain legislative provisions)?

12) If you experience data protection as one of the legal challenges, what are the specific issues you are facing and how are you tackling them?

13) Does a strong enforcement approach from the relevant independent authorities (e.g. data protection authorities) play a role in your approach to data sharing?

14) What type of key challenge do you see related to legal governance regarding data sharing across borders (if any)?

Power dynamics

15) Please select all the challenges related to the overall vision and principles of the data sharing (which are related to power dynamics) that you find important (from the perspective of your organisation) in the list below:

1. How to create tangible societal value and public benefits of data sharing and use.
2. How to level the playing field in terms of data sharing and reuse between different types of stakeholders.
3. How to clearly explain purpose of data sharing and reuse for each use-case and demonstrate this societal value/public benefit.
4. How to abide by the principles of technological and data sovereignty with particular attention to avoiding vendor lock-ins.
5. How to align with the European Green Deal objectives and with the European data strategy, including on data and technological sovereignty.
6. Other…

16) Please specify/elaborate on one or more of the challenges related to power dynamics around data sharing that you have ticked in the list.

17) What type of key challenge do you see related to power dynamics around data sharing across borders (if any)?

Extra questions

18) Is there any city or region (in the project) that you find particularly inspiring when it comes to data governance?

19) Do you have any other comments or suggestions?

Annex 2. Responses in the survey with deployEMDS local implementation sites

This annex contains **responses from the local sites** to a survey we sent to them in order to explore which governance challenges they face in mobility data sharing. A brief summary of the responses can be found in Section 2.3.2. The survey questions can be found in Annex 1. The survey was sent to all nine implementation sites, and six of them replied.

Organisational challenges

We asked the local implementation sites about organisational challenges related to the governance of data sharing, such as transparency, accountability, oversight/monitoring, representation of participants in data governance bodies and their ability to contribute to decision-making processes, enforcement, etc. They were asked to select from a list of 25 organisational governance challenges they experienced or were affected by. The list included 24 specified choices and a 25th option, 'other', which respondents could specify. They were also asked to elaborate on challenges they had selected and to identify any key challenges related to organisational governance in the context of cross-border data sharing.

The results reveal that *five out of six sites* experience or are affected by these challenges:

- How to organise around data sharing (decide on legal form, governance authority, assign roles and responsibilities, develop an effective governance framework, etc.).
- Limited capacity for data management (lack of human resources, skills, or technical solutions).

Additionally, *four out of six sites* experience or are affected by:

- Slow digital transformation.
- Trust issues (including understanding how to build trust and mitigate trust issues among actors involved in data cooperation).
- Opacity on data contracts.
- Unwillingness (by other actors) to share data of public interest.
- Insufficient financial resources (e.g., due to high costs related to collecting, processing, distributing, and sharing data).

Beyond these responses, the results were more scattered, but challenges that *half* of the respondents reported were a lack of data sharing culture, limited cross-silo collaboration, and the consensus process and reciprocity in data cooperation.

Challenges that *one or two* of the respondents mentioned were: absence of a formal data strategy, challenges related to defining common purpose and scope for data cooperation, how to ensure fair representation of participants in data governance bodies (and the ability of participants to contribute to the decision-making processes on an equal basis), how to ensure transparency in data cooperation; accountability in data cooperation, how to ensure effective oversight/monitoring and enforcement of rules and policies in data cooperation, insufficient stakeholder participation and/or low engagement, how to ensure effective onboarding/offboarding of participants; how to consider different needs and interests of stakeholders actively involved; how to deal with external stakeholders and consider their needs; lack of mandate to distribute and share data; how to leverage voluntary data sharing; a challenging political ambience when it comes to data sharing (e.g., lack of political interest in the issue).

Challenges were also added under 'other': poor data architecture and management processes to promote confidence in sharing and publishing data, as well as reluctance to publish low-quality data that could negatively impact institutional reputation or cause external perceptions of poor operational performance.

When asked to specify or elaborate on one or more of the challenges related to organisational governance that they had selected from the list, a lot of information was provided:

- For instance, one challenge mentioned was the lack of leadership for organisational governance; it is not clear which entity will be the data space authority (and maintain authority after the project).
- Others mentioned challenges related to lack of a data strategy and lack of a data-sharing culture.
- Lack of a business case was highlighted, along with challenges in evaluating real business value potential. Additionally, there is a need to incur extra costs, both human and technical, to process data, mostly due to uncertainty about the real costs, how to transfer part of the costs to the data beneficiary, and how to define a cost-sharing framework between stakeholders. Moreover, issues of reciprocity were noted, questioning whether data consumers should also share data proportionally.
- Challenges related to how to consider the different needs and interests of stakeholders actively involved were also mentioned, specifically on how to design strong use cases for data sharing that cater to every actor's interests. Also mentioned was how to deal with external stakeholders and consider their needs. This can be a complex issue. Sometimes, they would like to obtain different types of outputs or have simpler solutions for their case. Additionally, insufficient stakeholder participation and/or low engagement was mentioned. The level of uncertainty associated with data sharing, inadequate technological maturity, and the strategic and financial risks associated with data sharing may lead organisations to take a more passive approach to data sharing.
- Trust issues due to fears of data misuse were also highlighted.
- Some respondents pointed out that limited capacity for data management, due to a lack of human resources, skills, or technical solutions, is a common challenge for rapidly growing organisations.
- One of the respondents wrote from its perspective as a public organisation that it is committed to sharing data to increase transparency and foster development and innovation. However, the organisation is transitioning from a time when data was not prioritised to recognising its crucial role. The organisation is just beginning to organise its efforts to manage and share data effectively, ensuring collaboration among the right people with the necessary authority and expertise. This transition involves overcoming old practices and establishing new systems and processes. Additional challenges from the public organisation's perspective include, for instance, the mismatch between data sharing objectives and available resources. Hiring IT experts to meet data sharing targets is challenging for a municipality. Furthermore, data contracts between transport authorities and operators often do not specify or are technically vague in describing data sharing governance, leading to varied data sharing and governance processes among different companies.

When asked about *cross-border data sharing*, the respondents highlighted various organisational challenges. For example, one respondent mentioned the challenge of navigating different laws, regulations, and standards, which requires effective collaboration, communication, and coordination to meet regional needs while also ensuring compliance and data security. Otherwise, the risk of legal issues, data breaches, and ineffective data sharing increases. One respondent noted that finding skilled human resources is challenging, and with cross-border data sharing, infrequent work on the subject may lead to forgetting the rules and skills. Other challenges mentioned by the respondents included ensuring effective onboarding and offboarding of participants across borders; dealing with multiple agencies and levels of government, which can delay or complicate data sharing; and variations in organisational practices and cultural expectations that can affect cooperation and data sharing. A challenge mentioned from a city's perspective was that they currently do not share data across borders. While actors can access the city's open data like everyone else, there is no mechanism to collaborate with them on data that the city produces based on its own needs but that may be relevant to them. In addition, it may be the case that terms the city uses for its data lack international definitions. Additionally, respondents mentioned challenges related to current uncertainties regarding the overall governance of the future EMDS.

Legal challenges

We asked the local implementation sites about legal challenges related to the governance of data sharing, such as the complex legal landscape, legal compliance and risks, data protection, etc. They were asked to select from a list of 14 legal governance challenges they experienced or were affected by. The list included 13 specified choices and a 14th option, 'other', which respondents could specify. They were also asked to elaborate on challenges they had selected, specifying or describing an issue they had experienced in detail. Additionally, we inquired about the main legal frameworks they had difficulty with when it comes to data sharing (e.g., data protection, procurement), and asked them to share examples where legislation or legal uncertainty was a barrier to data access or sharing in their city/region.

We also sought their views on what they considered the biggest obstacle from a legal perspective to sharing data (e.g., lack of certain legislative provisions). If they experienced data protection as one of the legal challenges, we asked about the specific issues they were facing and how they were tackling them. Furthermore, we asked whether a strong enforcement approach from the relevant independent authorities (e.g., data protection authorities) played a role in their approach to data sharing. Finally, we asked them to identify any key challenges related to legal governance regarding data sharing across borders.

The results reveal that *all six sites* that responded to the survey experience or are affected by the challenge of understanding how new regulations, such as the Data Governance Act and the Data Act, impact or change the existing obligations under the Open Data Directive and the ITS Directive.

Additionally, *four out of six sites* experience or are affected by these challenges:

- Navigating and dealing with a complex and fragmented legal framework around accessing and sharing data.
- Challenges related to including data sharing obligations in tenders and contracts with suppliers of products and services.
- Addressing legal liabilities in case of data breaches or misuse.

Beyond these responses, the results were more scattered, but challenges that *half* of the respondents reported were lack of clarity on the laws applicable to data, mapping roles and responsibilities under different legal regimes (for instance, between the GDPR and the DGA), challenges related to entering into data contracts with private companies (for instance, voluntary data agreements with private companies), and understand how to benefit from data intermediary services and what the potential implications might be.

Challenges that *one or two* of the respondents mentioned were: legal uncertainties on how to respect the rights of individuals and the rights of companies (e.g., trade secrets) under protection laws when sharing data, lack of legislation mandating the sharing of private sector data deemed to be in the public interest, understanding the legal implications of using emerging technologies (e.g., AI, blockchain) in data sharing.

When we asked the sites to specify or elaborate on one or more of the challenges related to legal governance, they shared insights regarding:

- The importance of considering and being clear in describing data sharing governance when writing new tenders.
- One respondent mentioned that the list in survey opened their eyes to what they did not know but are keen to learn about, and realised the need to also map their internal rules and policies.
- One respondent mentioned, from their city perspective, challenges in understanding data coverage and sharing (how the data should be shared) under the ITS Directive.
- Lack of value capture and lack of related legal agreements makes it difficult to find business cases.
- Involving local administrations is a challenge.
- Addressing issues like data resale and freeriders is a challenge.

- Mapping roles and responsibilities under different legal regimes can be challenging, and understanding the implications of the legal regimes for the governance model for the use case.
- Another challenge is understanding the benefits and implications of data intermediary services.
- The need to better understand the impact of new regulations on existing obligations under the Open Data and ITS Directives on the local use case.
- Challenges related to entering into data contracts with private companies, for instance, challenges related to negotiating terms, protecting intellectual property, and ensuring data privacy.
- There are legal governance barriers to data sharing, including navigating complex legal frameworks and respecting individual and company rights. One respondent mentioned that legal uncertainty on data that may or may not be legally shared and/or the uncertainty on the legal basis for the use of data has been hindering the data sharing process among organisations in the city.

We also asked the sites *which main legal frameworks they are having difficulties with* when it comes to data sharing. Several respondents mentioned the new generation of EU data regulation (especially the DGA and DA). The new obligations under the updated ITS Directive were also mentioned. Respondents also highlighted challenges with complying with some of the GDPR's requirements, particularly obligations related to the rights of data subjects, such as the right to data portability and the right to be informed.

Additionally, we asked if they could share *an example where legislation or legal uncertainty was a barrier* to data access or sharing in their city or region. Some examples were not very concrete and mentioned legal uncertainties around GDPR or the new generation of EU data regulation (DGA and DA). One example provided by a respondent was that in Belgium, only the police are allowed to use ANPR (Automatic Number Plate Recognition) data if the camera is installed for their purposes, which limits other uses of this data, such as for traffic management. Another example mentioned by one of the sites involved an initiative to share urban mobility data with private companies to improve public transport in the city, but legal ambiguities around data protection and intellectual property rights hampered negotiations and delayed the data sharing process.

When asked about the *biggest obstacle from a legal perspective* to sharing data, respondents highlighted: uncertainty about applicable laws; lack of alignment between different legal frameworks; lack of legal resources; the complexity and time-consuming nature of legal issues; challenges for public authorities to demand data from private actors; GDPR compliance, particularly concerning data portability; and local legal framework context between PTAs, PTOs, and regional government. Additionally, they mentioned data privacy concerns and the uncertainty in meeting legal obligations while sharing data effectively and ethically.

We also asked them which *specific data protection challenges* they are facing (if any) and how they are tackling them. The responses were mixed. One respondent mentioned that ticketing data can lead to identifiable information, but partners are comfortable with data protection aspects and have security measures in place. Another respondent mentioned that they currently do not face any significant data protection issues as their data is stored on their own server with robust security measures, but they foresee potential challenges when moving to the cloud and will implement additional measures to ensure data privacy. Another respondent mentioned that they mostly work with open data, but this could change. Yet another response was that before sharing data with a third party, they ensure that the data is properly anonymised, follow GDPR compliance procedures, and involve the data protection officer. One respondent mentioned that the involvement of legal departments as new stakeholders in data governance requires continuous interactions, adding additional effort and cost.

On the question of whether a strong enforcement from relevant independent authorities (e.g., data protection authorities) plays a role in their approach to data sharing, some answered yes while others answered no.

When asked about *cross-border data sharing*, the respondents highlighted various legal challenges, such as the need for coordination among data authorities in different countries; the presence of different legal systems and the choice of forum in case of litigation; differences in data privacy laws and regulations; and the difficulty

of handling origin-destination data due to privacy implications and GDPR compliance, especially when sharing it across borders.

Technical challenges

In this part of the survey, we asked the local implementation sites about technical challenges related to the governance of data sharing, including aspects such as data and technology sovereignty, data quality, security and data protection, common standards, etc. They were asked to select from a list of 18 technical governance challenges they experienced or were affected by. The list included 17 specified choices and an 18th option, 'other', which respondents could specify. They were also asked to elaborate on challenges they had selected and to identify any key challenges related to technical governance in the context of cross-border data sharing.

The results reveal that *four out of six sites* experience or are affected by these challenges:

- Standards harmonisation.
- How to ensure data sovereignty (i.e., the possibility for individuals and organisations to control, govern, and ensure the protection of their own data).
- How to ensure (and understand) data quality.
- How to ensure data privacy and data protection (e.g., how to implement privacy-preserving mechanisms and privacy by design).
- Integrating legacy systems with new data sharing technologies.

Beyond these responses, the results were more scattered, but challenges that *half* of the respondents reported were how to implement the FAIR principles, how to ensure technological sovereignty, how to ensure data interoperability (decide on common standards, specifications, formats, languages etc.), discovery of data (finding other relevant data sources and also enhancing data discovery of your own datasets), and identifying shareable data that the city/region holds and define scope and conditions for access and reuse (and knowing others' need of data, i.e., what data would be valuable to others if distributed/shared).

Challenges that *one or two* of the respondents mentioned were: how to ensure data security; how to set and implement usage control policies; how to set and implement measures for identity, authentication and access control; challenges related to linked data; challenges related to open-source software; and managing data storage and scalability issues. Added under 'other' was the challenge of managing and transforming data to ensure GPDR compliance with published data.

When we asked the sites to specify or elaborate on one or more of the challenges related to technical governance, they shared insights regarding:

- Lack of standards and security concerns are major problems.
- Data available in different formats causes interoperability issues.
- Due to privacy/GDPR implications, it is not always possible to deal with origin-destination data.
- There is a lack of reference metadata profile.
- The control plane is immature locally, but the need is currently limited due to mostly open data.
- Different departments within the organisation have varied systems and rely on external consultants, but efforts are underway to centralise knowledge and improve data management roles.
- Technical barriers to data sharing involve data quality and data integrity, requiring standards, protocols, and issue resolution.
- There is a need for security standards and feedback processes on the data use.
- Setting and implementing usage control policies to ensure data is used as intended is challenging.
- Challenges related to open-source software are the lack of technical knowledge of such software and how to govern it.
- There are several GDPR compliance challenges. Ensuring all personal data is properly anonymised before publication is complex and resource intensive. Data accuracy and integrity must be

maintained throughout the transformation, which requires stringent validation and verification. Implementing and maintaining strict access controls to ensure that only authorised personnel handle sensitive data requires ongoing monitoring and updating of access permissions. Continuously monitoring compliance with GDPR involves regular audits and updates of data handling policies.

- When it comes to standards harmonisation and data interoperability, different semantic models and vocabularies manifest challenges in scalable data and service ecosystems. For example, combining vocabularies between traditional transport, on-demand transport and demand-responsive transport.
- Defining and implementing data usage policies is an advanced step in digitalisation and data sharing, and examples are needed to help onboard PTO participants.
- Identifying shareable data is challenging. Data sources often are not recognised immediately as potential "data products", especially from the public sector. These datasets are sometimes published on open data portals or sometimes not shared at all. There exist models in between, where data is granted in certain conditions, but these are often ad-hoc agreements and thereby lack reach to many private sector actors that can otherwise exploit this data under clear usage conditions.
- Ensuring data quality involves addressing gaps in data, which can be difficult. Interpolation and handling missing values are essential for maintaining data integrity and enabling accurate analysis.
- There are also challenges with linked data. Challenges often stem from interconnecting databases, especially when determining sensor geolocation, requiring cross-referencing between databases.
- Managing data storage and scalability becomes challenging with heavy traffic data due to the high volume of observations, potentially impeding scalable model implementation.

When asked about *cross-border data sharing*, one respondent stressed that the same challenges related to technical governance apply but with higher intensity and impact. Respondents also specified various challenges, such as interoperability issues due to different data formats and standards between countries, and the lack of a reference metadata profile. Inconsistent data formats and standards across borders complicate data sharing and require extensive data transformation efforts. Additionally, they mentioned that technical compatibility is challenging due to varied data management systems and technologies, making seamless integration difficult. Ensuring that different systems can work together and exchange data efficiently requires coordination and common protocols. In addition, aligning security measures and protocols to protect data during transmission and storage across different jurisdictions can be complex. They also noted that maintaining data quality during cross-border exchanges is challenging due to varying standards for data collection, storage, and management, which can affect the accuracy and reliability of data.

Power dynamics and power asymmetries

In this part of the survey, we asked the local implementation sites about challenges related to power dynamics and asymmetries in the governance of data sharing. For example, stakeholders often understand and prioritise value creation from data differently, which can create tensions in data governance. The sites were asked to select from a list of six challenges related to the overall vision and principles of data sharing that they found important from their organisation's perspective. The list included five specified choices and a sixth option, 'other', which respondents could specify. They were also asked to elaborate on challenges they had selected, specifying or describing an issue they had experienced in detail. Additionally, we inquired about the key challenges they see related to power dynamics around data sharing across borders.

The results reveal that *four out of six sites* assess that they have or are affected by the challenge of clearly explaining the purpose of data sharing and reuse for each use case and demonstrating its societal value/public benefit.

Additionally, *half* of the respondents reported that they have or are affected by the challenge of how to level the playing field in terms of data sharing and reuse between different types of stakeholders. The same proportion reported that they have or are affected by the challenge how to abide by the principles of technological and data sovereignty with particular attention to avoiding vendor lock-ins.

Two of the respondents mentioned the challenge of creating tangible societal value and public benefits of data sharing and use.

One challenge that was mentioned under ‘other’ was how to align different data cultures, organisational goals and objectives, technological maturity, and interests between private and public organisations.

Another challenge highlighted under ‘other’ was the need for a 'killer app' – a demonstrator that can clearly showcase the benefits of data spaces. This highlights the necessity for a concrete example (use case) that clearly demonstrates the potential and benefits, making it so compelling that it drives widespread active engagement in data spaces (or other forms of voluntary data sharing).

When we asked the sites to specify or elaborate on one or more of the challenges related to power dynamics around data sharing, they shared insights regarding:

- Designing a governance framework that aligns data cultures, organisational goals, technological maturity, and interests of private and public entities, while centering on societal value, is challenging.
- Clearly explaining the purpose of data sharing and reuse, and demonstrating societal value and public benefit, specifically designing tangible use cases that suit both private and public interests and showing a positive cost-benefit for data sharing, especially for private entities.
- One respondent mentions from their city’s perspective that data is made open when there is a legal mandate or for efficiency in investigations. It is sometimes easier for the city to make the data open to all instead of sharing it with an external investigator.
- Remaining compliant with interoperability principles and ensuring freedom of choice from different data space technology providers is challenging.
- Levelling the playing field between different types of stakeholders requires a governance model with clear conditions for reuse of data products to generate new ones within the ecosystem. The need to ensure that startups and non-profit organisations have fair access to city data to develop innovative solutions that benefit society is also mentioned.
- When it comes to technical sovereignty and data sovereignty, with particular attention to avoiding vendor lock-ins, concepts like the DGA definition of data intermediary need to be better understood.
- Also mentioned is the need to ensure that the data sharing initiatives at the site are aligned with environmental sustainability goals and EU data governance standards to strengthen cooperation and interoperability at the regional level.

When asked about *cross-border data sharing*, the respondents highlighted challenges related to power dynamics: different speeds and levels of maturity between countries (even in deployEMDS), and disparities in markets between different countries that can lead to unequal conditions in data sharing agreements.

Annex 3. Questions for (self-)evaluation based on Ostrom's design principles

In this annex, we unpack Ostrom's eight principles (for these principles, see Section 2.4.2) and list questions used in Section 2.5. These questions can be used for self-assessment by data spaces.

Ostrom's design principles have already been translated to the contexts of data commons (see e.g. Ruhaak et al. (2021), which also cite other studies). In particular, Ruhaak et al. (2021) stress that it is not only the data itself that needs to be governed but also other aspects, such as the management of money and shared values, the value of contributors' time and the rules for their behaviour. We are taking these aspects into account below in the definition of theory and the relevant questions to ask to the cases at hand. Ruhaak et al. (2021) have also created grids with excellent questions that help to design and evaluate data commons" (see Tables 1 and 2 in Ruhaak et al. 2021).

Please note that we have renamed some of the principles to adapt to the analysis of digital commons. Ostrom's original conceptualisation of principles is shown in Appendix B.

Principle 1: Clearly defined boundaries

- What is the scope and vision of the data commons examined?
- What are the boundaries for the data commons in the national case studies that we are examining? Who has access and can share the data?
- Which actors are involved in the governance, management, and use of resources?
- How has this evolved over time?
- Are values that should be created by the commons defined? E.g. public, economic values (based on Ruhaak et al. 2021)

Principle 2: Appropriate rules

ORGANISATIONAL ASPECTS

- Are there clear rules defining the rights, duties and authority of the different stakeholders in the organisation? (Ruhaak et al. 2021)

ECONOMIC ASPECTS

- Funding rules: are there rules around how the data commons is funded or supported? (Ruhaak et al. 2021)
- Spending rules: are there rules around how money can be spent? (Ruhaak et al. 2021)

DATA PRODUCTION, ACCESS AND USE

- Data **collection and production** rules and mechanisms:
    - Are there rules to govern how data can be collected or produced and by whom, how is the integrity of the data protected and how can data be changed? (Ruhaak et al. 2021)
- Data access rules and mechanisms: are there rules in place to govern who can **access** the data, in what way, for what purpose and duration?
    - Is there a difference between how contributors, other stakeholders (if any), and the general public can access the data I.e. rights of exclusion? (Ruhaak et al. 2021)

- Data **use** rules and mechanisms:
    - Are there rules in place to govern who can **use** the data, in what way, for what purpose and for what duration?
    - Is there a difference between how contributors, other stakeholders (if any), and the general public can use the data, i.e., rights of exclusion? (Ruhaak et al. 2021)
- How are processes for managing access/benefits and rights/duties to the data (i.e., in terms of use and contribution to the data shared within the data space) shaped?
- What are the processes and technical infrastructure used for enabling use of and contribution to the shared data?

LICENCES

- Data licensing: are there rules in place to govern what licence is applied, stipulating which terms for use of data, adaptation, etc. Is there a default intellectual property licence attached to contributed data? (Ruhaak et al. 2021)
    - Is it clearly specified how contributors can deviate from the default licence (e.g. a specified list of licences)?
    - Do the rules allow contributors to attach a licence or other terms to the data they contribute that deviate from specified options?
- Is registration required? How are data covered by licensing priced and structured?
- Does the licensing and related costs impede re-use?

SECURITY

- Data storage and security rules and mechanisms: are there rules that govern what methods and tools are used to store, secure and protect the integrity of the data? (Ruhaak et al. 2021)

Principle 3: Collective-choice arrangements

- Who is able to shape the rules and the overarching governance structure of the data ecosystem?
- Are there different levels of governance?
- How is it ensured that those affected will be able to influence the data commons governance structure and rules?
    - Are there means through which the perspectives of stakeholders (including data users, data producers, and potentially data subjects) are articulated, and interests represented? (Ruhaak et al. 2021)
    - Is there a body through which decisions about the organisation are made and are there platforms for making decisions (e.g. discussion platform, voting rules, membership rules)? (Ruhaak et al. 2021)
- Is there a clear process that describes how decisions about the organisation and its representation are made and updated?
- Is there a clear process that describes how decisions about data collection, storage, access and use are made and updated?

Principle 4: Monitoring

- How is monitoring performed that ensures that rights and duties for access, use and collection/contribution of data are ensured? (i.e. mode of access, length of access, type of use, purpose of use etc. at specific time intervals (or continuously) (Ruhaak et al. 2021))
- Who has the responsibility of performing the monitoring?
    - How are these individuals assigned and controlled in turn?

- Are monitoring mechanisms transparent and accountable?
- Are there both external and internal monitoring mechanisms?
- Are there mechanisms monitoring the public good?
- Are there mechanisms to (Ruhaak et al. 2021):
    - ensure data quality and integrity?
    - monitor the security of the architecture (e.g. security breaches, hacks and misuse)?
    - ensure compliance with business rules and rule of law?

Principle 5: Sanctions

- Are there sanctions in place for enforcing the rules and duties related to the access, use of data, and contribution to the data commons? How are they defined and enforced?
- Do rules/licences related to data access and use have a corresponding set of accountability measures (e.g. privately reaching out, publicly naming and shaming, going to court)? (Ruhaak et al. 2021).
- What are the possible violations of the rule? (Ruhaak et al. 2021).
- Is there a code of conduct that is used as a baseline to impose sanctions (e.g. signed by all the actors joining)? What are the sanctions for not applying the Code?
- Are there sanctions for not applying the FAIR principles?
- Do rules related to data security and integrity have a corresponding set of accountability measures? (Ruhaak et al. 2021).
- Do funding and spending rules have a corresponding set of accountability measures? (Ruhaak et al. 2021).
- Are there mechanisms in place to ensure that actors understand the rules and accountability measures? (Ruhaak et al. 2021).
- Are there mechanisms in place to ensure that accountability measures are fair and proportional? (Ruhaak et al. 2021).
- Are there mechanisms in place to ensure actors can re-earn trust from the community? (Ruhaak et al. 2021).

Principle 6: Conflict-resolution mechanisms.

- How are conflicts within the data ecosystem managed?
- Are there internal mechanisms in place to resolve conflict? Including conflict that does not violate an existing rule (Ruhaak et al. 2021).
- Are there formal (external) conflict resolution mechanisms in place?
    - How rapid are they?
    - How costly?
    - Is there agreement about when you fall back on formal legal systems? (Ruhaak et al. 2021).
- Are conflict resolution mechanisms easily accessible by all stakeholders? Are there mechanisms in place to ensure stakeholders raise complaints and grievances? (Ruhaak et al. 2021).
- Is there a procedure to appeal decisions made (especially around sanctions)? (Ruhaak et al. 2021).

Principle 7. Minimal recognition of rights to organise.

- Is the data ecosystem (the sharing and reuse) supported/legitimated by external entities (e.g., government institutions or other institutional actors)? (Ruhaak et al. 2021).
- Is the sharing and collaboration within the ecosystem in any way regulated by formal regulations? How?
- Is the organisation compliant with external regulations and laws?

Principle 8. Nested enterprises.

- Is the data ecosystem nested or part of any overarching ecosystems and collaborative initiatives, explicitly or implicitly?
- How do all the other principles work between the layers (provision, monitoring, enforcement, conflict resolution, and governance)?
- Is the coordination between layers effective?
- Is it clear how the initiative interoperates with larger systems or other data commons? (Ruhaak et al. 2021)

Annex 4. Case survey for Section 2.5

The case survey aimed to synthesise evidence from four cases (see Table A) using a combination of convenience and purposeful sampling to get a representative set with different yet overlapping characteristics. One of the researchers, Johan Linåker, had existing knowledge from earlier research on most of the cases, which has helped data collection and cross-case analysis.

Table A – Brief description of the four cases

Case	Description	Main data source
Trafiklab	Swedish national data ecosystem founded in 2011. Facilitates data sharing on public transport data between public transport authorities and private transport operators. Governed through Samtrafiken, a legal entity co-owned by the public and private actors.	Previously reported on in Linåker & Runeson (2022) with prolonged engagement on one of the authors.
HSL DevCom	Finnish regional data ecosystem founded in 2009. Facilitates data sharing on public transport data between municipal public transport authorities in the Helsinki region. Governed through HSL, a legal entity co-owned by 9 municipalities	Previously reported on in Linåker & Runeson (2022) with prolonged engagement on one of the authors.
OpenStreetMap	An international data ecosystem founded in 2004. It has already been defined as a Data Commons. Facilitates data sharing on a common world map. Constituted by branches of subcommunities of individuals collaboratively mapping down to a local level. Governed through a decentralised structure on consensus norms and peer-review.	Thoroughly reported on in several studies, with rich online documentation available. Context knowledge by both authors.
Mobilidata	In the Mobilidata programme in Flanders governments, companies, and researchers work together to bring technological traffic solutions to road users (e.g. travel directions, traffic alerts tailored to specific routes and lights turning green quicker at intelligent traffic lights).	The information comes from a desk-based survey, the programme website, and an email interview with one of its representatives.