DELPHI

FeDerated nEtwork of pLatforms for Passenger and freigHt Intermodality

Grant Agreement Number: 101104263

D.2.5: Methodology framework for secure, safe and efficient data sharing/storage/usage

Document Identification			
Status	Final	**Due Date**	Tuesday, 31 December 2024
Version	1.0	**Submission Date**	23/12/2024
Related WP	WP2	**Document Reference**	D.2.5
Related Deliverable(s)	D2.4, D2.5, D2.1	**Dissemination Level**	PU
Lead Participant	eBOS	**Document Type:**	R
Contributors	Mihai Hulea (NTTD), Manos Barmpounakis (MbL), Marion Cottet (ALICE)	**Lead Author**	Kyriaki Psara (eBOS)
		Reviewers	Mihai Hulea (NTTD)
			Vasilis Agouridas (AUM)

Funded by the European Union

DELPHI project has received funding under grant agreement No 101104263. It is 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 Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.

Document Information

Author(s) – in alphabetical order		
First Name	**Last Name**	**Partner**
Kyriaki	Psara	eBOS
Marion	Cottet	ALICE
Mihai	Hulea	NTTD
Thanasis	Christofides	eBOS

Document History			
Version	**Date**	**Modified by**	**Modification reason**
0.1	30/08/2024	Thanasis Christofides (eBOS)	ToC Created
0.2	20/10/2024	Kyriaki Psara (eBOS)	1st draft input
0.3	8/11/2024	Mihai Hulea (NTTD)	1st round of inputs
0.4	15/11/2024	Kyriaki Psara (eBOS)	Updates in structure
0.5	29/11/2024	Marion Cottet (ALICE)	Final Input
0.6	16/12/2024	Mihai Hulea (NTTD)	Peer review
0.7	17/12/2024	Vasilis Agouridas (AUM)	Peer review
0.8	20/12/2024	George Agapiou (WINGS)	Quality Assurance review
1.0	23/12/2024	Kyriaki Psara (eBOS)	Final version to be submitted

Quality Control		
Role	**Who (Partner short name)**	**Approval Date**
Deliverable leader	EBOS	03/10/2024
Quality manager	WINGS	20/12/2024
Project Coordinator	ICCS	23/12/2024

Executive Summary

The DELPHI project aims to create a secure, interoperable data-sharing ecosystem for multi-modal transport systems. By addressing the challenges of fragmented data governance and interoperability, DELPHI supports collaboration among stakeholders, including transport operators, public authorities, and technology providers.

This deliverable, D2.5 “Methodological Framework for Secure, Safe, and Efficient Data Sharing”, presents a comprehensive framework to guide secure and effective data exchanges within the DELPHI platform. The framework ensures compliance with EU regulations, supports data sovereignty, and promotes interoperability across diverse stakeholders. It builds on the insights from prior deliverables, D2.1, which provided a state-of-the-art analysis of governance models and stakeholder ecosystems, and D2.4, which outlined user requirements, services, and stakeholder needs for data sharing and digitalisation of information flows.

The content of this deliverable includes:

- A Methodological Framework: A structured approach to enable secure, safe, and efficient data sharing among mobility and logistics stakeholders. It integrates best practices from industry and research to ensure robust governance and technical standards.

- Guidelines for Secure, Safe, and Efficient Data Sharing: Practical measures for data security, integrity, and efficiency, including access controls, encryption, validation protocols, and optimisation strategies to support seamless operations.

- Regulatory Recommendations: Guidance on meeting EU regulatory standards. These recommendations ensure legal alignment and reinforce trust among participants in the federated ecosystem.

- Governance Structure: A neutral and impartial governance model defining roles, processes, and entities required to manage data sharing securely and transparently.

Table of Contents

Executive Summary **3**

1. Introduction **8**

1.1 Purpose of the document 8

1.2 Intended readership 8

1.3 Document Structure 8

2. Background on Relevant Methodologies **10**

2.1 Frameworks 10

2.2 Standards 12

2.3 Concepts 14

2.4 Initiatives 15

2.5 Methodologies 19

2.6 Governance Models 22

3. DELPHI Methodological Framework for Secure, Safe, and Efficient Data Sharing **31**

3.1 The DELPHI Platform 31

1.1 Objectives of the Framework 33

4. Guidelines for Secure, Safe, and Efficient Data Sharing **36**

5.1 Data Security 36

5.2 Data Safety 37

5.3 Efficient Data Use 38

5. Regulatory Framework Recommendations **39**

6. Neutral Governance Structure **43**

6.1 Governance Roles 43

6.2 Governance Bodies 44

6.3 Governance Legal Entity 45

6.4 Governance Processes 46

7. Conclusions **48**

References **49**

List of Tables

Table 1: Mapping of Standards and Regulatory Frameworks to DELPHI Data Governance and Security Requirements.....39

List of Figures

Figure 1: Gaia-X Ecosystem Visualisation 22
Figure 2: Fenix Design Principles and Governance 24
Figure 3: Design Principles for Data Spaces 25
Figure 4: IDS-RAM Reference Architecture Model 27
Figure 5: eFTI Architecture and its Main Components 28
Figure 6: PEPPOL four-corner model 30
Figure 7: Objectives of the Methodological Framework 34
Figure 8: Guidelines for Data Management 36
Figure 9:Governance Legal Entity Responsibilities 45

Abbreviations & Acronyms

Abbreviation / acronym	Description
DELPHI	FeDerated nEtwork of pLatforms for Passenger and freigHt Intermodality
GAIA-X	European project for creating data spaces through trusted platforms and federated infrastructure
IDSA	International Data Spaces Association
ISO/IEC	International Organisation for Standardisation / International Electrotechnical Commission
GDPR	General Data Protection Regulation
NIST	National Institute of Standards and Technology
CIS	Center for Internet Security
SOC 2	Service Organisation Control 2
EMDS	European Mobility Data Space
MaaS	Mobility as a Service
ADASIS	Advanced Driver Assistance Systems Interface Specifications
DTLF	Digital Transport Logistics Forum
FENIX	Federated Network of European Transport Information eXchange
DCAT	Data Catalog Vocabulary
iSHARE	International Secure Handling of Authenticated Resources Exchange
eFTI	Electronic Freight Transport Information
SDL	Shared Data Language
OWASP	Open Web Application Security Project
ITIL	Information Technology Infrastructure Library
DMBOK	DAMA Data Management Body of Knowledge
PEPPOL	Pan-European Public Procurement OnLine
EFTI4EU	European Electronic Freight Transport Information for EU
SD-WAN	Software-Defined Wide Area Network
PIMS	Privacy Information Management System

1. Introduction

1.1 Purpose of the document

An increasing number of logistic companies are beginning to adopt new business models, where platforms represent one of the most important economic and social development tools. These businesses are using platforms to deliver services by exploiting best practices and digital strategies to remain competitive. However, due to the increased connectivity and technological innovations, various systems, such as transport management systems, terminal operation systems, port community systems and many others, some of which are newcomers (e.g. drones), require extensive and complex information exchanges.

There is a lack of interoperability at the technical, semantic, and business levels, which requires the creation of a community ecosystem and deploying bilateral solutions to share data. As a result, the different actors in the logistics chain started collaborating and deploying their own data platforms, aiming to alleviate these ad-hoc one-to-one collaborations in a highly fragmented market.

To support this transition, policies and guidelines are implemented to govern and protect the data collected by these platforms. In this sense, data governance refers to the practices and rules to monitor the community's behaviour by exchanging data to avoid potential misuse and to streamline efficient business operations.

This deliverable outlines the methodological framework of DELPHI for secure, safe, and efficient data sharing and management between different mobility providers in multi-modal transport systems. This deliverable aims to set the foundation of DELPHI data governance, which aims to develop federated solutions for integrated freight and passenger transport systems.

1.2 Intended readership

The intended readership of this deliverable is for project stakeholders, including policymakers, transport operators, and technology providers. The consortium partners also benefit from these deliverables since they aim to guide them through managing diverse data through recommendations and guidelines of already existing data governance frameworks and regulations. This deliverable guides understanding the frameworks, methodologies and governance structures proposed to ensure secure and efficient data exchange in the DELPHI platform.

1.3 Document Structure

The document is structured to provide detailed research of the existing governance frameworks and methodologies required for secure and efficient data sharing and management. Following the introductory Section 1, Section 2 provides an overview of

relevant knowledge on data governance, including frameworks, standards, concepts, initiatives, and methodologies. This section is the cornerstone of the deliverable, providing data governance knowledge from similar initiatives and projects as input, which will then be tailored to the needs of the DELPHI project. Following, we have Section 3, which introduces the DELPHI Methodological Framework for Secure, Safe, and Efficient Data Sharing based on the DELPHI platform architecture, requirements, and information model. Section 4 provides the guidelines for secure, safe, and efficient data sharing and offers detailed strategies and methodologies for achieving these criteria. Regulatory framework recommendations are presented in Section 5, which addresses compliance with EU standards. Section 6 presents the neutral governance structure of DELPHI, which explores various data governance mechanisms. Finally, Section 7 summarises the findings and highlights the significance of the proposed.

2. Background on Relevant Methodologies

This section covers the most related frameworks, standards, concepts, and initiatives that can be used as guidance to make data-sharing practices in DELPHI more secure, safe, and efficient. These frameworks ensure data security and operational efficiency in mobility as a service (MaaS) and, therefore, serve as a guide for designing a federated platform like DELPHI. The following sections explore how several well-established frameworks provide the foundations for secure and efficient data management, which can inspire the DELPHI solution.

In the frame of this deliverable and overall, of the work conducted in DEPHI's WP2 on *Governance, Regulatory and Stakeholder Analysis*, ALICE has worked with Geodis and Mines Paris Tech's expert group on Physical Internet to map as exhaustively as possible the landscape of initiatives linked to secure, safe and efficient data sharing/storage/usage at European level. Conducted by Jean Delaplace during his internship at ALICE, his work has been summarised in a document "Digitalisation of the logistics: Cartography of the data sharing and exchange initiatives in Europe and recommendations for the introduction of the "Shared Data Language" developed by Geodis into this landscape" and extracts of this report are included as part of this deliverable D2.5.

2.1 Frameworks

This section presents frameworks that establish best practices for secure, safe, and efficient data usage. These frameworks aim to offer data integrity, trust, and security within systems like the DELPHI platform while ensuring compliance with various standards and regulations.

1. NIST Cybersecurity Framework (CSF)[1]

The National Institute of Standards and Technology (NIST) provides a set of cybersecurity best practices and recommendations that offer a systematic method for dealing with cyber threats. This framework recommends methods such as identification, protection, detection, response, and recovery from threats to address cyber risks. It can be used as an all-encompassing strategy for safeguarding data and data-related infrastructure within a multi-modal transport environment.

[1] https://www.nist.gov/cyberframework

2. CIS Critical Security Controls[2]

The CIS Critical Security Controls provide a set of prioritised controls that enhance cybersecurity by ensuring secure data exchanges across stakeholders. These controls focus on data integrity, secure endpoints, threat monitoring, and threat responses. By implementing these actions in multi-modal systems, vulnerabilities can be reduced, and the system's overall security can be improved.

3. Zero Trust Architecture[3]

Zero Trust Architecture is a cybersecurity approach based on zero trust principles, which assume that no user or system can be trusted inside or outside the network. To prevent data breaches, this approach limits exposure to unauthorised users by requiring continuous device and user authentication. In federated platforms of multi-modal transport systems where multiple users or systems can access shared data, this approach can be adopted to ensure that each interaction is authenticated and authorised.

4. Blockchain [4]

Blockchain technology is a decentralised, distributed and public digital ledger that can be used to ensure data integrity and trust in multi-modal transport systems. Blockchain is blocks of data linked into an uneditable digital chain. This makes data transactions traceable and immutable, which, as a result, enhances data sovereignty and security for multi-stakeholder data exchanges.

5. Shared data language[5]

The Shared Data language aims to provide a universal framework for exchanging data between entities in a logistics chain. It consists of a data model aiming at covering the logistics processes that are common to all transport modes, a communication protocol relying on a decentralised infrastructure and APIs, and security and identification specifications. The Shared Data Language (SDL) is a framework developed by GEODIS (French Logistics Service Provider). The SDL consists of an overarching data language that describes commonalities between logistics processes, from contracting and ordering to traceability. Ultimately, it aims at being combinable with core dataspaces components (e.g. connector) and other existing frameworks. Since 2020, GEODIS has

[2] https://www.cisecurity.org/controls
[3] https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
[4] https://www.ibm.com/topics/blockchain
[5] https://internationaldataspaces.org/semantic-interoperability-a-common-language-for-data-sharing/

been progressively implementing the SDL in its local branches to achieve interoperability for the group's operations.

6. Intelligent Transport Systems (ITS) Directive [6]

A new Directive (Directive (EU) 2023/2661) amending the ITS Directive was adopted on 22 November 2023, with the aim to adapt to the emergence of new road mobility options, mobility apps and connected and automated mobility. The objective is to stimulate the faster deployment of new, intelligent services, by proposing that certain crucial road, travel and traffic data is made available in digital format, such as speed limits, traffic circulation plans or roadworks. It will also ensure that essential safety-related services are made available for drivers along the TEN-T network. The directive is supported by five co-operating Directorates-General: DG Mobility and Transport (lead), DG Communications Networks, Content & Technology, DG Research & Innovation, DG Enterprise and Industry and DG Climate Action.

7. European Mobility Data Space (EMDS) [7]

The European Mobility Data Space (EMDS) initiative aims to accelerate the digital and green transformation of the European mobility and transport sector by creating a secure and interoperable data-sharing environment. EMDS can serve as a foundational framework that provides data sovereignty, interoperability, and trust standards that allow mobility providers to employ cross-border data exchange across Europe. This initiative ensures compliance with EU regulations while promoting data sharing seamlessly and securely in a federated and secure manner.

2.2 Standards

Data-related standards provide a set of rules that apply secure data practices and regulatory compliance across multiple platforms. The DELPHI framework will adopt standards that are necessary for secure data exchanges, interoperability, and data protection.

1. Information Security Management (ISO/IEC 27001)[8]

ISO/IEC 27001 is a standard used for creating an Information Security Management System (ISMS), which is used to ensure that all data-related processes maintain data confidentiality, integrity, and availability and thus are protected from cyber threats. By following the guidelines of ISO/IEC 27001, transport and logistics organisations can

[6] https://transport.ec.europa.eu/transport-themes/smart-mobility/road/its-directive-and-action-plan_en
[7] https://deployemds.eu/
[8] https://www.iso.org/standard/27001

manage information security risks, which ensures the protection of personal data, financial information, and trade secrets in transport and logistics.

2. General Data Protection Regulation (GDPR)[9]

The General Data Protection Regulation is a European Union legal framework on information privacy in the European Union and the European Economic Area, which guides how personal data is stored, processed, and shared. Since DELPHI handles personal data in multi-modal transport systems, strict privacy rules should be set, especially for passenger information. As such, compliance with GDPR ensures that obtaining, storing, or processing personal and operational information and their respective rights are protected across Europe.

3. Service Organisation Control 2 (SOC 2)[10]

SOC 2 is a cybersecurity compliance framework developed by the American Institute of Certified Public Accountants (AICPA) dedicated to managing data security in cloud environments, which guides systems on how to store and process client data in a secure manner. SOC 2 presents the security, availability, and privacy requirements which can be used for auditing and monitoring cloud-based and distributed services in terms of data security.

4. Data Quality (ISO 8000)[11]

ISO 8000 is an international standard that provides guidelines for data quality regarding accuracy, integrity, and consistency. These guidelines define the features and the requirements for the standard exchange of Master Data among business partners such as logistics and transport stakeholders. This data exchange is done in a reliable and trustworthy manner, which can benefit businesses by enhancing decision-making and operational efficiency.

5. Privacy Information Management (ISO/IEC 27701)[12]

ISO/IEC 27701 specifies the requirements and guidelines for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS). This international standard for information security focuses on privacy management by helping organisations manage privacy controls to reduce the risk to the privacy rights of individuals. Since federated data

[9] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[10] https://www.aicpa-cima.com/resources/download/see-what-service-organization-management-needs-to-know-about-soc-2-r
[11] https://www.iso.org/obp/ui/#iso:std:iso:8000:-1:ed-1:v1:en
[12] https://www.iso.org/standard/71670.html

spaces aim to protect personal data privacy, this standard can assist in guaranteeing data sovereignty and securing the handling of personal information.

2.3 Concepts

This section outlines foundational concepts that are essential for effective data governance and secure, efficient data sharing in multi-modal transport. These concepts comprise of best practices for managing IT services and data, as well as innovative methods for enhancing data security, privacy, and interoperability. They can be used as valuable techniques that guide platforms like DELPHI in establishing a secure and compliant data governance.

1. Information Technology Infrastructure Library (ITIL)[13]

The ITIL framework, a guide for best practices in IT service management, was developed by the UK government in 1989. The ITIL is widely adopted across industries as guidance and best practice for managing the five stages of the IT service lifecycle: service strategy, service design, service transition, service operation and continual service improvement. ITIL is a systematic approach to IT service delivery consisting of 34 practices under the categories of general, service, and technical management practices.

2. DAMA Data Management Body of Knowledge (DMBOK)[14]

DAMA International develops the DMBOK as a comprehensive guide for data management. This guide describes the challenges of data management and how to resolve them by defining guiding principles within data management functional areas. It is a functional framework for best data governance and management practices, methods and techniques. The latest edition, DMBOK2, plays a critical role in the certification of Certified Data Management Professionals (CDMP), establishing a shared vocabulary for data management concepts and serving as the basis for best practices for anyone working in data management.

3. Zero-knowledge proof[15]

A zero-knowledge proof is a protocol that allows one party (the prover) to convince another party (the verifier) that some given statement is true without revealing the fact itself. In cryptography, ZKP is a powerful method that enhances privacy and security.

---

[13] https://www.ibm.com/topics/it-infrastructure-library#:~:text=ITIL%20stands%20for%20Information%20Technology,practices%20in%20IT%20service%20management.

[14] https://www.dama.org/cpages/body-of-knowledge

[15] https://www.nttdata.com/global/en/insights/focus/what-is-zero-knowledge-proof#:~:text=In%20general%2C%20a%20zero%2Dknowledge,%2Dknowledge%20(Table%201).

This technology can verify the validity of a statement without exposing sensitive, valuable information in systems requiring verification without disclosure of sensitive data.

4. Mobility as a Service (MaaS)[16]

Mobility as a Service allows users to plan, book, and pay for different mobility services using a single combined platform. Integrating various transport options services, such as public transport, taxis, bike-sharing, and more, into a single service achieves intermodal travel. The foundation of this system is secure and transparent data sharing, which promotes collaboration between public authorities and private operators. MaaS relies on APIs and open data standards, fair data sharing, compliance with privacy regulations, user transparency, data anonymisation and consent to accomplish this.

2.4 Initiatives

Several initiatives in the European Union share similarities or main objectives with the DELPHI project, which aims to create a federated platform architecture. These initiatives were studied and reviewed to provide the basis for the governance model for DELPH.

1. GAIA-X[17]

GAIA-X is a collaboration between Germany and France that was launched in 2019 to establish a digital governance that can be applied to any existing cloud/ edge technology stack. This ensures a secure, next-generation data infrastructure for Europe, emphasising digital sovereignty and innovation. The governance structure of GAIA-X distinguishes between legal, service, and technical layers, creating an ecosystem where data and services can be securely shared between service providers and consumers.

2. International Data Spaces Association (IDSA)[18]

International Data Spaces Association is a not-for-profit association working towards establishing a trusted data-sharing framework across industries that allows participants complete control over their data. IDSA promotes an open, vendor-neutral architecture of user-driven governance and certification, which could influence DELPHI's approach to trust and security in data sharing.

[16] https://urban-mobility-observatory.transport.ec.europa.eu/document/download/6b706858-11c6-41c2-b9f7-466e2bec0499_en?filename=maas_and_sustainable_urban_mobility_planning.pdf
[17] https://gaia-x.eu/
[18] https://www.idsociety.org/

3. FENIX[19]

The FENIX project aims to create a European federated architecture to support developing, validating, and deploying digital information systems along the EU transport Core Network. Its governance structure ensures interoperability between stakeholders in the European logistics community, such as shippers, logistics service providers, mobility infrastructure providers, cities, and authorities.

4. iSHARE[20]

iSHARE is a non-profit organisation that removes barriers to data sharing in the logistics and transport sectors. This is achieved by providing and maintaining a Trust Framework for data spaces offering secure identification, authentication, and authorisation. This agreement-based system facilitates data sovereignty and trust, allowing stakeholders to share data quickly and securely.

5. Advanced Driver Assistance Systems Interface Specifications (ADASIS)[21]

ADASIS is an initiative created by an open group of prominent organisations from the global vehicle industry who joined forces to define the ADAS Interface. This initiative develops interface standards for sharing data between vehicle systems and external services. This initiative focuses on enabling ADAS applications to be provided with data from maps, on building predictive and vehicle environment data based on geo-referenced data, on providing the industry with a de-facto standard, on contributing as one enabling technology to the development and deployment of all Automated Driving.

6. SENSORIS[22]

The SENSORIS is an innovation platform of actors committed to standardising vehicle sensor data exchange between vehicles and external services. The aim is to define this global standardised interface that supports real-time traffic information and enhances location-based services, resulting in new services and increased business opportunities.

7. Traveller Information Services Association (TISA)[23]

TISA is an international membership-driven association connecting stakeholders to develop and maintain standards, software, and traffic and travel information tools. TISA standards support collaboration between public and private entities to ensure

[19] https://fenix-network.eu/
[20] https://framework.ishare.eu/
[21] https://adasis.org/
[22] https://sensoris.org/
[23] https://tisa.org/

worldwide seamless traffic, travel services, and interoperability. TISA offers new business opportunities to all public and private stakeholders in the Intelligent Transport System (ITS) value chain by facilitating networking with other organisations sharing the same goal. Seamless traffic and travel services are provided using TISA standards, guaranteeing interoperability worldwide and reducing organisation costs.

8. OpenPEPPOL[24]

PEPPOL is a large-scale pilot project financed by the European Commission to enable frictionless trade between private and public sector bodies. The Peppol eDelivery network provides a decentralised open network that uses a common data standard, enabling digital invoices and other procurement documents to be exchanged between suppliers and buyers. The OpenPEPPOL framework features a central coordinating authority and delegated authorities at the local level.

9. FEDERATED[25]

The FEDeRATED project is an initiative funded by the European Union to enable digital logistics cooperation. It involves multiple EU member states and aims to allow all law enforcement agencies to access pull-based data value and added services. The project focuses on developing federated data-sharing models by maximising logistics and supply chain visibility, optimising asset use, and making digital technology accessible to all operators while enabling them to create new services.

10. EFTI4EU[26]

eFTI4EU is a cooperation of a pan-European consortium of 23 partners focused on developing the Electronic Freight Transport Information (eFTI) architecture. The project aims to create a unified approach to the operation of eFTI Gates and implement a reference architecture for exchanging transport and logistics data. A significant outcome of the eFTI4EU project is the creation of the EU Regulation 2020/1056, funded under the Connecting Europe Facility (CEF) program. EFTI4EU is a project that develops a well-harmonised and interoperable European-wide eFTI exchange environment.

11. Open Web Application Security Project (OWASP)[27]

The Open Worldwide Application Security Project is an online community that provides guidelines and best practices such as articles, methodologies, documentation, tools, and technologies for securing web applications. Specifically, OWASP aims to protect

[24] https://peppol.org/
[25] https://www.tno.nl/en/newsroom/insights/2022/08/federated-project-digital-co-operation/
[26] https://efti4eu.eu/
[27] https://owasp.org/

against critical vulnerabilities such as insecure authentication and security attacks. OWASP's guidelines and best practices can be used in transport and logistics to strengthen platform resilience and protect web-based services from common security risks.

12. Digital Transport Logistics Forum (DTLF)[28]

The Digital Transport Logistics Forum (DTLF) is an expert group, composed of both public and private stakeholders, that assists the European Commission in the implementation of eFTI regulations and in developing frameworks for interoperability in the Transport & Logistics sector. It is composed of three subgroups dedicated to thematic: Paperless Transport, Corridor Freight Information System, and Electronic Freight Transport Information (eFTI) Delegated Act. Concepts developed by DTLF are deployed by initiatives FEDERATED and FENIX.

13. Shared data language[29]

The Shared Data Language (SDL) is a framework developed by GEODIS (French Logistics Service Provider). The SDL consists of an overarching data language that describes commonalities between logistics processes, from contracting and ordering to traceability. Ultimately, it aims at being combinable to core dataspaces components (e.g. connector) and other existing frameworks. Since 2020, GEODIS has been progressively implementing the SDL in its local branches to achieve interoperability for the group's operations.

14. Data Act [30]

Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data. The Data Act aims to maximise the value of data in the economy by ensuring that a wider range of stakeholders gain control over their data and that more data is available for innovative use, while preserving incentives to invest in data generation.

15. Data Governance Act [31]

A European Data Governance Act, which is fully in line with EU values and principles, will bring significant benefits to EU citizens and companies. A key pillar of the European strategy for data, the Data Governance Act seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles

[28] https://transport.ec.europa.eu/transport-themes/digital-transport-and-logistics-forum-dtlf_en
[29] https://www.etp-logistics.eu/wp-content/uploads/2024/05/ALICE-data-sharing-discussion-paper_V0.6_0205024_1.pdf
[30] https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

[31] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

to the reuse of data. The Data Governance Act will also support the setup and development of Common European Data Spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills. The Data Governance Act entered into force on 23 June 2022 and, following a 15-month grace period, is applicable since September 2023.

16. Cybersecurity Act [32]

The Cybersecurity Act, which incorporates the NIS2 Directive, establishes EU-wide legislation aimed at ensuring a high standard of cybersecurity across the Union. It amends Regulation (EU) No 910/2014 to strengthen the resilience of critical infrastructure, improve risk management practices, and enhance cooperation among member states in addressing cybersecurity threats.

2.5 Methodologies

This section presents the methodologies that allow the optimisation of data efficiency for secure and efficient data sharing, storage, and usage. The DELPHI project aims to enable effective, seamless multi-modal transport environments. These methodologies enable coordinated data exchange among traffic participants to provide a seamless and efficient data exchange mechanism.

1. Data Transfer Protocol Optimisation

Data Transfer Protocol Optimisation [1] optimises transfer protocols, such as HTTP/2, gRPC, to ensure minimal latency and overhead. This optimisation can be achieved through data flow analysis, compressing payloads, minimising handshake processes, and using caching mechanisms for repeated requests. This, as a result, boosts speed and reduces bandwidth consumption.

2. Data Caching

Data caching [2] is a process that stores multiple copies of data in a temporary storage location so they can be accessed faster. Optimising data caching strategies, such as distributed and edge caching, allows data to be stored frequently and accessed closer to the data consumer. This reduces network load and improves latency since the cache memory can be accessed quickly in cases when the system would otherwise need to query centralised databases or distant services repeatedly.

[32] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

3. Network Infrastructure Optimisation

Advanced network optimisation [3] techniques are data-driven processes that enhance network performance and efficiency. These include techniques like traffic shaping, load balancing, bandwidth management, and Software-Defined Wide Area Networks (SD-WAN), which ensure that data packets are transmitted through the most efficient routes across different network segments. This is achieved by measuring performance metrics and then making strategic changes to optimise network resources, which as a result minimises latency and improves data transmission resilience.

4. Efficient Data Formats

Data formats [4] are used as a common language that allows data to be interpreted correctly by different systems. Employing common data formats, such as JSON, Protocol Buffers, or CBOR establishes a common approach on how information should be structured, represented, and manipulated. This allows businesses to ensure compatibility and interoperability between diverse technologies whilst reducing their data footprint during transmission and storage.

5. Database Optimisation

Database optimisation [5] involves tuning databases through indexing and query optimisation to maximise the speed and efficiency with which data is retrieved. Optimising system performance through diverse methods ensures high availability and speed when accessing large datasets across federated platforms.

6. Data Quality

Data quality [6] measures how well a dataset meets the criteria for qualitative or quantitative pieces of information. Data is considered high quality if it is accurate, complete, valid, consistent, unique, and timeless. Data quality is maintained through validation, cleansing, and governance procedures which result in having consistent, accurate, and usable data across platforms.

7. High-Performance Storage

High-performance storage [7] is a management system designed to deliver exceptional data transfer rates, low latency, and high throughput. This system moves large amounts of complex data across the network while ensuring exceptional data transfer rates, low latency, and high throughput. These systems are optimised for demanding workloads, such as scientific research, high-performance computing, big-data analytics, and enterprise applications. It leverages technologies like Storage Area Networks (SAN), Solid-State Drives (SSDs), and Non-Volatile Memory (NVM) to provide fast and reliable access to data.

8. Asynchronous Data Sharing

Asynchronous data sharing [8], involves producers sending data to the receivers independently, improving performance and scalability. In synchronous data transfer the sending and receiving parties do not need to interact in real-time. One of the characteristics of asynchronous sharing is that data can be transmitted, stored, and then accessed by the recipient at their convenience, independent of the sender's timing. This technique is usually used in systems where live data exchange is not required, but on the other hand, network latency or system availability can affect direct communication.

9. Data Access Patterns Optimisation

Data access patterns [9] refer to the mechanisms used for managing, retrieving and storing data effectively. Optimising access patterns is crucial as it can significantly influence performance, data usage efficiency, reliability, and scalability. Data access patterns depend on the frequency of data retrieval, which ensures a balanced load across the database system.

10. Infrastructure Scalability

Infrastructure scaling [10] means changing the size and power of a system to accommodate changes in demands and workloads without compromising performance, efficiency, or cost. Scalable infrastructure allows the system to dynamically allocate resources so that a system can easily adapt and grow to support high-availability architectures.

11. Performance Monitoring and Tuning

Continuous system monitoring involves checking various system metrics to ensure that bottlenecks are quickly identified and resolved. Adjusting system parameters and configurations through automated tuning solutions [11] can improve performance.

12. Compute Continuum/edge and cloud

Edge-to-cloud architectures can seamlessly integrate edge computing with cloud services, forming a continuum [12] of distributed computing and network infrastructure management. In this continuum, data can flow seamlessly between the cloud and the edge, allowing for data processing and more intensive computations in the cloud. This methodology offers the option between an edge-only computing platform or a multi-cloud computing platform to meet performance, security, and cost efficiencies.

2.6 Governance Models

This section provides an overview of data governance models that are related to federated platforms like DELPHI. These models comprise a set of principles that leverages people, processes, and technology to define how data is collected, stored, managed and used within a system.

1. GAIA-X

Gaia-X is a European initiative that enables and boosts the creation of data spaces through trusted platforms as a federated infrastructure. All participating platforms comply with common rules focusing on data sovereignty and interoperability. GAIA-X employs strict governance structures that allow participants to trust each other to safely and freely share and exchange data thus fostering innovation.

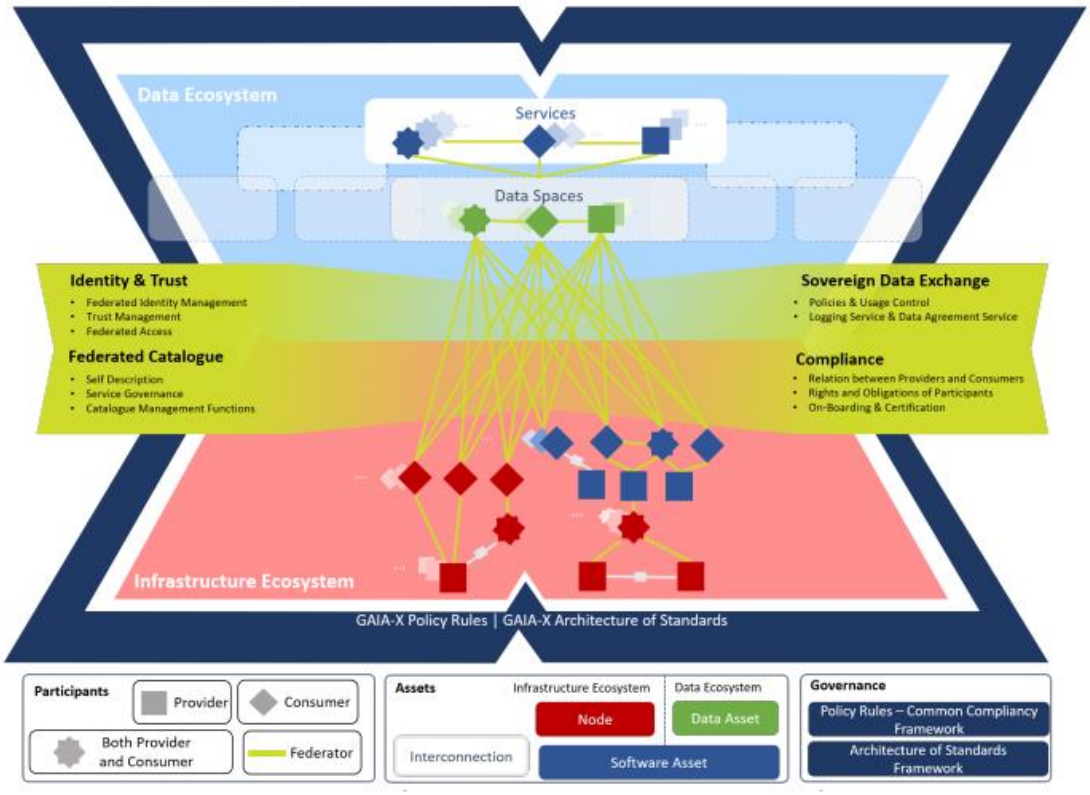

Figure 1: Gaia-X Ecosystem Visualisation[33]

The Trust Framework proposes rules to ensure shared governance and basic levels of interoperability across individual ecosystems while allowing users to control their

[33] https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf

choices fully. In Gaia-X, identity, access management, compliance services, and self-descriptions enforce trust while safeguarding data protection, transparency, and security. The Gaia-X Architecture defines a multi-layered governance model which includes the following Federated services:

- **Identity and trust:** Participants create user profiles, sharing information about their business, their data, and their service offerings that can be verified by others in the Federation.
- **Federation Catalogue:** The federation catalogue serves as a repository for one Federation, where participants can find other participants. This alleviates the lack of trust in the current data storage, sharing, and handling landscape, facilitating ecosystem interoperability.
- **Data Sovereignty:** Data owners retain sovereignty over their data by offering services that can create transparency and maintain complete control. Distributed Ledger Technologies (DLT) facilitate contract negotiations and traceable and transparent data transactions.
- **Compliance:** Gaia-X verifies compliance for shared services to help assess whether participants adhere to Gaia-X principles. This is done through compliance checks during a new participant's onboarding and ongoing monitoring.

2. FENIX

FENIX is a European project that provides the first European federated architecture serving the European logistics community with interoperability between any individual existing and future platforms. The FENIX governance structure provides a set of roles and procedures needed to become part of the FENIX ecosystem. This model ensures stakeholders adhere to the agreed-upon FENIX requirements that ensure a trusted, interoperable, and high-quality data exchange.

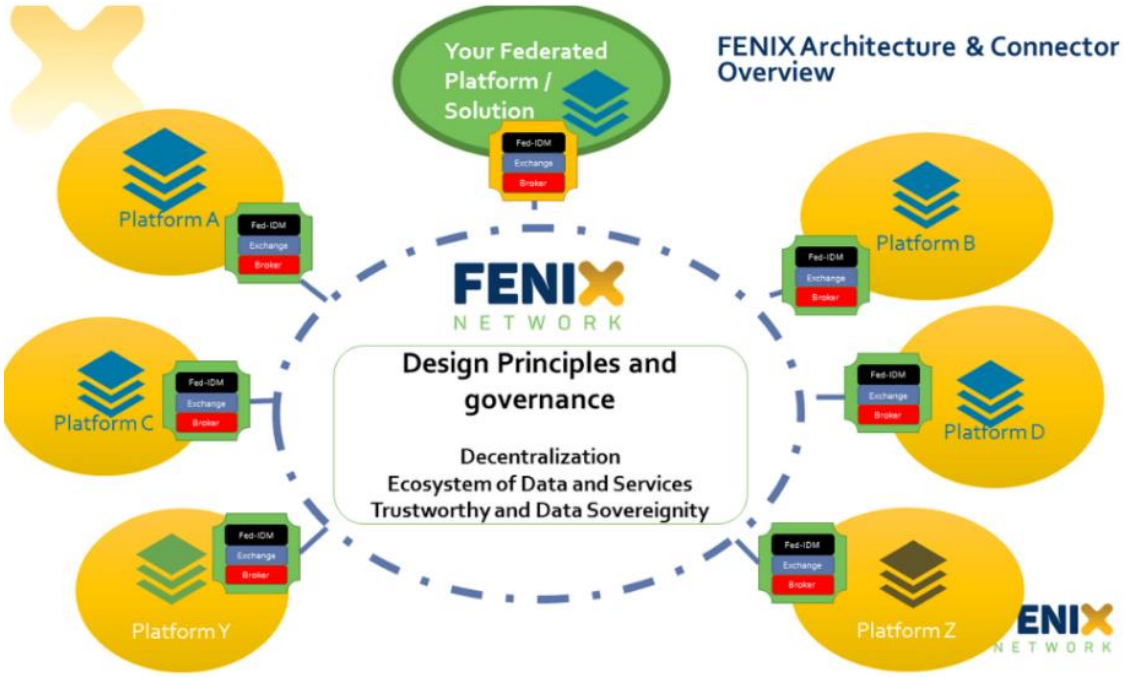

Figure 2: Fenix Design Principles and Governance[34]

FENIX focuses on securely sharing logistics and transport data across a network of platforms [13]. Its governance structure emphasises:

- **Decentralised Data Governance:** FENIX uses decentralised governance principles, where participants are considered network nodes and always retain their internal control. This means all data remains local while being shared securely across the network using secure APIs and trusted intermediaries.
- **Trustworthy and Data Sovereignty:** The FENIX architecture provides technical solutions and governance models to ensure trust between the network participants through smart contracts and auditable transactions.
- **Ecosystem of Data and Services:** FENIX composes a network of platforms where data assets and services are made available for secured consumption or sharing via the federated network. Stakeholders can communicate using legally binding agreements with their platform providers, who are responsible for following data-sharing rules and compliance

3. iSHARE

The iSHARE Foundation provides and maintains a Trust Framework for data sharing, enabling federated trust governance of data spaces. Data Sovereignty and Trust is

[34] https://erticonetwork.com/presenting-innovations-in-logistics-to-the-australian-government-with-fenix-and-aeolix/

facilitated by standardised identification, authentication, and authorisation protocols. The iSHARE model focuses on data sovereignty, allowing data owners to control access and usage.

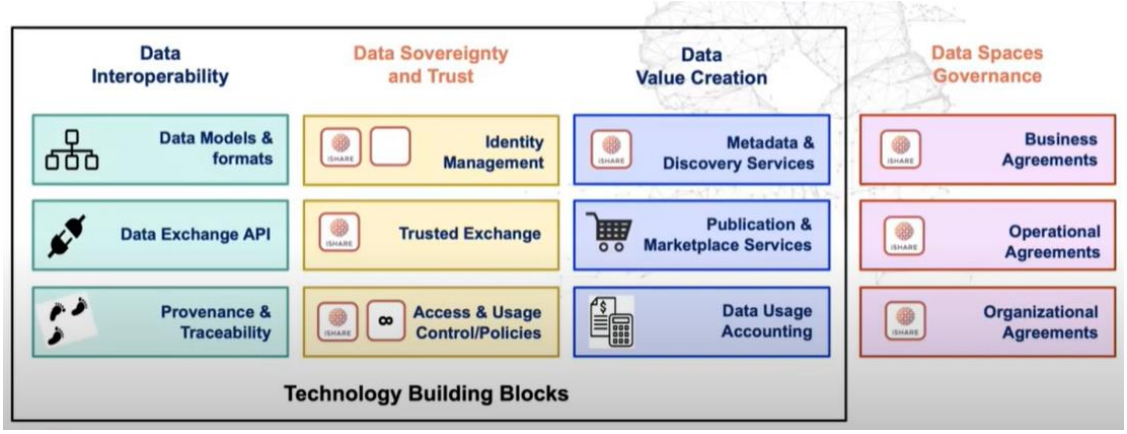

Figure 3: Design Principles for Data Spaces[35]

The iSHARE trust framework [14] focuses on secure identification, authentication, and authorisation for data sharing. Key technical elements include:

- **Identification:** Identification is the action or process of identifying something by presenting characteristics called identity attributes. The identity provider and identity broker roles facilitate identification. The identity provider provides identifiers and credentials, manages authorisation records, identifies something based on credentials, checks permissions, and confirms powers. On the other hand, the identity broker supports multiple identity providers by allowing people to select identity providers they prefer to authenticate themselves.

- **Authentication:** Authentication is the process of determining whether something is what is claiming to be by validating with the right credentials, such as a username, e-mail address, etc. Authentication can be used alone or in combination of something the entity knows, something the entity possesses, something the entity is, something the entity does, and something about the context of the entity.

- **Authorisation:** Authorisation is giving permission to access services, data, or other functionalities. Authentication enables authorisation, where specific policies determine what types of access rights an entity is permitted. This process is facilitated by the authorisation registry, which manages records of

[35] https://www.youtube.com/watch?v=-lCy_ckrY0U&ab_channel=iSHARE

authorisation, checks the registered permissions, and confirms the established powers

4. International Data Spaces Association (IDSA)

IDSA defines a reference architecture model defines the roles and information model for data spaces that allow data providers retain control over their data, even after it is shared with other parties. This is achieved through the following:

- **Role Model:** The reference architecture serves as a blueprint of the ethical and design principles that ensures all participants adhere to high standards for security and data governance
- **Data Sovereignty:** Data owners in IDSA maintain control over data usage, including defining and enforcing policies on data access, usage, and sharing, rather than passing to large data exchange platforms. The framework enforces usage control at the data layer, ensuring data cannot be used outside the agreed terms.
- **Information Model:** The information model is agnostic and open regarding domains and technologies, ensuring data exchange within the ecosystem while preserving data sovereignty.
- **Usage Policy Enforcement:** The framework is a basis for technically enforced agreements for data sharing in combination with already existing contracts

The IDS Reference Architecture Model (IDS-RAM) [15] provides a structured framework for enabling secure and sovereign data exchange between organisations within a data space. IDS-RAM comprises of five layers and the three perspectives, each addressing different components and aspects of the IDS.

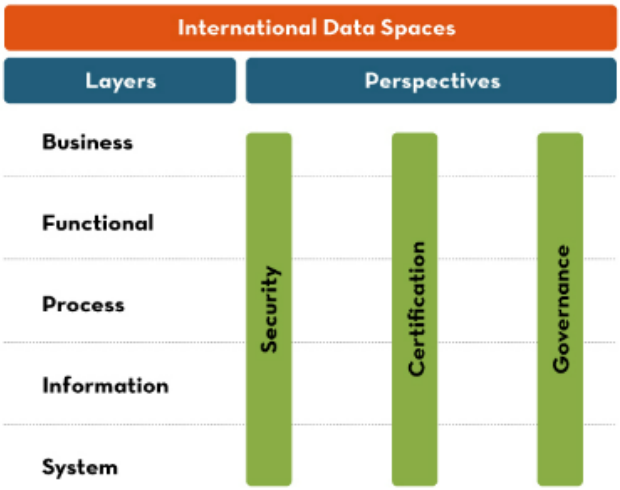

Figure 4: IDS-RAM Reference Architecture Model[36]

- **Business Layer:** This layer defines and categorises the rules and policies governing data sharing between participants. This layer also establishes the different roles of the participants and the basic patterns of interaction taking place between these roles.
- **Functional Layer:** The Functional Layer specifies the functional requirements, and the features to be implemented within the data space. It includes requirements related to trust, security and data sovereignty, an ecosystem of data, standardised interoperability, value adding apps, and data markets
- **Information Layer:** This layer specifies the information model of the International Data Spaces, including a common language, standardising data formats, and semantic interoperability. The Information Model is a common agreement shared between different systems, platforms, and stakeholders of the IDS, facilitating compatibility and interoperability.
- **Process Layer:** The Process Layer specifies the processes and workflows taking place between the different components of the IDS. It provides a dynamic view of the Reference Architecture Model focusing on facilitating secure and efficient data sharing in terms of onboarding, data offering, contract negotiation, exchanging data, publishing and using data apps.
- **System Layer:** The System Layer maps, the roles specified on the Business Layer and the processes defined in the Process Layer onto a concrete data and service

[36] https://datos.gob.es/en/blog/ids-ram-reference-architecture-model-and-its-role-data-spaces

architecture. These constitute the technical infrastructure that supports secure and efficient data exchanges, resulting in what can be considered the technical core of the International Data Spaces.

5. Electronic Freight Transport Information (eFTI4EU)

The eFTI4EU project is particularly relevant because it deals directly with freight transport information, which aligns with DELPHI's focus on freight and passenger transport services. Its governance model ensures compliance with EU regulations on electronic freight information and provides a framework for secure, interoperable, and standardised data sharing across the logistics sector. This model is vital for ensuring DELPHI's platform can handle freight data in compliance with legal requirements.

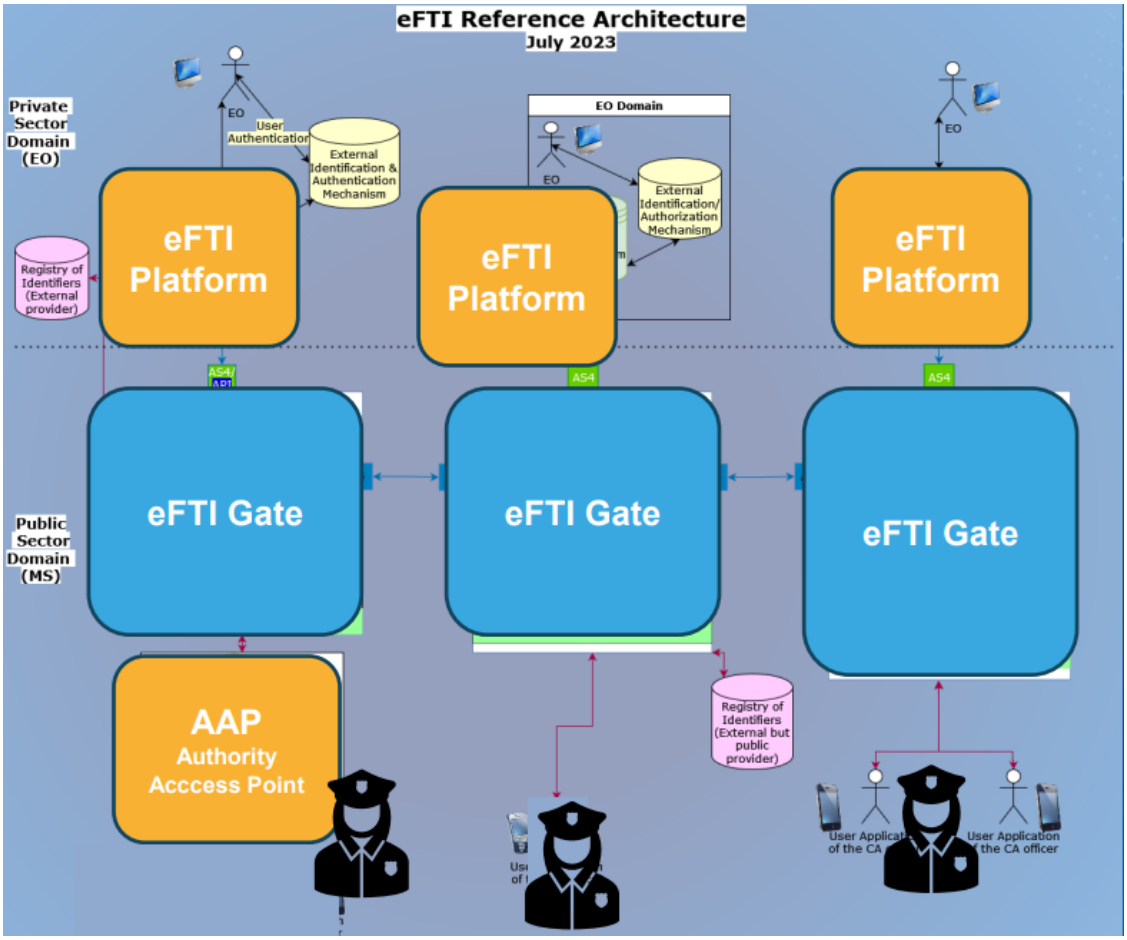

Figure 5: eFTI Architecture and its Main Components[37]

[37] https://efti4eu.eu/wp-content/uploads/2024/04/eFTI4EU-Project_Proteger2024.pdf

Its governance model focuses on the secure freight information exchange between authorities, logistics providers, and operators across Europe.

- **Data Compliance:** EFTI4EU provides a governance framework that ensures compliance with the EFTI regulation, allowing public authorities to accept electronic freight transport information, resulting in a uniform implementation of the obligatory acceptance by authorities.
- **Cross-border Interoperability:** EFTI4EU promotes IT systems and solutions interoperability between European Union member states. This is achieved through a well-harmonised and interoperable European-wide eFTI exchange environment that uses common data models and standardised protocols.
- **Security and Privacy:** The eFTI system adheres to the data protection regulations set by the European union to ensure security and privacy of sensitive documents and data. The EFI certified platform uses data encryption and access controls to store, validate, and process freight information and provides secure access to the information to authorised parties

6. OpenPEPPOL

OpenPEPPOL [16] offers a governance framework for cross-border data sharing with a strong emphasis on interoperability and security in public-private partnerships. This model is highly applicable to DELPHI's need to facilitate seamless data exchanges across different countries and systems in transport and logistics, ensuring data integrity and compliance with various regulations.

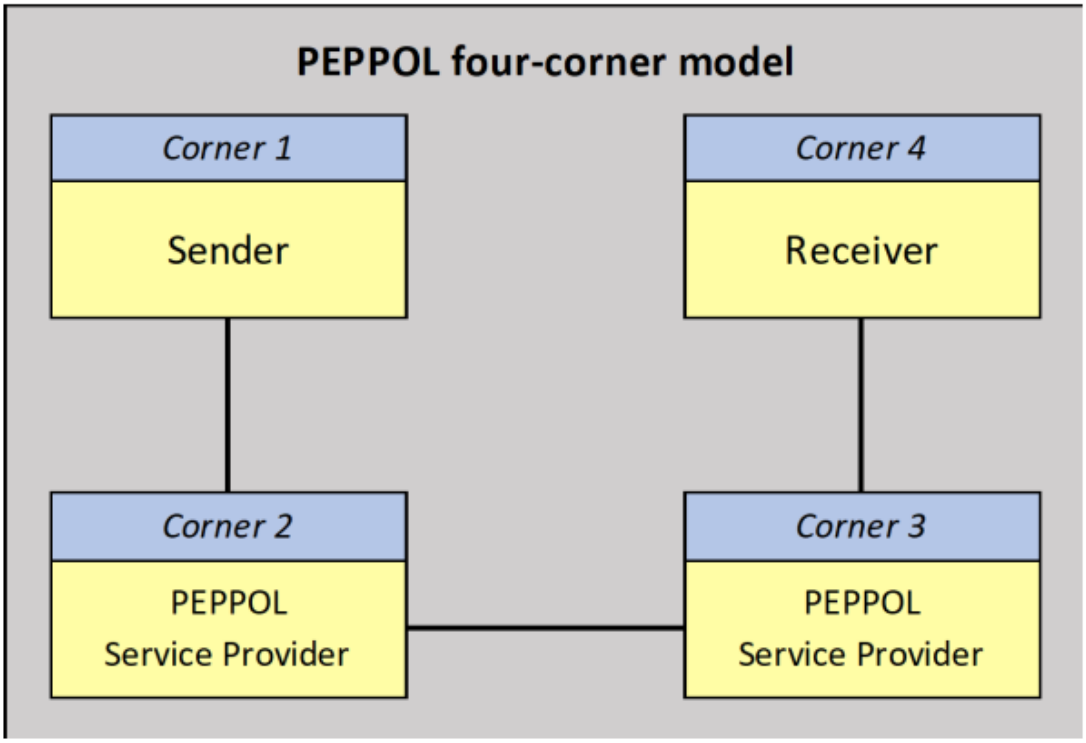

Figure 6: PEPPOL four-corner model[38]

OpenPEPPOL provides a governance framework for a cross-border e-procurement network. Its governance structure includes:

1. **Coordinated and Delegated Authorities:** OpenPEPPOL divides governance among, OpenPEPPOL AISBL which is responsible strategic, sustainable and development governance, the PEPPOL Authorities which are responsible for thePEPPOL eDelivery Network and PEPPOL Business Interoperability Specifications (BIS), and the Service providers which are responsible for delivery of services to PEPPOL End Users.

2. **Four-Corner Model:** OpenPEPPOL's technical model enables businesses to communicate electronically by ensuring that both senders and receivers can choose independently their access points

[38] https://www.gs1.org/sites/default/files/openpeppol_gs1_standards_conference_2019-09-10.pdf

3. DELPHI Methodological Framework for Secure, Safe, and Efficient Data Sharing

The Methodological Framework for Secure, Safe, and Efficient Data Sharing in the DELPHI project is a structured approach to facilitate trustworthy and compliant data exchanges among stakeholders within multi-modal transport networks. This framework provides the necessary guidelines, principles, and technologies to ensure data sharing across transport and logistics providers remains secure, interoperable, and efficient while aligning with EU regulatory requirements.

3.1The DELPHI Platform

The DELPHI platform handles secure, safe, and efficient data-sharing among multiple mobility providers. This section introduces how the platform will integrate data security, safety, and efficiency measures to support seamless transport operations while safeguarding sensitive information.

Deliverable D2.3 provides the high-level multilevel governance requirements, spreading beyond strict focus on data governance, and identifies new potential stakeholders and sources of socio-political processes and information needed for the deployment of the DELPHI solution that can have ultimately and impact on the DELPHI's data governance framework.

Deliverable D2.4 focuses on analysing and specifying the requirements and services necessary for the implementation of the DELPHI solution. It provides an assessment of the current (As-Is) and envisioned future (To-Be) models of urban transportation and logistics systems aligned with project and use cases objectives. The deliverable introduces the "Delphi Town" concept, which serves as a hypothetical model for seamless multimodal urban transportation, incorporating both passenger mobility and freight logistics.

The work began with the development of the DELPHI Town concept, which serves as a framework for defining integrated multimodal transportation services. Within this concept, five key business cases were identified:

1. Consolidated network and traffic management - featuring services for network updates, authority confirmations, and real-time traffic monitoring
2. Multimodal transportation for passengers - including services for trip planning, execution, charging, and disruption management
3. Multimodal urban logistics - comprising services for route identification, logistics execution, and unified charging

4. Multimodal transport optimisation - offering services for demand prediction, traffic forecasting, and disruption prediction

5. Federated data sharing - providing services for data registration, access control, and consumption

Analysis was then conducted for four pilot locations (Madrid, Athens, Mykonos, and Cluj-Napoca), documenting their current ("As-Is") transportation systems and envisioning future ("To-Be") states. For each pilot, relevant DELPHI Town services were mapped to their specific needs. The mapping revealed distinct focus areas:

- Madrid's focus on metro integration for urban logistics
- Athens' emphasis on tollway and metro system integration
- Mykonos' addressing of seasonal transportation challenges
- Cluj-Napoca's concentration on digital service integration

Based on this mapping and the defined services, a set of user requirements was developed. These requirements were categorised by business case and prioritised (Required, Recommended, Optional) to guide implementation. This approach ensures that the technical solutions developed in later project phases will address actual user needs. Below is presented a summary of requirements categorised by business.

Consolidated Network and Traffic Management
The requirements here focus on capabilities necessary for network and traffic management functionalities, with a focus on ensuring secure access, effective communication, and real-time updates across the DELPHI platform. The system supports user authentication and authorisation for transport operators, enabling them to access the platform and manage network objects securely. Key functionalities include mechanisms for user confirmation and authorisation of network updates, as well as an approval workflow to notify and seek validation from relevant authorities before changes are implemented.

Multimodal Transportation for Passengers
The requirements here focus on providing an integrated travel experience for passengers across multiple transport modes, including public transportation and bike-sharing. Important features include user registration, destination input, and route suggestions based on real-time data. The system also supports service reservations and alternative travel options when transport modes are unavailable. In terms of journey management, integrated ticketing and real-time journey updates are supported, as well as payment processing and disruption management with alternative route suggestions.

Multimodal Urban Logistics
For urban logistics, requirements include facilitating efficient multimodal routes by gathering shipment information, analysing transportation options, and generating optimised routes. Key logistics features like tracking shipments, coordinating

multimodal transfers, and notifying users about in-transit adjustments ensure a smooth flow of goods across urban areas. Additional requirements for charging and invoicing cover the aggregation of service charges, cost optimisation, and payment processing.

Multimodal Transport Optimisation
These requirements centre on data integration for forecasting traffic, predicting demand, and managing disruptions. The system enables data integration from multiple sources, setting custom analysis parameters, and selecting AI/ML models for predicting transportation disruptions. Requirements also address the need for displaying analysis results on an interactive dashboard and collecting user feedback to improve model performance.

Federated Data Sharing
In federated data sharing, the requirements focus on cataloguing data, managing access, and providing a marketplace for data exchange. Essential functions include data registration, ownership, access control, and contract enforcement to ensure data security. Additional requirements for transaction management and data-sharing notifications support secure data transactions and provide data providers with usage transparency.

1.1 Objectives of the Framework

DELPHI's methodological framework aims to establish secure, efficient, and safe data sharing among multi-modal transport providers and platforms. The DELPHI project covers optimisations across product and freight flows in supply chains which require interoperability among diverse transport services and stakeholders. Thus, the framework utilises a federated, technology-neutral approach that aims to ensure data security, safety, and compliance with EU regulations. The following list presents the objectives of the framework:

Figure 7: Objectives of the Methodological Framework

1. To Ensure Data Sovereignty

The framework focuses on data sovereignty, which allows providers to have clear control over their data throughout their lifecycle within the DELPHI ecosystem. Inspired by GAIA-X and IDSA principles, it allows data providers to monitor access and set permissions in a way that enforces data access policies consistently across the platform. This allows data owners to share data confidently and assures them that they have control over how their data is used and with whom it is shared.

2. To Support Compliance

Assuring the DELPHI platform participants have trust and regulatory alignment can be achieved by complying with several EU standards, such as GDPR and ISO/IEC 27001. The DELPHI framework integrates all necessary standards to ensure that any data handling practices such as collection, transmission, storage, deletion and sharing comply with legal and regulatory requirements for privacy, security, and data integrity. This compliance could be evaluated through compliance audits and certification processes, which in turn can create a legally sound, trustworthy and ethically responsible data-sharing ecosystem.

3. To Enhance Interoperability

Due to the nature of the project, interoperability is essential for enabling multi-modal transport where passenger and freight data flow across different systems. To achieve integrated, responsive, and efficient transport services across different stakeholders and transport modes, a unified data ecosystem should be created where data can be

exchanged seamlessly enables. This interoperability is achieved by establishing standard data models, APIs, and protocols that allow various independent systems to communicate and share data effectively.

4. To Maintain Data Quality

Since reliable data is essential for effective decision-making and operational efficiency, one of the framework's objectives is to ensure the quality and accuracy of data across the platform. Data validation protocols can be utilised to check for data accuracy and integrity before the data is shared or stored within the platform. For example, redundancy reduction mechanisms can be used to prevent accumulating outdated or inaccurate data. Such mechanisms minimise risks related to erroneous or incomplete data and therefore enhance the overall trustworthiness of the platform.

5. To Promote Trust

Federated transport platforms such as DELPHI that enable a collaborative data-sharing ecosystem that requires trust and transparency. To ensure this DELPHI adopts a transparent data governance structure, including participant roles, processes and governance bodies, to promote accountability in line with the findings of D2.3. Certification processes can verify that each participant adheres to the platform's governance processes and data protection standards. Additionally, audit trails can provide a record of data exchanges, allowing stakeholders to verify data origin.

4. Guidelines for Secure, Safe, and Efficient Data Sharing

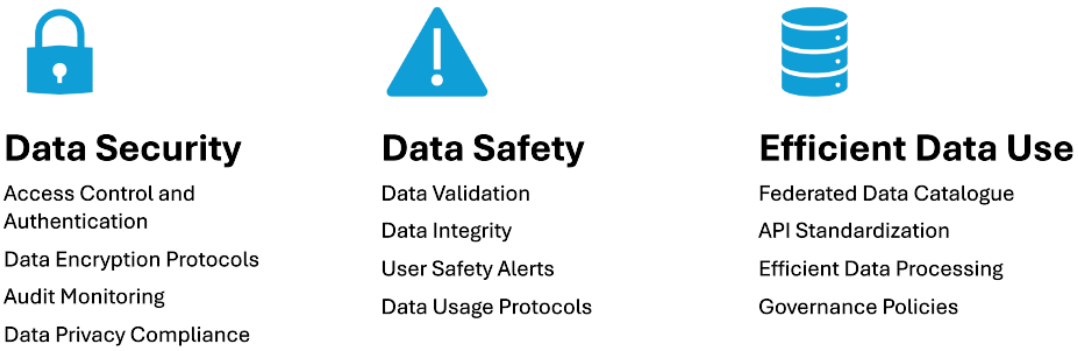

Figure 8: Guidelines for Data Management

This section presents how the platform will assure data security, safety, and efficiency to support transport operations while safeguarding sensitive information. Following, several methodologies are presented that can be within the DELPHI platform:

5.1 Data Security

Data security is foundational for federated data sharing when it comes to sensitive information exchanges. The DELPHI project can implement a multi-layered security strategy to protect data throughout its lifecycle, from sharing to storage and usage.

Access Control and Authentication:

DELPHI could implement Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) across all platform participants. These mechanisms restrict data access to authorised users/systems based on their permissions. Standard frameworks like OAuth2 are used to oversee API access and therefore provide additional protection for data exchanges.

Data Encryption Protocols:

Enforcing end-to-end encryption for data in transit secures data exchanges among mobility providers. High-grade encryption protocols like AES-256 could be applied to sensitive information, including passenger data and logistics tracking, aligning with GDPR and other privacy standards.

Audit Monitoring:

Audit logging can be used for all access and data-sharing activities to enhance transparency and accountability. Adhering to ISO 27001 standards allows continuous monitoring and automated alerts to quickly detect and respond to unauthorised or unusual activities.

Data Privacy Compliance:

DELPHI should adhere to GDPR and other regulatory requirements to protect user privacy. This could be achieved by incorporating data anonymisation when data is shared for analytical purposes and using consent mechanisms when user trust is needed.

5.2 Data Safety

Data safety in a federated environment like DELPHI is essential to protect stakeholders from data risks. DELPHI can implement the following data safety measures to maintain the reliability of shared data.

Data Validation:

DELPHI could deploy data validation protocols to verify that incoming data from each source is consistent, accurate, and complete, especially in time-sensitive applications like transport and logistics planning. Using tools to standardise and clean data before processing can help reduce the risks associated with erroneous data.

Data Integrity:

Implementing data integrity mechanisms such as data entry controls, data encryption, and data quality checks will allow DELPHI to protect against data corruption. Additionally, data streams such as traffic or logistics can benefit from failover and redundancy strategies during system interruptions.

User Safety Alerts:

Integrating real-time alert systems in the DELPHI platform enables users to receive prompt notifications about data-related disruptions that may affect services, such as traffic blockages or delays. Notifying end-users promptly about inconsistencies or safety concerns will enable quick responses, supporting reliable data usage.

Data Usage Protocols:

DELPHI should identify and document the data usage protocols used in the platform, such as HTTP, SSL, IMPA, SMTP etc. These protocols prioritise end-user safety by covering data sharing, storage, and usage guidelines across stakeholder interactions.

5.3 Efficient Data Use

Data efficiency ensures the DELPHI platform operates smoothly with optimised data storage, transfer, processing, and energy usage. The DELPHI federated platform can adopt strategies for efficient data use to optimise data resources across multiple platforms and transport providers.

Federated Data Catalogue:

A federated data catalogue system allows each participant to maintain its metadata repository. Applying standards like the Data Catalog Vocabulary (DCAT), these catalogues can enable standardised metadata description, allowing users to search for and retrieve metadata across distributed nodes without creating a central point of dependency. Adopting federated catalogues achieves efficient data discovery and retrieval, minimises redundancy, and respects data sovereignty and decentralisation principles.

API Standardisation:

DELPHI could use standardised APIs to enable interoperability and streamline data access across mobility platforms. Load balancing and caching mechanisms within these APIs could manage high-volume requests more efficiently by using tracking usage metrics that optimise API availability according to demand patterns.

Efficient Data Processing:

DELPHI can reduce the need for repetitive raw data analysis by using advanced AI/ML algorithms for data pre-processing and predictive analytics. Employing data deduplication and compression mechanisms will help minimise storage needs, costs and data access speeds for large datasets.

Governance Policies:

DELPHI should define a data governance structure (Section 6) to formalise data-sharing policies across federated platforms. This includes automating data-sharing agreements and providing traceability and accountability across stakeholders to ensure that data use remains efficient, transparent, and aligned with DELPHI's stakeholder expectations as defined in D2.3.

5. Regulatory Framework Recommendations

To make sure that the DELPHI platform meets the necessary legal, security, and privacy standards, the following section presents regulatory framework recommendations that integrate specific regulations. This section outlines key areas such as data sovereignty, privacy compliance, security, auditability, standardisation, data quality, smart contracts, and governance. For each area, we highlight specific standards and practices relevant to achieving DELPHI's objectives.

Table 1: Mapping of Standards and Regulatory Frameworks to DELPHI Data Governance and Security Requirements

Standards and Frameworks for DELPHI Governance		
Aspect	**Standard/Regulation**	**Implementation**
Data Sovereignty	GDPR, ISO/IEC 27701	Usage policies, data control
Data Privacy	GDPR	Consent Management, transparency
Data Security	ISO/IEC 27001, NIST CSF	Risk assessment, access controls
Auditability	SOC 2, ISO 27001 MMAE	Compliance monitoring, alerts
Data Standardisation	EMDS, JSON/XML Standards	Interoperability, data brokers
Data Quality	ISO 8000, EMDS Guidelines	Accuracy, timeliness validation
Smart Contracts	GAIA-X, IDS-RAM	Policy enforcement automation
Data Governance	GAIA-X Principles, ISO/IEC 27701	Governance roles, committees

1. Data Sovereignty

The following standards establish strict data sovereignty controls, allowing data owners to retain control over their data even post-sharing:

- Enforcing GDPR ensures that data owners can define specific **data usage policies**, such as usage restrictions for their personal data. GDPR guidelines allow data owners to set terms for accessing, processing, and deleting personal data.
- ISO/IEC 27701 “Privacy Information Management” sets **privacy controls** to manage personal data, including users' rights to data alterations and deletions.

Specifically, it suggests structured data usage policies that align with privacy regulations.

2. Data Privacy Compliance

Compliance with GDPR for data privacy is a necessity when handling personal data in transport and logistics services:

- GDPR requires obtaining user **consent**, ensuring transparency about how personal data is used within a platform. Consent management tools give users clear options to grant or revoke consent for data processing.
- GDPR **rights**, such as data access and deletion, allow data owners to have control over their personal information.

3. Data Security Standards

To protect data across DELPHI's federated platform, the framework should incorporate data security standards, which establish strong security baselines:

- Developing an **Information Security Management System (ISMS)** aligned with ISO/IEC 27001 mandates regular risk assessments, access controls, and incident response procedures which as a result protects data integrity and confidentiality.
- The NIST Cybersecurity Framework can be used for **risk management** to identify and recover from cybersecurity attacks. A federated platform with multiple stakeholders such as DELPHI requires establishing secure endpoints and continuous threat monitoring.

2. Auditability

Continuous auditing and monitoring standards can be used to ensure compliance with security and privacy regulations:

- SOC 2 is a standard for the **compliance of cloud service organisations**, and it specifies how organisations should manage customer data. Platforms with cloud-based services can use this standard to meet security, availability, and confidentiality criteria.
- MMAE is a process in ISO 27001 for monitoring, measuring, analysing and evaluating the performance of an information security management system. **Continuous monitoring** in line with ISO 27001, could include automated alerts for unauthorised access attempts and breaches.

3. Data Standardisation

The European mobility data space (EMDS) provides guidelines for the data shared across the European transport sector to be interoperable, secure, and compliant with EU regulations:

- Using standardised **data formats** (e.g., JSON, XML) and EMDS-compliant protocols across transport and logistics platforms can ensure compatibility with the EMDS framework.
- **Federated data** brokers, as specified by IDS and EMDS, ensure that metadata is catalogued correctly and that data providers can control how their data is discovered and accessed within the DELPHI ecosystem.

4. Data Quality

For data quality and reliability and operational efficiency, data need to be complete and accurate, which is a crucial foundation for building data trust across DELPHI:

- As part of **data quality management**, all data shared could meet ISO 8000 guidelines for accuracy, consistency, and completeness. As a result, this means that the data are fit for analytics and to good quality standards, enhancing the reliability of decision-making processes.
- As part of **data quality compliance**, the EMDS guidelines can be enforced to ensure data accuracy, completeness, validity, consistency, uniqueness, timeliness, and fitness for purpose. This ensures that shared data have no inconsistencies that could disrupt multi-modal transport services.

5. Smart Contracts

Smart contracts are utilised to automate the execution of a data-sharing agreement so that all participants can immediately obtain the outcome without any intermediary's involvement or time loss. As highlighted in D2.3, the adoption of smart contracts is also important for the delegation and execution of operational responsibilities among stakeholders:

- Adhere to GAIA-X's **smart contract principles** of using automated contracts to enforce agreed-upon enforceable data-related rights and obligations. These include duration, processing restrictions, and permitted applications, which ensures that all exchanges are compliant without manual oversight.
- IDS-RAM's enforcement of data usage restrictions (**policy enforcement**) automatically triggers compliance alerts or policy-based actions when terms are breached.

6. Data Governance

Structured governance sets internal data policies that apply to how data is collected, stored, processed, and deleted, which is critical for maintaining accountability and compliance within a federated platform like DELPHI:

- ISO/IEC 27701 can be used to define roles and responsibilities related to **privacy governance**. Designate roles can be defined to oversee privacy compliance and maintain accountability for managing personal data.
- Using the GAIA-X **governance principles** to establish a governance committee allows data platforms to handle cross-stakeholder issues, update data policies, and ensure compliance with regulatory requirements. This is also in line with D2.3, where effective arbitration mechanisms in multilevel governance schemes were identified for addressing conflicts arising from diverse stakeholder interests.

6. Neutral Governance Structure

Data governance structures are designed to create a secure, transparent, and efficient data-sharing environment across data sharing ecosystems. Specifically, this structure is an organised framework designed to manage, control, and standardise data management procedures within a platform. To design this structure specific rules, roles and processes need to be defined in order to be able to ensure that data are managed securely, consistently, in compliance, and in alignment for its intended purposes. The term "neutral" ensures that the structure is designed in a way that it functions impartially where no single participant or stakeholder has influence over the platform. The following lust presents the main characteristics of a neutral data governance structure:

- The structure should be able to prevent any single from affecting decision-making processes in order for all parties to have equal opportunities.
- A neutral governance body provides impartial oversight which encourages trust and fairness among participants.
- A neutral entity oversees compliance across the board, ensuring that all participants adhere to data protection, security, and interoperability standards. As highlighted in D2.3, arbitration mechanisms are critical for resolving disputes and ensuring fairness across different stakeholder interests.
- A neutral governance structure enables unbiased conflict resolution in cases of disputes or compliance issues, which enables balanced relationships between participants.
- The structure enforces governance rules which ensure that each participant retains control over their data according to agreed-upon policies.

6.1 Governance Roles

The governance structure of DELPHI is organised into distinct roles with specific responsibilities to ensure accountability and oversight within the platform. By considering the project carefully to identify tailored roles suitable to the project's needs and objectives, the following roles were defined:

1. Data Owner

The Data Owner has complete control of its data by setting the rules for data access and usage and therefore retaining data sovereignty. This entity has complete control over data assets and, therefore, is able to ensure transparency and ownership rights.

2. Data Consumer

Data consumers are able to access and utilise data following the permissions established by data owners. They are accountable for adhering to governance guidelines, data accuracy, and agreed-upon terms.

3. Data Space Provider

This role provides the technical foundations for data sharing, data storage, transfer protocols, and interoperability. Within DELPHI, Data Space Providers work to ensure that data exchange processes meet governance standards for security and compliance.

4. Federated Identity Manager

This entity is responsible for identity verification and access control thus supporting secure data exchanges within DELPHI. This role manages identity attributes and access tokens for secure data access across federated participants.

5. Trust Broker

The Trust Broker verifies if participants comply with security standards before allowing them access to DELPHI's data-sharing environment. This role additionally maintains participant certifications and manages trust levels.

6.2 Governance Bodies

The governance bodies are the enablers for implementing and maintaining data governance standards within the DELPHI data-sharing framework. These entities guarantee that policies, compliance, and processes are managed effectively to facilitate secure and compliant data exchanges within the platform. The following list presents the main governance bodies in DELPHI:

1. Oversight Committee

This committee oversees DELPHI's data governance policies to make sure that data management remains aligned with security, compliance, and trust standards. The committee reviews operations and updates policies in response to changes in governance needs. As discussed in D2.3, the committee can also establish clear arbitration processes to mediate disputes, ensuring fair conflict resolution and maintaining balanced relationships among stakeholders on the system.

2. Technical Governance Committee

This committee is responsible for managing technical standards by making sure that all data security protocols, such as encryption and access control, are implemented effectively across DELPHI. It also supervises interoperability and integration within the data spaces framework.

3. Certification Body

This is an independent body that verifies if all participants meet DELPHI's data security and compliance standards. As part of its responsibilities, this body conducts audits as part of a certification process that guarantees that only verified entities can join the data-sharing ecosystem.

6.3 Governance Legal Entity

Within the DELPHI governance framework, the governance legal entity is responsible for enforcing data-sharing policies and managing compliance for all participants. This legal entity is an impartial body that enforces policies, maintains compliance, and ensures that data-sharing activities are secure, transparent, and legally compliant. This entity is structured as an independent, neutral organisation to maintain transparency and impartiality. In line with the discussion in D2.3, the governance legal entity also addresses the need for effective arbitration mechanisms, ensuring that any disputes arising between participants are handled fairly and efficiently, thereby reinforcing the integrity of the governance framework.

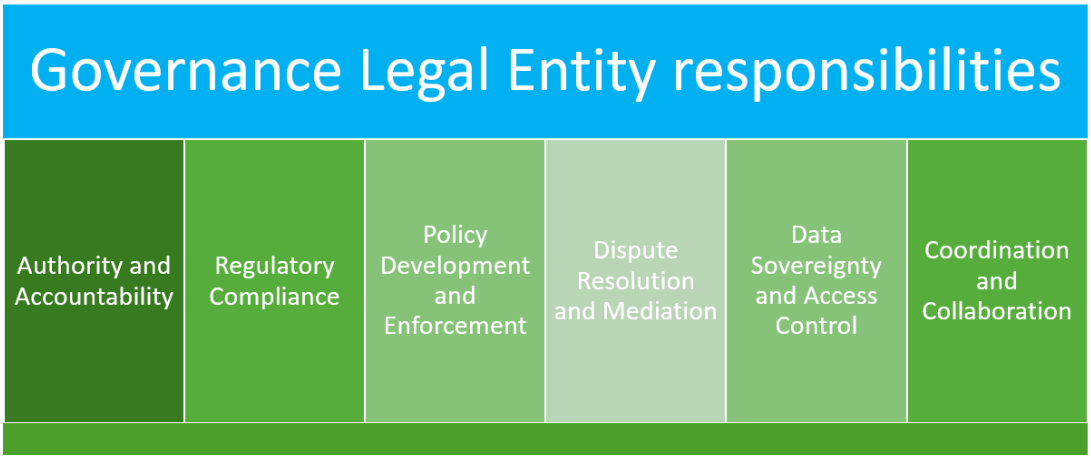

Figure 9:Governance Legal Entity Responsibilities

The following are some of the responsibilities of the Legal Entity:

1. Authority and Accountability

The legal entity provides formal authority to enforce the governance framework, by defining roles and processes for all participants.

2. Regulatory Compliance

This body ensures compliance with regulations (e.g., GDPR), regularly updates policies and conducts audits to align with evolving standards.

3. Policy Development and Enforcement

The entity creates and enforces data sharing, access, and security policies and makes sure that all stakeholders adhere to the related standards.

4. Dispute Resolution and Mediation

The legal entity, as a neutral authority, is responsible for providing structured dispute management which as a result resolves conflicts and fosters trust.

5. Certification and Trust

Following ongoing compliance checks, the entity certifies participants that meet security standards as a way of maintaining network trustworthiness.

6. Data Sovereignty and Access Control

The role of this entity is to enforce data sovereignty principles by ensuring that data owners retain control over access permissions and usage policies.

7. Coordination and Collaboration

As a coordinating body, it facilitates cross-platform collaboration, interoperability, and secure participant data sharing.

6.4 Governance Processes

In the DELPHI data governance framework, governance processes are used to enforce policies, compliance, and accountability within the data-sharing ecosystem. The following list presents the core governance processes applied in the framework:

1. Policy Enforcement:

The governance body defines clear policies to guide participants that cover data ownership rights, security measures, and compliance with regulatory standards. Enforcement mechanisms ensure that all platform users adhere to these rules and resolve any policy violations on data sharing, access, and usage.

2. Compliance Monitoring:

Compliance monitoring through regular audits is conducted to verify that all participants in the platform meet the required security and regulatory standards.

As part of these checks, monitoring of data access and usage logs should be conducted to ensure transparency, accountability, and trustworthiness.

3. Dispute Resolution:

To address any disagreements or issues arising from data access, use, or compliance requires an impartial process for handling conflicts. The governance legal entity manages these processes as a way of ensuring fair and unbiased resolution of disputes.

4. Certification:

The framework includes a certification process that verifies if participants meet the platform's data-sharing and security requirements. Through ongoing audits, the participants become certified Cas away from maintaining their trusted status within the ecosystem.

7. Conclusions

This deliverable establishes a comprehensive methodological framework designed to enable secure, safe, and efficient data sharing within the DELPHI platform, addressing the complexities of multi-modal transport systems. It addresses the challenges inherent in multi-modal transport systems, with a particular focus on data exchange and collaboration among diverse mobility providers.

The primary contribution of this deliverable is the development of a comprehensive methodological framework that addresses the complexities of data sharing in a federated environment. This framework integrates key principles of data sovereignty, privacy, and security, ensuring that stakeholders maintain full control over their data throughout its lifecycle.

The deliverable presents detailed guidelines for secure, safe, and efficient data sharing. These guidelines cover critical aspects such as data validation, encryption, access controls, and auditability. They also emphasise efficient data usage strategies, including caching, optimised transfer protocols, and standardised APIs, to enhance the performance and reliability of the platform.

Regulatory recommendations outlined in this document ensure that the DELPHI platform aligns with key standards and legal frameworks, including GDPR, ISO/IEC 27001, and EMDS guidelines. These recommendations address data sovereignty, privacy, security, and interoperability, creating a reliable and legally sound data-sharing ecosystem.

The governance structure proposed in this deliverable is achieved by adopting data governance principles inspired by initiatives such as GAIA-X and IDSA and pertinent requirements on arbitration as derived in DELPHI's D2.3. It defines clear roles, processes, and entities, such as data owners, consumers, space providers, and trust brokers, to ensure accountability and compliance. The structure is neutral and impartial, fostering trust among participants while maintaining strict adherence to data governance principles. The inclusion of oversight committees and certification bodies ensures ongoing monitoring, compliance, and dispute resolution.

References

[1] Arslan, E., Pehlivan, B.A., and Kosar, T. (2018). Big data transfer optimisation through adaptive parameter tuning. Journal of Parallel and Distributed Computing, 120, pp.89-100.

[2] Liu, Y., He, Q., Zheng, D., Xia, X., Chen, F., and Zhang, B. (2020). Data caching optimization in the edge computing environment. IEEE Transactions on Services Computing, 15(4), pp.2074-2085.

[3] Haibeh, L.A., Yagoub, M.C., and Jarray, A. (2022). A survey on mobile edge computing infrastructure: Design, resource management, and optimization approaches. IEEE Access, 10, pp.27591-27610.

[4] Rossi, E., Emerson, A., and Evangelisti, S. (2003). Common data format for program sharing and integration. In Computational Science—ICCS 2003: International Conference Melbourne, Australia and St. Petersburg, Russia June 2–4, 2003 Proceedings, Part II 3 (pp. 316-323). Springer Berlin Heidelberg.

[5] Colley, D. (2021). Development of a Dynamic Design Framework for Relational Database Performance Optimisation (Doctoral dissertation, Staffordshire University).

[6] Fan, W., and Geerts, F. (2022). Foundations of data quality management. Springer Nature.

[7] Yang, Z., Harris, J.R., Walker, B., Verkamp, D., Liu, C., Chang, C., Cao, G., Stern, J., Verma, V., and Paul, L.E. (2017, December). SPDK: A development kit to build high performance storage applications. In 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 154-161). IEEE.

[8] Das, S., Xiang, Z., and Ren, L. (2021, November). Asynchronous data dissemination and its applications. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 2705-2721).

[9] Cho, D., Pasricha, S., Issenin, I., Dutt, N., Paek, Y., and Ko, S. (2008, June). Compiler driven data layout optimization for regular/irregular array access patterns. In Proceedings of the 2008 ACM SIGPLAN-SIGBED conference on Languages, compilers, and tools for embedded systems (pp. 41-50).

[10] Hsieh, Y.M., and Hung, Y.C. (2009). A scalable IT infrastructure for automated monitoring systems based on the distributed computing technique using simple object access protocol Web-services. Automation in Construction, 18(4), pp.424-433.

[11] Costa, R.L.D.C., Moreira, J., Pintor, P., dos Santos, V., and Lifschitz, S. (2021). A survey on data-driven performance tuning for big data analytics platforms. Big Data Research, 25, p.100206.

[12] RAC, S. (2024). Optimization and Orchestration in the Cloud-to-Edge Computing Continuum.

[13] Apruzzese, M., and Bresseleers, P. (2023). Business requirements for logistics data sharing: recommendations from the FENIX project. Transportation Research Procedia, 72, pp.3925-3932.

[14] Bastiaansen, H.J.M. (2022). ISHARE as generic trust framework capability. Available at: https://topsectorlogistiek.nl/wp-content/uploads/2022/07/TNO-2022-R11094-Report-iSHARE-as-generic-capability-1.pdf [Accessed 18 June 2024].

[15] Pettenpohl, H., Spiekermann, M., and Both, J.R. (2022). International Data Spaces in a Nutshell.

[16] Douloudis, K., Siapera, M., Dimitriou, G., and Prentza, A. (2020). Application of automated trust verification and delegation mechanisms in PEPPOL eProcurement network. In Information Systems: 16th European, Mediterranean, and Middle Eastern Conference, EMCIS 2019, Dubai, United Arab Emirates, December 9–10, 2019, Proceedings 16 (pp. 448-457). Springer International Publishing.