# VISION DOCUMENT

Final version

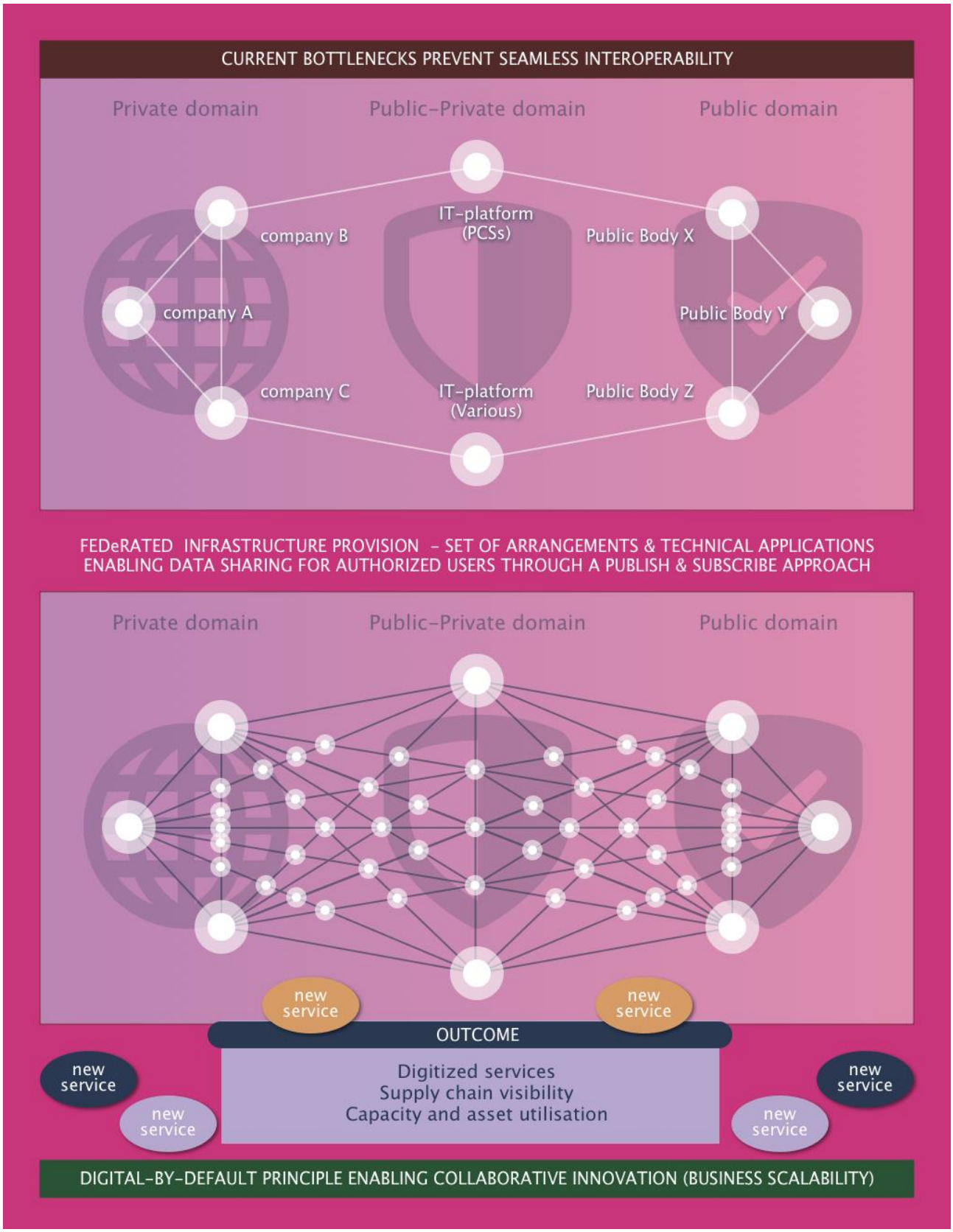
**FEDeRATED MILESTONE 1**

17 December 2019

www.federatedplatforms.eu

FEDeRATED
NETWORK OF PLATFORMS

Co-financed by the Connecting Europe Facility of the European Union




This publication has been produced with the assistance of the European Union. The content of this publication is the sole responsibility of the FEDeRATED project consortium and can in no way be taken to reflect the views of the European Union.

# EXECUTIVE SUMMARY

This FEDeRATED Vision:

- defines the need for developing an innovative information infrastructure provision for allowing connectivity for all operators and public authorities in the supply chain;
- identifies the key elements for digitalisation in the context of FEDeRATED: interconnectivity, the need for an open structure, technological solutions, possible bottlenecks, lessons learnt, the business process, semantics and the design, organisational and legal issues.

### *Setting the scene*

Digitalisation means to Information what Electricity meant to Energy. In freight transport and logistics, a digital (connecting) transport technology grid – an overarching infrastructure - is emerging. All stakeholders are challenged. New operators emerge. Data – considered by many the new gold - add substantial value to the supply chain. Companies and public authorities have to act on it. The success and failures of businesses and public authorities depend on their ability to actively engage and make use of this emerging information technology grid. The Western industrialized countries pursue an open system development. The operators in the transport and logistics markets increasingly depend on a future proof decentralised, secure, neutral and open information technology grid.

The realm for an architecture approach to enable information systems to connect has been around for some time. Within freight transport and logistics, the sentiment is to substantially reduce the existing bottlenecks and develop an open to all infrastructure provision. The major bottlenecks are a lack of interoperability of semantics, insufficient data savviness in many companies and public administrations, technical incapacities, organisational unawareness, and legal restrictions. These bottlenecks have prevented end-user systems to seamlessly connect with the established operational systems in businesses and provide for flexibility to keep pace with the development of users' needs and emergence of new technologies integration within existing IT systems. Also, many logistics operators still lack the ability to engage into the process from traditional business operations towards a data-based operation.

Times are changing. Increasingly, it is felt that bottlenecks can be overcome. Change can happen. The implementation of the digital-by-default principle is taking shape. Four major drivers for change are:

- Seamless data flow management is becoming of essential importance in developing and executing business operations and public policy responsibilities. Subsequently the information systems within the various organisations have to provide services and support to all segments within their organisations and to a multitude of stakeholders;

- New technologies are emerging and allow for enhanced IT interoperability. Global and EU/national approaches in data semantics are merging, i.e. WCO/IMO FAL. Technical

applications, such as API, and protocols allow system interconnectivity. Pull-based technologies, based on a publish and subscribe approach, allow data to be made available in their IT systems to other authorized users;

- Globally expanding data driven technology platforms exercise fierce market powers that offer an all embracing, dominant and closed-in architecture approach. The global supply chain fails to provide for an overarching regulatory framework allowing containment of the undesired effects of unlimited use of data for commercial reasons. The winner-takes-all principle is manifestly having counterproductive effects on the European way of life; EU competition and privacy legislation is challenged. This requires a countervailing EU and national policy approach, demanding technological sovereignty and antitrust actions;

- The EU transport policy and digital single market policy promote seamless services and data flows for European public administrations and business. Businesses are free to trade and operate in all EU Member States. In doing so, they inevitably have to interact electronically with Member State public administrations[1]. The lack of interoperability is a major obstacle to progression. Policy initiatives and programmes support seamless data flows, i.e. common European data space, EU Connecting Europe Facility (CEF), European Interconnectivity Framework, eGovernment and the EU Digital Transport and Logistics Forum (DTLF). EU and EU Member States legal frameworks increasingly allow paper-based information to be replaced by data. Sustainable transport, circular economy and smart mobility are policy transitions.

### *DTLF and FEDeRATED*

Within the context of the EU Digital Single Market, the DTLF has been operational since 2015. In 2018, the DTLF proposed the federated network of platforms concept to allow the European logistics and transport market to benefit from the information infrastructure that is emerging. Plug and play, federation, independent technology services and a safe, secure and trustworthy environment constitute the starting points towards a tangible approach on how to structure such an infrastructure.

To follow suit, the FEDeRATED Action was founded by 15 partners with the **purpose** to deliver on the need for developing tangible building blocks, to provide showcases and to engage various stakeholders identifying a futureproof reference architecture. Within the context of consultation and cooperation with all stakeholders, it would be a challenging thought to identify the need for an EU federated network of platforms legal initiative.

The FEDeRATED **objective** is to deliver the foundations for a trustworthy and interoperable business and administrative data sharing infrastructure for seamless, secure, sustainable, safe, and compliant freight transport and logistics, thus contributing to the Digital Single Market and the EU

[1] As stipulated in the Treaties of the European Union (EU), the EU's internal market guarantees four 'freedoms' - the free movement of goods, capital, services and people between the EU Member States. These freedoms are assured by common policies supported by interconnected, interoperable networks and systems.

White Paper for Transport.

The FEDeRATED **aim** is to kick start – to create a snowball effect for - the realization of an open digital data sharing infrastructure for smooth, safe and sustainable freight transport in Europe and its trading partners in particular.

The FEDeRATED **goal** is to assist the EU and its partners in designing an infrastructure for combining the existing information systems that have the following desirable properties:

- It is sufficiently practical and cost-effective today, with the human and financial resources likely to be available;
- It is comprehensible, capable of covering the full range of corporate needs as they exist today and as they can be foreseen in the near future;
- It is appropriate, in a strategic way, for the public authorities and the business it must serve.

The FEDeRATED **scope** is data sharing[2]. Data sharing covers end-to-end transportation chains, from the consignor to the consignees thus ensuring enhanced visibility and transparency and enabling value adding service development for third parties.

For advanced digital cooperation between business and administrations, involving namely B2A and B2B data exchange, the most important issue is to improve situational awareness and thus decision-making by all stakeholders involved. This is based on the need for visibility, transparency, booking and ordering to improve agility, optimised capacity utilisation, reliability, security and other types of compliance from societal and economic perspectives such as sustainability and employment.

Overall, the FEDeRATED vision can be summarized as:

**To provide for an infrastructure provision containing a set of agreements and technical applications to enable data in existing IT systems (platforms) of companies and public administrations to become available to authorized users through a publish and subscribe approach.**

The outcome of this FEDeRATED infrastructure provision is:

- supply chain visibility;
- capacity and asset utilisation;
- digitization of services (can be business and public authority services).

Within the context of the application of the digital by default principle, the FEDeRATED infrastructure provision enables collaborative innovation, i.e. opportunities for new business models.

In terms of transport policy goals, the infrastructure provision can be translated into indicators relating to:

[2] The focus will particularly be on smart data sharing. The various parties in the logistics chain - data providers and authorized users - can identify and chose the single data to share, a simple data or a smart data.

- Preventing congestion;
- Loading factor mobile assets;
- Less CO2/nm or CO2/km emission;
- Business profitability;
- Logistics efficiency, reliability and throughput;
- Carbon footprint reduction;
- Truck platooning;
- Synchromodality;
- Tracking and tracing optimization;
- Circular economy targets;
- Others.

In general, the benefits of a data-sharing environment for business and public authorities would be to enable seamless logistics and smart mobility services. It enables the mutual and secure availability of high-quality data between companies and governments and offers opportunities for structural innovations, new data driven business services and the ability to deal with data differently. Streamlining of processes is taking place to an ever-increasing extent and leads to efficiency benefits (such as improved use of infrastructures, increased load factor and reduced CO2 emissions). The accessibility of data leads to transparency and makes it clear where hidden costs and failure opportunities occur and can be reduced.

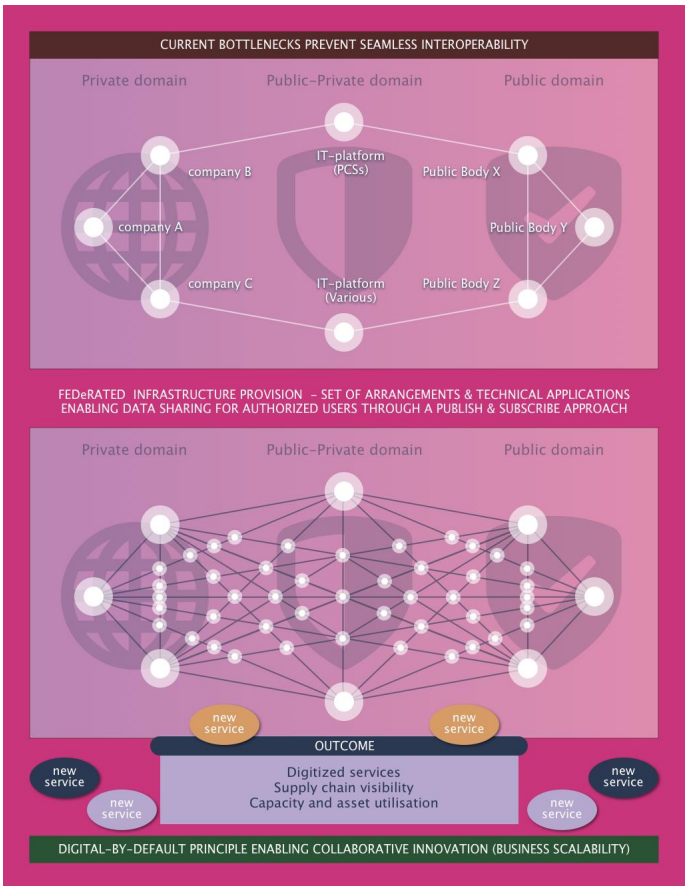



*Figure 1: The FEDeRATED approach*

The FEDeRATED Vision approach is illustrated in figure 1, page 6. Based on a set of arrangements and technical applications, current bottlenecks can be overcome and data sharing between authorized users, under specific conditions, can take place. The FEDeRATED infrastructure provision enables decentralized data exchange based on open source and interoperable programming interfaces that support development of solutions for a wide range of purposes. An important feature is that the data sharing infrastructure provision allows to access data at the source, based on availability. This would ultimately make policy driven constructions such as Single Windows – that serve as an intermediary post office – to become redundant in future.

### *Relevant logistics data sharing approaches*

There are other approaches to data sharing in general and for logistics in particular. International Data Spaces (IDS), Internet of Logistics, and the European Blockchain Services Infrastructure (EBSI) are three of them, relevant to FEDeRATED.

IDS was originally founded for data sharing in industry and enlarged its focus to other areas such as logistics. IDS is a foundation with over 100 members. IDS has developed a reference architecture for peer-to-peer (p2p) data sharing. The architecture, consisting of p2p connectors, a broker functioning as a type of registry, and a clearing house for logging and clearing and settlement of shared data, can be implemented by anyone. Of course, data sharing is only feasible if two stakeholders have a connector. Applications can add functionality to the connectors, e.g. applications for data transformation.

The Internet of Logistics, initially developed by Ericsson and IATA and specified as ONE Record, is a data sharing architecture based on the concept of a single web API (Application Programming Interface), linked data, ontologies and a data security framework. Logistics and transport data is accessed through a network of linked data (through URLs) in a RDF (Resource Description Framework) format based on W3C standards. This enables shared data on a distributed network of platforms. Direct access to the logistics and transport data creates visibility in the supply chain. Logistics and transport companies like shippers, forwarders, airlines and other partners, are developing implementations. The semantics of logistics data is being developed by IATA together with logistics and transport partners and other associations.

BCT or Distributed Ledger Technology (DLT) is expected to disintermediate particular functions in the chain by automating them, see for instance BitCoin. There are many initiatives in this area, each with its particular governance structure and business model. Where IDS and Internet of Logistics are associations with open membership, DLT initiatives have particular membership rules related to services offered to their end-users. EBSI launched by the EC as part of the CEF program is open to authorities for setting up their services, for instance in reporting and services to citizens. Initiated by one Member State, DLT services can be developed, for instance to support the eFTI Regulation in the public domain.

IDS, the Internet of Logistics, and EBSI are three different approaches to data sharing. They are generic and thus agnostic of the data that is shared. Their common capability is the (rapid) deployment with new services. These (IT) services are extensions to achieve transport goals as

formulated earlier. FEDeRATED will explore how these three approaches can be applied to provide the aforementioned infrastructure provisions and to implement the DTLF building blocks.

### *Requirements*

To begin the task of designing an information infrastructure architecture, first the requirements must be defined. The requirements reflect the purpose that the infrastructure must serve, and they also reflect the environment within which the infrastructure should function. To recognize what the requirements are, we need to look at the infrastructure from:

1. A marketing viewpoint – what are the customer's needs? How should we aim to satisfy them? This viewpoint has two angles: - the perspective within the organisation and of the people that are served in the marketplace.
2. An engineering viewpoint – What structural qualities should the infrastructure have? What topology? How should we fit the components together?

**1. The marketing viewpoint**

For public authorities, the infrastructure provision should serve the following needs:

1. Insight into actual goods flows and load factor (international and national);
2. The availability of accurate data on the use of the infrastructure (road, water, rail, airport, in time, based on historical data) for traffic management tasks; - under certain conditions and/or restrictions, this data can also be made available to companies for the planning of goods movements;
3. Sharing public rules and other relevant data for access and use of urban infrastructure by municipalities and regions for urban distribution;
4. Supervision and enforcement with risk analyses (with data analytics) on the available data, partly to ensure that the streamlined interoperability in the freight transport chain is not interrupted;
5. Providing (static) overviews for policy making and investment issues based on current data;
6. Insight into changes in goods movements (growth, decrease), for example, the calculation of effects on the use of the infrastructure and research into the causes of these changes;
7. Rapidly measurable effects of policy choices and government investments. Consider, for example, means for managing climate objectives and (re-)structuring, for example, city distribution;
8. Relaxation of cooperation between various government supervisory services by exchanging data, monitoring results and coordinating planning of controls;
9. Enable a more efficient and effective use of public resources.

For business, the infrastructure provision should serve the following needs:

1. Visibility of data throughout the supply and logistics chain. This allows companies to plan more accurately and manage risk of loss, misplacement or delayed arrival of freight

allowing them to manage and mitigate such risks;
2. An opportunity for new ventures and business models that benefit from new and reliable business connectivity;
3. Better opportunity for scaling up services, due to the many-to-many approach;
4. Increased customer service levels through more accurate and timely information;
5. Downward pressure on cost of digital service delivery and an incentive for competitive innovation due to more competition between digital solution providers and business leverage on the need for additional investments;
6. Shift from traditional human-to-human interaction on to digital machine-to-machine business exchanges, i.e. online reservation and management systems;
7. Cost savings through the prevention of errors in retyping, automatic reading of data in systems, checks on the quality of sent and received data, etc.;
8. Process synchronization of different companies by inspecting deliveries and their expected time of arrival/departure in order to prevent waiting times, to have personnel and (transport) resources available in the right place in time;
9. Transparency of goods movements and (availability of) transport capacity on the basis of which the load factor can be increased;
10. A transparent choice between different modalities by insight into available capacity, travel and route schedules, etc.;
11. Proportional use of the capacity of logistical (sub) networks, through the availability of data about (future) use of that network, also in combination with route and travel information of vehicles;
12. The deployment of new forms of autonomous assets, such as self-driving trucks and robots in distribution centres, by freight forwarders, carriers, distribution centres and transhipment companies. This can bring about a reduction in costs;
13. The use of control towers by the business sector for the control and coordination of goods and transport movements to realize various forms of process synchronization and utilization of logistical (sub) networks;
14. Bundling of cargo flows;
15. Reduction of transaction costs.

There is a multitude of examples of how a federated network of platforms could function. To give some examples:

- The federated network of platforms regulates that public authorities has access to certain streams of data;
- Port Community Systems (PCS) could request data from other 'squares' (data corridors) on behalf of public authorities;
- The federated network of platforms can integrate local, regional and national systems and applications[3] to EU level and vice versa;
- Operators and stakeholders can combine and enrich data on behalf of each other, and subsequently exchange data with each other via the federated network of platforms;

[3] See for examples paragraph on “Getting towards showcases - pilots and testing beds”.

- Various parties can offer a multimodal service package for parties that also operate multimodally (for example, almost all trucking companies).

**2. The engineering viewpoint**

The federated network of platforms concept allows various information hubs and enterprises to connect and serve as an infrastructure distributing high quality data amongst relevant stakeholders and enables those enterprises and public authorities to develop services and new business, and to improve their operation. A metaphor is to integrate isolated islands towards standardised, regulated networks designed for delivering predictable, dependable services across the infrastructure network. In transport and logistics, the information hubs, or islands, comprising different networks do not connect, yet. The federated network of platforms concept is about developing Europe as an integrated, digitalised metropole in the world for logistics and transport by capitalising on existing investments.

The structural qualities that should be engineered in the infrastructure provisions cover the following issues:

- Trust;
- Accessibility - (controlled) open or closed;
- Legislation and legal framework;
- Data quality and integrity;
- (Cyber) Security;
- Operational management;
- Sustainability objectives;
- From chains to networks;
- Data sovereignty
- Accessing data at its source;
- Investments;
- Governance.

Within the DTLF the following design principles have been defined:

- Plug and play;
- Technology independent services;
- Federation;
- Trust, secure and open.

To achieve this ultimate goal of interoperability at different layers, certain basic “rules”, agreements or requirements need to be established by data users and IT providers. The overarching conditions are covered in the Core Operating Framework. The Core Operating Framework sets out:

- The key principles that need to be adhered to in order to ensure that the interoperability issues are safeguarded in such a way as to enable a federated network of platforms approach;
- The high-level requirements that should be applicable to the interoperability layers and be constraints to formulating the leading principles as part of the FEDeRATED Master Plan.

The further development of a federated network of platforms has to rely on the comprehensive consideration of certain definable design requirements as well as legal and organisational boundaries, constituting the following key principles:

1. ensure data sovereignty;
2. create trust among platforms and participants;
3. provide a framework to enable interoperability;
4. be open and neutral to any participating party;
5. data quality.

*The topology*

A federated network of platforms is an information infrastructure for sharing data in transport and logistics, including the following components (necessary, non-exhaustive):

- Data models for all (combinations of) modalities and cargo types, including data definitions;
- The Core Components Library (CCL) for technical representation of particular concepts;
- International recommendations of value lists (UN ECE Recommendations on for instance country codes, item codes, rates, etc.);
- Standards for exchange, such as protocol standards and other technical exchange standards: (REST) API, JSON(-LD), RDFs, SHACL, HTTPS, OAUTH2, URI standards, security, etc. Including interpretation of minimum required common components;
- Directory services with which business services, spare capacity, and timetables can be found (also depending on chosen URI standards);
- Joint implementations and domain-specific standards: iSHARE, OneRecord PMD, DLF, legacy messaging standards;
- Connection conditions and quality requirements / agreements regarding data and services;
- Governance of the system: who determines what and how it is implemented, entry and exit / granting and withdrawing of access, etc. This also includes a legal track;
- (Optional) agreements on data enrichment for one of the other “squares”;
- Monitoring functions for monitoring the system - this is a (real) technical layer;
- Agreements about management, maintenance and expansion (and who will pay for it and implement it, or how you determine that).

The following *guidelines or restrictions* apply:

- Digital by default;
- Use of open source data and open standards;
- Legally anchored;
- Cost-effective solutions (in line with developments in the supply chain);
- Future-proof solutions, considering that every solution requires adjustment to new technological developments;
- "Decentralized, unless", with the emphasis on maximum use of existing IT legacy systems and not on the development of a new system;
- Financial involvement from government in IT developments, leading to open source software and open standards that can be applied and further developed by governments and

companies;
- Minimum administrative and transaction costs;
- International standards 'by default';
- Equal and international playing field.

To execute their work, public authorities need data from business. A legal provision should be in place to allow public authorities access to business data. That can be done either by direct reporting of data or by accessing data from business through controls. Suitable data interoperability, protocols, legal agreements and technical applications are required. An innovative approach (pull-based) would be direct access of public authorities into the IT systems, data lakes of companies. This is called a publish and subscribe approach.

Public authorities can improve business efficiency and service performance by exchanging data amongst each other. A decentralised approach allowing public authorities' access into one another's IT-system would provide a collaborative and innovative step forward. The data is not always readable and legal and system requirements limit the ability of public authorities to (re-)use the data[4].

### *Getting towards showcases - pilots and testing beds*

The many initiatives to date have built on sound business cases from both the public and private sectors. Digitalisation initiatives are varied in scope and scale; whether designed to optimise specific processes and procedures within the normal operating sphere of a company or galvanise the public sector approach towards monitoring and enforcement as well as modal shift and infrastructure utilisation aspects. To elaborate:

- Within the public sector these initiatives focus on utilising existing digital infrastructure from one sector for another (e.g. the Spanish "SIMPLE", to make MSW interoperable with rail), creating basic digital infrastructure interoperability capacity and rules cross-sector and focussing on digitalisation of a particular operation as part of the groundwork for future interoperability (e.g. the Spanish Shift2Rail project).
- Within the private sector these initiatives focus on developing, for example, door-to-door tracking and tracing services for clients, load factor optimisation, deployment of autonomous assets and secure data sharing.

These business cases often serve a particular purpose. In order to open up the potential for supply chain visibility and capacity utilisation it is necessary to realise an interoperable, trustworthy and open information infrastructure. That does not mean that all efforts to date are suddenly obsolete or not fit for purpose. On the contrary, it means that transformation efforts should focus on the core conditions for data sharing and interoperability, namely ensuring data sovereignty and quality, creating trust, as well as being open and neutral and thereby embracing and supporting existing

[4] Preferably, the FEDeRATED data sharing infrastructure provision constitutes the overarching framework for the implementation of all EU logistics chain related legislation. This infrastructure provision could be supported by a pull-based mechanism, called Publish and Subscribe. The provision allows for multiple use of data – within restrictions – to enable services for a seamless EU multimodal transport. The implementation of the EMSWe or the eFTI Regulations should be perceived as services derived from such an infrastructure provision, rather than a stand-alone infrastructure provision.

standards. This infers the need to consider the technical, semantic, organisational, and legal interoperability layers.

Other initiatives, within both the public and private sectors, have addressed aspects of these layers. To mention some examples: for air cargo, OneRecord specifies data security and identity standards and management. Its sets a standard from a single common API and a data model for airfreight based on an ontology (semantics); or indeed specific supporting layers (e.g. iSHARE Identity and Access Management frameworks); another example is the CaaS concept (Corridor as a Service), which offers new digital value adding solutions for logistics by combining ITS information (intelligent transport systems) and logistics information together under Public Private Partnership ecosystems collaboration. These tools and concepts can be embraced and further elaborated and experimented on within an overriding data sharing infrastructure for transport and logistics.

# TABLE OF CONTENTS

# Abbreviations

| | |
|---|---|
| A2A | Administration to Administration (of data exchange) |
| A2B | Administration to Business (of data exchange) |
| AI | Artificial Intelligence |
| API | Application Programming Interface |
| B2A | Business to Administration (of data exchange) |
| B2B | Business to Business (of data exchange) |
| CEF | Connecting Europe Facility |
| CIM | Uniform Rules Concerning the Contract of International Carriage of Goods by Rail |
| CMR | Convention Relative au Contrat de Transport International de Marchandises par la Route (of road) |
| DLF | Digital Library Federation |
| DLT | Distributed Ledger Technology |
| DTLF | Digital Transport and Logistics Forum |
| EC | European Commission |
| EDI | Electronic Data Interchange |
| EDSN | Energie Data Services Nederland (Dutch energy sector collaboration) |
| eFTI | Electronic Freight Transport Information (proposed EU Regulation) |
| EIF | European Interoperability Framework |
| EMSWe | European Maritime Single Window environment |
| ERA | European Union Agency for Railways |
| EU | European Union |
| FAL | Convention on Facilitation of International Maritime Traffic (of IMO) |
| FMS | (Freight) Forwarding Management Software |
| GDPR | General Data Protection Regulation (EU Regulation 2016/679/EU) |
| GS1 EPCIS | Electronic Product Code Information Services |
| HTTPS | Hypertext Transfer Protocol Secure |
| IANA | Internet Assigned Numbers Authority |
| ICAO | International Civil Aviation Organization |
| ICS2.0 | Import Control System (of Customs) |
| ICT | Information and Communications Technology |
| IETF | Internet Engineering Task Force |
| IMO | International Maritime Organization |
| IoT | Internet of Things |
| IT | Information Technology |
| JSON | JavaScript Object Notation |
| M2M | Machine to Machine (of data exchange) |
| MSW | Maritime Single Window |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OAUTH2 | open standard for access delegation |
| PMD | Programming Mistake Detector |
| REST | REpresentational State Transfer |
| RIPE NCC | Réseaux IP Européens Network Control Centre |
| SME | Small and Medium-sized Enterprise |
| TAF-TSI | Telematics Applications for Freight - Technical Specifications for Interoperability |

| | |
|---|---|
| TFEU | Treaty on the Functioning of the European Union |
| TMS | Transportation Management Software |
| TOGAF | The Open Group Architecture Framework |
| UN | United Nations |
| UN/CEFACT | United Nations Centre for Trade Facilitation and Electronic Business |
| URI | Uniform Resource Identifier |
| W3C | World Wide Web Consortium |
| WCO | World Customs Organization |
| WTO | World Trade Organization |

# 1 INTRODUCTION

The FEDeRATED Action is an EU Member State driven initiative to contribute to the establishment of a viable federated network of platforms for data sharing in the freight transport and logistics domain at EU level (and beyond). The main objective is to enable a smooth and effective public involvement with logistic chains for the execution of public and private duties.

The Action builds upon the work and recommendation of the Digital Transport and Logistic Forum (DTLF) to create such viable and valid federative network of platforms as an enabler for Business to Administration (B2A) and Business-to-Business (B2B) data exchange and sharing.

The Action will design and validate a federated network of platforms concept to enable data sharing in the logistics chain while providing interoperability and harmonisation between individual platforms. It will deliver a validated[5] Master Plan for an EU federated network of platforms concept and a prototype of a data sharing environment for business and public sector use.

The planned activities include:

- Vision
- Master Plan
- Pilots, Living Labs & Testing
- Collaboration
- Project Management

The Action will contribute to enhanced supply chain visibility and bundling capacity and will enable synchronised operation planning for a responsive, resilient and multimodal transport ecosystem.

## *1.1 Place of this Report*

This report is the main output of Activity 1 of the FEDeRATED Action (Milestone 1). This report forms the basis from which the Interim Master Plan (Activity 2) can be further developed.

## *1.2 Purpose*

The purpose of this Vision document is fourfold:

- It sets out the Policy Context amongst the FEDeRATED partners;
- It sets out the considerations for Legal Interoperability in terms of potential constraints and/or opportunities;
- It expands on the Operational, Semantic and Technical Interoperability considerations and implications for public and private sector bodies;
- It is the means against which all future, together with the Master Plan, (within the lifetime of

[5] Validation will be conducted through the Living labs and Pilots by the Beneficiaries using criteria based on the Interim Master Plan and Vision Documents.

FEDeRATED) development and validation can be measured.

In effect the Vision document should enable the FEDeRATED Beneficiaries to:

- Identify with the reasoning behind the need for a federated network of platforms, i.e. the Vision will link the policy and business context of the Beneficiaries with capabilities and features that are (uniquely) offered by a federated network of platforms approach;
- Highlight any boundary conditions (e.g. political, legislative, economic, etc.) that can influence the scope and implementation of a future "system";
- Already have insight into the "roles" and "responsibilities" of eventual stakeholders making use of such a "system" (i.e. public/private driven, role of administrations, promoting/supporting implementation, degree of flexibility and/or adaptability envisaged, etc.).

This report incorporates:

- State of the art on digitalisation in the transport sector from public administration perspective;
- State of the art on digitalisation in the transport sector from the private sector perspective;
- Core Operating Framework in which the FEDeRATED federative platform concept will be developed.

### *1.3 Outline*

This Vision Report sets out the long-term vision developed by the FEDeRATED project for the digitalisation of supply and logistics – the bigger picture –, i.e. to enable all players in the logistics chain and freight transport to take full advantage of the opportunities of digitalisation.

The starting points of this vision are:

- the work developed by the Digital Transport and Logistics Forum (DTLF), advice to the European Commission (June 2018), to pursue data sharing through the federative network of platforms concept;
- the experiences gained by the 15 FEDeRATED partners.

In practical terms, this vision constitutes the objective, scope, goals and direction for the 15 FEDeRATED partners and the many organisations that will participate in the FEDeRATED project between 2019-2023. The FEDeRATED Vision is the first step in establishing a validated data sharing architecture and prototype within 5 years. A commitment of the EC and EU Member States, together with other authorities and the business community, is pursued enabling various parties to invest sustainably in order to make streamlined data exchange possible.

With an eye to the FEDeRATED work ahead, the concepts of collaborative innovation, change management and interaction and involvement, as well as the lessons learnt based on various use cases of the FEDeRATED partners, are elaborated.

The Vision identifies the key elements (interconnectivity, the need for an open structure, technology, possible bottlenecks, lessons learnt, the business process, semantics and the design, organisational and legal issues) for digitalisation in the context of FEDeRATED. These key elements will have an

impact on the ambition level and relationship between the partners, their contribution to the project, the shared sense of urgency and the design of the federated network of platforms concept.

Based on the Vision, the FEDeRATED project will ultimately deliver a validated Master Plan for a federated network of platforms concept and a prototype of a data sharing environment for business and the public sector use.

The Vision has been developed through a collaborative effort of all FEDeRATED partners. This Vision report has been written as a matter of fact document - that presents the major issues leading towards the development of a data sharing infrastructure for transport and logistics in a straightforward style. Additional issues developed by the partners and not incorporated in this report can be retrieved at the FEDeRATED website (www.federatedplatforms.eu).

From the considerations made, the Vision culminates in the Core Operating Framework, this being the main input to the FEDeRATED Master Plan.

The Vision is presented so as to address interoperability aspects as covered under the European Interoperability Framework (EIF), i.e. legal, organisation, semantic and technical interoperability, under the auspices of an overriding Policy Context. The Policy Context sets out the key drivers for change in terms of the perceived direction that trade will be conducted and the expected impacts on transport and logistics processes. Further, potential legal sensitivities for change are highlighted.

The Vision is presented through the following chapters:

1. Vision essentials
2. Policy Context
3. Setting the scene
4. Elaboration of the starting points
5. Developing a federated network of platforms
6. Designing a federated network of platforms
7. The Core Operating Framework

## *1.4 Getting started*

The FEDeRATED Vision does not provide a blueprint[6] for the steps that must be taken to achieve the goal of digitalisation of transport and logistics. The challenges along the way to this goal can be diverse and large. They will often be cross sectoral, can change due to technological developments and can only be resolved in mutual coherence and through cooperation between the parties involved.

Data sharing is a process rather than an IT project. The FEDeRATED Vision does not provide a blueprint for the nature and (financial) scope of the steps that must be taken to achieve the goal. The challenges along the way can be diverse and large. They will often be cross sectoral, can change due to technological developments and can only be resolved in mutual coherence and through

[6] This is considered in the FEDeRATED Master Plan

cooperation between the parties involved.

Interaction and involvement between all stakeholders are a prerequisite for the successful execution of the FEDeRATED Vision. Work is being done at local, national and EU level on implementation plans. In the development of this FEDeRATED Vision, we collaborated with various ministries, government departments, private sector entities and interest groups.

The process towards data sharing is not at its start. Various steps have been taken in various programs and projects over the past years, both by business as well as by governments; locally, national, EU, and globally. What was lacking in taking those steps was an overarching framework from an innovative perspective with respect of real business initiatives. New legislative initiatives of the EU, especially from the objective of an EU internal digital market, technological developments and the development of dominant market players are challenging. They urge the FEDeRATED partners to show case a sustainable data sharing environment providing a level playing field, applying state of the art technology and lessons learnt so far as well as provide legal, technical and organisational insights.

The proof of the pudding is in the eating. From its CEF task, the FEDeRATED project wants to play a proactive role with public authorities and business in digitizing processes and services and solving the bottlenecks mentioned above. As the process towards establishing data sharing will be long it is important to establish and celebrate successes.

Fully fledged implementation of this FEDeRATED Vision would require a very long period, including the engagement of a multitude of different stakeholders and possibly a regulating framework. FEDeRATED aims to kick-start the process on a structured and concrete level over the coming 4-year period.

# 2 THE VISION – GETTING STARTED

The FEDeRATED project partners have agreed on the following project essentials:

The **objective** is to kick start the realization of complete and streamlined digitalisation (digital by default) of multimodal freight transport in general and a future-proof open digital data sharing infrastructure for smooth, safe and sustainable freight transport in Europe and its trading partners in specific. FEDeRATED intends to create a snowball effect.

The **scope** is to develop a future proof data sharing environment for business and public authorities enabling seamless logistics and smart mobility services. Thereto, harmonized information infrastructure services should be developed that allows various organisational networks (data spaces) to interconnect with one another and share data. Within transport and logistics many data spaces already exist, but they do not have the ability yet to adapt, interconnect, co-evolve and integrate and make full advantage of each other.

The **goals**, are:

- to deliver the validated foundations and elements of building for a trustworthy, open, interoperable and neutral data sharing infrastructure for business and public sector use in freight transport and logistics (local, national, EU and global); and,
- to show practical and tangible results.

## *2.1 The starting points*

A number of **starting points** have been defined for achieving the FEDeRATED goals. Most of these starting points are further elaborated in the upcoming chapters; some are further specified in this chapter.

1. To take into consideration the current policy frameworks;
2. Application of the European Interoperability Framework concept relating the layers: legal, organisation, semantics and technical interoperability;
3. To further develop the federated concept of platforms based on the work of DTLF I SG2;
4. Use of existing and new technologies (such as a Pull-based data approach, Blockchain Technology and Artificial Intelligence);
5. Lessons learnt - further development based on experience gained in previously initiated developments;
6. Choosing decentralized system development in the market with links to each other instead of new central system development;
7. Minimal transaction costs for governments and companies;
8. Maintaining the autonomy of people above machines;
9. Linking government funding with open data and open source development;
10. The concept of collaborative innovation - innovation can only be successful when done in a collaborative manner;
11. Ensuring that small- and medium-sized enterprises are actively participating;
12. Need to engage in a change process, rather than an IT project only.

The Vision acts as the central focus - or bulls' eye - of the FEDeRATED project. From this focus the following are derived: the Master Plan; the validation criteria for the pilot projects and the living labs; and the basis for collaboration with the partners and external parties.

In terms of designing an infrastructure provision, first the requirements must be defined. The requirements reflect the purpose that the infrastructure must serve, and they also reflect the environment within which the infrastructure must function. To recognize what the requirements are, we need to look at the infrastructure from:

1. A marketing viewpoint – This relates to the needs for data sharing within companies and public authorities and of the people that are served in the marketplace, how to satisfy them?
2. An engineering viewpoint – What structural qualities should the data sharing infrastructure have? What topology? How should we fit the components together?

## *2.2 Lessons learnt*

In the EU, various data exchange platform initiatives have been initiated and materialized. Mostly these initiatives led to a data information hub - a platform -, which actually constitutes the basis of a federated network of platforms. Based on a multitude of projects the following *Guidelines when starting an information node* have been established when starting up a new node:

1. Explore for each party a recognizable and quickly achievable advantage in having the node;
2. Organize based on trust between the parties and start the growth core of the node;
3. Do not start with a design but initiate a process;
4. Place the node in the hands of a party who does NOT benefit from the exchange. See additional information in Annex 1

## *2.3 Collaborative innovation.*

The road towards full paperless transport and streamlined data exchange allows innovations to be stimulated and to take place structurally. The basis of these innovations is the provision of an information infrastructure (see pink block in figure 2) that allows for a cross-sectoral exchange of data of sound quality to be used for Intelligent Transport Services as well as Logistics services such as smart mobility. This innovation can only be realized through collaboration. The collaboration between public and private sectors allows realisation of the targets of both sectors.

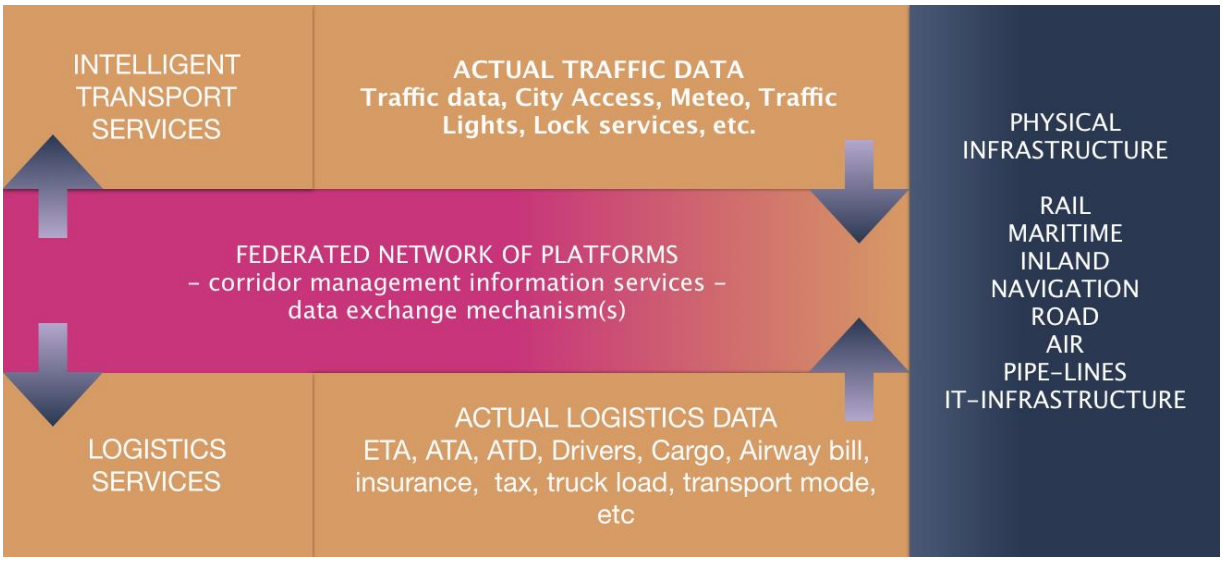



*Figure 2: A federated cross-sectoral data-sharing infrastructure as a facilitating layer*

## 2.4 Government funding

Linking government policy combined with funding in open data and open source developments is one (important) tool for driving digitalization of both government and private sector processes, systems and frameworks.

# 3 POLICY CONTEXT

## *3.1 Global supply chain digitalisation*

New (free) trade agreements, increased globalisation of the transport sector, emerging world trade disruptions and Brexit, the proliferation of emerging markets and improved or new infrastructure and technology are but a few of the drivers for change within logistics and the transport sector. Global, national and local shifts have led the sector to explore ways to capitalise on the new opportunities and to mitigate risks. This in turn has led to businesses devising new business processes and models that rely on digitalisation.

Further, the development of eCommerce and the expectations of the consumer require the transport and logistics sector to not only seek operational and cost efficiencies but also improve visibility and reliability across the supply chain.

International trade inevitably involves the physical movement of goods or persons from place of origin to place of destination. Digitalisation and new business processes and models have led to the emergence of a parallel trade route, that involving the movement of data and information associated with the physical goods. It may involve different stakeholders and means and will undoubtedly operate in a different time period. The stakeholders will be involved in generating the data, or managing and orchestrating the exchange of the data, or be dependent on the receipt of data to carry out their own processes. These processes may be business orientated and related to both the physical and virtual movement of the goods or persons or they may be regulatory and enforcement in nature and linked to just the virtual movement.

Recognising the international nature of trade, the international community, in and outside of the EU, have set out internationally binding standards, regulatory frameworks, Agreements and Conventions, exchange and application of best practices etc. through e.g. UN Specialised Agencies (ICAO, IMO, etc.), other UN bodies (such as UNCTAD, UNECE (incorporating UN/CEFACT), etc.) and other independent intergovernmental organisations (such as WCO, WTO, etc.).

The new business processes and models rely on digitalisation and availability of data. Data to support not only in terms of Artificial Intelligence (AI) and enhanced analytics but also towards enhanced predictability and visibility across the chain. This leads to a stronger reliance on data in all phases of operation, the need to enable integration across the value-chain.

These new business processes and models are not limited to the private sector. Deregulation for reporting requirements implies that less information is to be reported by the private sector. However, this is often because the relevant government agencies have employed new processes or models that afford them the necessary level of confidence to be able to still conduct their role and responsibilities, possibility also to improve the quality of their work, develop collaboration between various public authorities and to deliver tailor made services to business. Government agencies such as Customs seek ways to improve visibility of the chain in the risk-based procedures, starting for example on the basis of the initial transaction details (the what, who, where, when and to some extent how) of the goods movement. This may lead to more “pull” than “push” and thereby a form of deregulation.

### 3.2 The EU Digital Single Market Policy

In recent years the EU policy on the Digital Single Market, initiated in 2014, has been the catalyst for several initiatives, aiming to reduce barriers and offer more opportunities to do business across EU borders in a legal, safe, secure and affordable way. Unlocking the potential of a European data economy requires innovative strategies towards the re-use potential of different types of data and facilitating its free flow across borders.

The EU Digital Single Market has a potential impact on various policy domains and also has cross-sectoral effects. To safeguard the further development of the four EU freedoms, i.e. movement of goods, persons, services, capital and services, the principle of digital by default is to be applied in freight transport and logistics: meaning paperless transport.

Further, with in the context of the EU Digital Single Market, the EU has developed the European Interoperability Framework (EIF) as a guidance to public administrations through recommendations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that both existing and new legislation do not compromise interoperability efforts. The interoperability concept of the EU relates to the four layers: technical, semantic, organisational, and legal interoperability.

1. Technical – the set of standards for actually interconnecting systems and being able to share data. These sets of standards comprise communication protocols that might include security and reliability functionality.
2. Semantic – Semantics are like a “language of freight” and refer to the ability to add contextual meaning around data so it can be understood, searched, and shared, enabling both people and computers to see and discover relationships in the data. Meaning is also provided in the context of processes. Referring to the process of advanced digital cooperation between business and administrations, the elements that emerge as the most important are the need for visibility, booking, transparency, agility, optimized capacity utilization, reliability, security and other types of compliance to meet social and economic goals such as sustainability and employment. To develop paper information into electronic data requires a lot of effort and mutual understanding on what is to be done. (*See Annex 2*)
3. Organisational – This relates on the one hand to governance and on the other hand to culture and organisational structure and strategy. It is also important that organisations and their IT systems, within an information hub, can connect technically (technical interoperability) and are able to support semantics and processes.
4. Legal – The legal framework relates to the global, EU and national applicable legislation for freight transport (waste, health, dangerous goods, multimodal transport, security and safety, personal documentation, technical requirements for transport modes etc), logistics and international trade, i.e. Customs (Union Customs Code) and the current legal initiatives. Especially relevant are the implementation of the current EMSWe Regulation and upcoming eFTI Regulation. Preferably they should be dealt with from a data sharing perspective as advocated in the DTLF, thus allowing maximum benefit for all parties involved. On a national level, a lot of “paper-based” legislation is still in place and data sharing is not a generic legally accepted concept in most, if not all, EU Member States (except for customs data sharing). Apart from legislation fostering or hindering the digital-by-default principle it should also be

established that data sharing as such is legally permitted under specific conditions. Emerging legal issues that need more study are platform liability and data sharing rules, i.e. making data available to third parties (FAIR principles – Findable, Accessible, Interoperable, Re-usable). As companies and administrations interconnect through platforms, the responsibilities and liabilities should be clear. (*see Annex 2*)

### 3.3 DTLF and FEDeRATED

In 2015, the EC initiated the Digital Transport and Logistics Forum (DTLF), comprising experts from both the public and private sectors, in order to build a common vision and road map for digital transport and logistics. DTLF work on corridor management information system(s) have seen recommendations towards paperless (e.g. through the eFTI proposals) and interoperability (e.g. through the federated network of platforms concept).

In further support of the EU policies towards digitalisation, both national (public sector) policies and self-driven business initiatives have been developed. Further, in order to facilitate the Digital Single Market, various EU legislative measures have been adopted in recent years.

Interoperability, or the current lack of, is recognised as a major stumbling block that has to be addressed if these new business processes and models can be realised. As such FEDeRATED addresses interoperability aspects as covered under the European Interoperability Framework (EIF), i.e. legal, organisation, semantic and technical interoperability.

FEDeRATED embraces the DTLF concept of a federated network of platforms as a means to overcome current obstacles in the exchange and availability of data. However, the federated network of platforms is not only about simply having access to data, it is about the flexibility it can afford to all facets, in both the private and public sectors, in services.

The FEDeRATED Action relates to a large extent on contributing to the further development and testing of the technical aspects surrounding potential implementation this federated network of platforms in an operational setting. These technical aspects are to be developed so as to be fit for purpose within a given scope. To be fit for purpose, it is necessary that the technical solution can anticipate on any potential constraints. This scope is to a large extent framed by policy, organisation and legal considerations and boundaries.

Policy, both in the public and private sector, relates to opportunities and what an organisation wants (or does not want) to do achieve them and how. It is often governed or framed by economic choices. Policy can be interrelated with legislative requirements, but it is not necessarily bound by them. Laws can be adapted to meet the needs of the policy. Organisations (both in terms of interrelations and mindset) can be adapted to facilitate.

### 3.4 Legal Sensitivities

The policies and foreseen trends directly influencing transport and logistics have the potential to test legal sensitivities to the limit. Relatively straight-forward solutions such as obliging the acceptance of electronic data by authorities (such as with the proposed eFTI regulation) are overshadowed by more complex legal challenges down the line.

The opening up of data accessibility, as well as the increased reliance on that data, raise issues concerning responsibilities and liabilities towards how and when data is to be made accessible, of what quality, to whom and for what purpose. Also, questions arise through changes in the overall processes such as third-party liability through the introduction of (new) stakeholders in the chain, i.e. platforms, [7] or the impacts of increased visibility on confidentiality and competition.

Ultimately, we are not just dealing with intra-EU trade and data exchange and the vast majority of data exchange will involve transport and logistics services from and to non-EU countries, leading to potential cross-jurisdictional impacts. Depending on the nature and the intended use and disclosure of data, compatibility with other jurisdictions regarding data generation, processing and storage, a wide array of legal obligations may need to be considered (not just EU).

Further, logistics act in response to contractual obligations initiated from the original transaction. These contractual obligations will bring with them data handling obligations concerning data collection, use, storage and disclosure (exchange).

In general, the adoption of the federated network of platforms concept brings with it a number of pre-requisites. For data initiators (originator or owner) this may include ensuring: data input is of sufficient accuracy and quality for all intended purposes; sufficient visibility, also in terms of required permissions or access rules (e.g. who needs, or has the right to, what); data ownership, etc. For the data handlers (platforms) it includes: respecting owner and user confidentiality and security requirements at all stages (irrespective of the jurisdiction that platforms are located in or make use of); and that platforms, or platform operators, fulfil a role and provide the services they are contracted to provide. For data (end-)users it may include reliability of access through recognised platforms; quality and fit-for-purpose data.

The following legal sensitivities form the crux of the issues to addressed when considering potential (legal) boundaries towards the federated network of platforms:

- Changing responsibilities towards data provision, access and use (including reliance, authenticity and integrity);
- Liability, both in terms of protecting existing (transaction-oriented) rules and required (platform-focused) regulations;
- Extent and need for regulation concerning the design and operation criteria of such a decentralized trust-generating mechanism.

[7] See Annex 2 on legal issues of platforms, relating to liability issues

# 4 SETTING THE SCENE

## *4.1 The trends*

In freight transport and logistics substantial growth and diversification of freight flows and connected data, especially related to eCommerce, IoT applications and emerging technologies, is foreseen. This will eventually lead to a large and increasing demand for more sustainable and multimodal transport. This in turn will demand harmonized data interoperability and technical solutions to share data between heterogeneous IT systems of a large number of stakeholders.

Digitalisation has structurally initiated a transformation in the way in which freight transport and logistics will operate. With respect to this transformation, the following trends will have to be considered:

1. Increased data traffic, including the shared use of data for chain optimization and the necessity of all parties in the enforcement chain to be connected;
2. Increasing power concentration, in which the powerful parties impose their standards for data exchange and logistical chain arrangement on other parties in their network;
3. A demand-driven (pull) design of the economy (consumer market) with further individualized products in general and the goods transport chain in particular;
4. Localization of production through increasing automation (Smart Industry) leading to different demands on goods flows;
5. Technology developments that enable decentralization of data management and exchange, including the shared use of data for chain optimization and the need for all parties in the (enforcement) chain to be connected;
6. Development of multifaceted platforms as a new kind of intermediary that brings people and organisations together. Various forms of cooperation - B2B, B2A, A2A, A2B[8] - can arise in a platform[9];
7. Collaboration between various 'intelligent, autonomous' resources, people and organisations for achieving individual goals. There are also first versions of intelligent containers[10]. Coherence and alignment of goals and possibilities for each of these resources, people and organisations is necessary.

Within the perspective of data sharing there are three modes of production, namely: state or centralized control towards an integrated infrastructural ideal; private or decentralized involvement; and, a community-led-network. It appears that the latter, also because of the large number of participants that contribute to and benefit from a federated network of platforms, will potentially be

[8] Business-to-Business (B2B), Business-to-Administration (B2A), Administration-to-Administration (A2A), Administration-to-Business (A2B)

[9] Consider, for example, two-sided platforms (Uber, AirBnB), but also platforms for crowd-sourcing and co-creation for mobilizing knowledge and experience of people (GitHub for open source software development). New services are also created based on data, for example Planning or Expected Arrival Time for prediction algorithms.

[10] Decision-making processes can be implemented anywhere; means of transport, containers, terminals or other hubs and organisations will each have their own decision-making processes.

the best option to choose. This will have an effect on the governance of this infrastructure.

### 4.2 What should the FEDeRATED approach in general deliver

The operational perspective of FEDeRATED has a focus on actual data sharing for business benefits, both for enterprises and authorities. The overall perspective is that of seamless, safe, secure and compliant trade flows, contributing and in line with sustainability requirements.

Within the field of transport and logistics, both the public and private sector do share a common vision on where digitalisation can offer the greatest impact, namely increasing and enhancing:

- supply chain visibility;
- capacity and asset utilisation;
- digitization of business services

For governments, supply chain visibility provides insight into the actual goods flow and a means to anticipate on and enable a more efficient and effective use of public resources. This may include streamlining public enforcement tasks (also for sustainability objectives) or implementing proactive traffic management.

For business, supply chain visibility allows companies to plan more accurately and manage risk of loss, misplacement or delayed arrival of freight allowing them to manage and mitigate such risks

Although there are already initiatives that develop and provide these services, visibility services are not widely implemented and used by relevant stakeholders. These visibility services can be the basis for sharing spare capacity for booking and ordering, thus contributing to sustainability goals.

Supply chain visibility ultimately leads to opportunities for enhancing capacity utilisation. Enhanced capacity utilisation is achievable through e.g. the proportional use of the capacity of logistical (sub) networks and choice between different modalities as well as optimising load factors and e.g. potential bundling of cargo. It also unlocks the potential for new innovative business services aimed at furthering these aspects as well as overall competitiveness.

Business services define data requirements of individual enterprises. The description of these business services can be standardized, but individual enterprises have to formulate their services and thus their data requirements. Timetables, flight schedules, and voyages are also representing business services, thus formulating data requirements. Customers will have to formulate their goals, linked to business services of service providers, to allow for matching of available capacity provided by business services.

### 4.3 Operations and Business benefits

The next figure illustrates the overall business benefits, building upon the federation of platforms supported by interoperable platforms and interoperability amongst heterogeneous IT systems of end-users of these platforms.

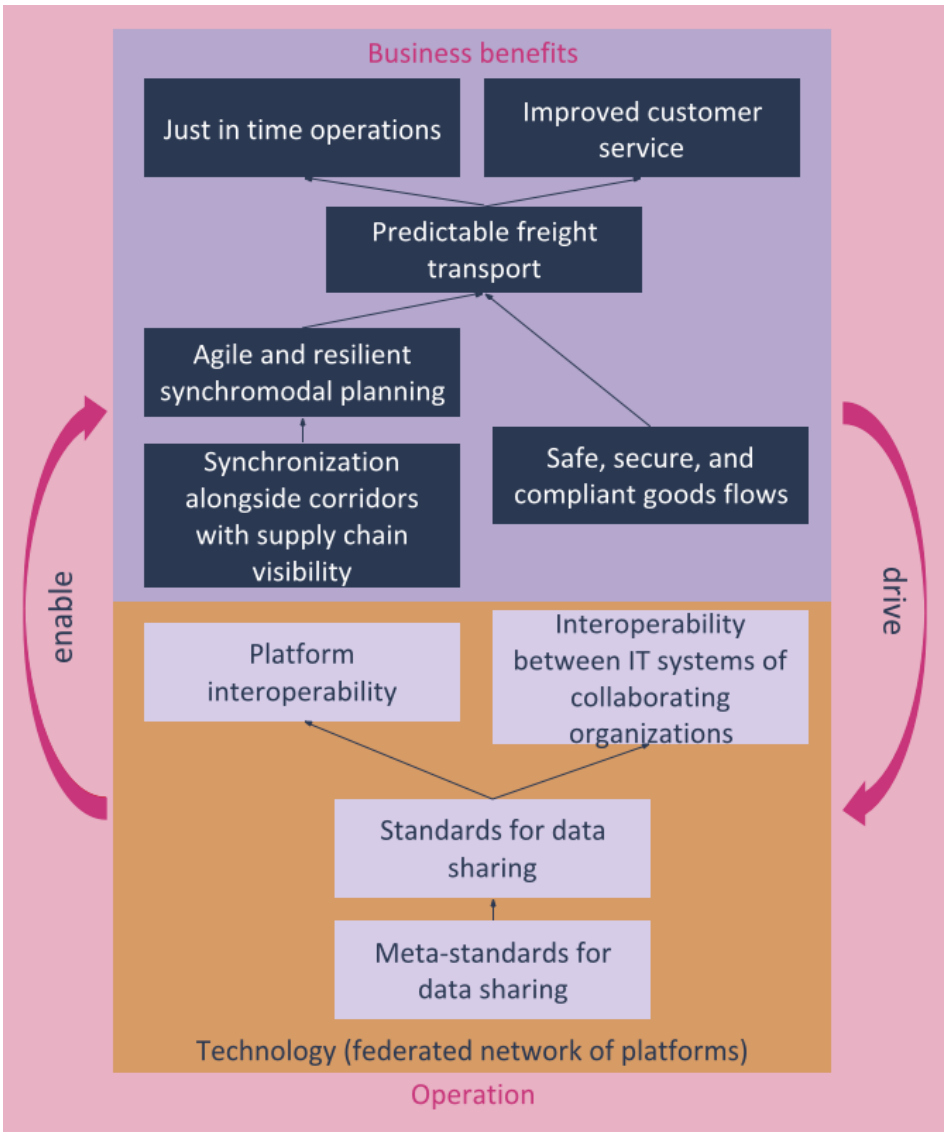



*Figure 3: Delivering value added for business through a federated network of platforms*

Business benefits should either select available functionality provided by the technology and/or define requirements for additional functionality that is not yet supported by the technology. Thus, the technology should be able to support any new business benefits that emerge when developing FEDeRATED but can also already provide ('enable') functionality already identified, building upon past experience. The testing beds (Activity 3) will have to formulate their business benefits and transform them into functionality requirements of the technology.

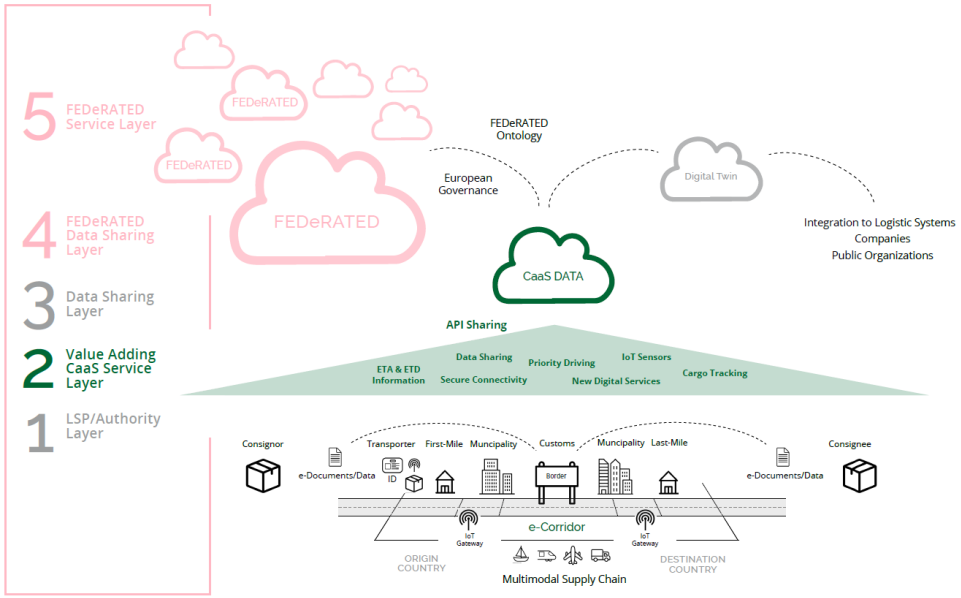
The success of the federated network of platforms will in future very much depend on the application of the digital by default principle. Many companies and public authorities are not fully digitalized yet. This hampers the opportunities for seamless transport and interoperability. These features enable many-to-many business, which enlarges current business environments. In current operations supply chains are linear processes wherein agreements are made between a couple of actors and information is transferred between stakeholders in parallel with the physical cargo. The FEDeRATED approach provides an opportunity to operate over the linear process boundaries and thereby replace paper documents with data.

**Corridor as a Service (CaaS)**

The CaaS programme is a Finnish public private partnership engaging companies and public authorities towards the integration between a FEDeRATED data sharing infrastructure provision and the development of national and local transport and logistics services. It also aims to demonstrates what value added the federated network of platforms approach – allowing different existing and emerging platforms being connected – can contribute to seamless supply chain management.

The main idea of the CaaS concept is to integrate digital infrastructure information i.e. ITS information and freight information, and hence improve supply chain visibility and efficiency. The goal of CaaS is to provide a data sharing environment for logistics stakeholders and foster situational awareness about digitalized logistics processes.

Apart from tailormade services development, an international and interoperable federation of platforms enables also many-to-many business. This enlarges the current scope of the business environments and provides opportunity for the business sector to scale up their services. Currently, operational supply chains are linear processes. Often, agreements are done between a limited number of actors (i.e. one-to-one) and information is transferred between stakeholders in parallel with physical cargo flows. The FEDeRATED approach provides the opportunity to operate beyond the linear process boundaries. Thereby, paper documents are replaced by data, being available for authorized stakeholders when needed. The CaaS concept aims to integrate the FEDeRATED approach within a Finnish public private partnership also integrating the physical supply chains and infrastructure to the data layer. See Illustration 8 below, explaining the interrelationship between the national-EU layers.




While in the first instance data and information are shared between companies and collaboration networks on national and regional level, the FEDeRATED approach provides the opportunity to scale up data sharing. With interoperable, secure and controlled data sharing, the business and public sectors can utilize services and data beyond current system and country boundaries. **Layer 1** – *Logistics Service Provider/Authority layer:* Physical supply chain process and related data; Intelligent infrastructure. **Layer 2** – *Value adding CaaS service layer:* Data fusion from layer 1; Service and packaging of digital services. **Layer 3** – *Data sharing layer*: Data sharing on national and regional level; One-to-many approach. **Layer 4** – *FEDeRATED data sharing layer*: EU level data governance; Data and information interoperability; Trust. **Layer 5** – *FEDeRATED service layer.* Many-to-many approach; EU level scalability; EU level service interoperability.

### 4.3.1 Predictability and low costs

The main business benefit currently identified by FEDeRATED and based on past experience in (EU funded) projects is the creation of predictable freight transport with a low administrative cost. This low administrative cost refers not only to data sharing between business and authorities (also known as administrative burden, B2A and A2B), but also to reduction of paper documents for B2B, B2A, and A2B. The latter has been one of the goals of the IATA OneRecord where links to data are shared and data duplication is prevented as much as possible to prevent any rekeying and errors. The reduction of paper documents is also part of the eFTI regulation, where a business case with the Benelux eCMR pilot will be conducted by FEDeRATED. This latter business case also considers the compliance to regulations.

Predictable freight transport enables just in time operation for inbound logistics of a particular organization, for instance by having the proper parts at the proper place and time for manufacturing a product or having sufficient stock with agreed quality available to meet customer demands in retail stores. One of the Finnish business cases on transport of salmon from Norway via Finland to retail stores in China.

For outbound logistics, an organization exactly knows what products are on their way to their customers. They can provide visibility to these customers with updates of for instance planning data (i.e. updates of the estimated time of arrival). Not only will this prevent any duplicate (express) deliveries in case of customer demands that lead to high costs and waste, but it will also enable a customer to synchronize its processes. One of the EU FP7 SEC CORE cases of flowers transported by air from Kenia to the Netherlands was based on this type of visibility, enabling the flower auction to have sufficient personnel available to handle the flows.

Predictable freight transport is based on two pillars, namely compliance with any international regulations governed by authorities and the consideration of any disturbances and delays during transport. Compliance with international regulations provides a safe and secure logistics operation, compliant with trade regulations and VAT. As much as possible, the technology should enable these types of compliance rules. The Benelux eCMR pilot will address a number of these issues.

Resilience of logistics operations implies the capability to handle these in an agile way, meeting customer demands for logistics operations. Agility also considers synchromodal planning, which also enables bundling of goods flows. Thus, agility and resilience require an overview of available capacity and business services. They are built upon synchronization of the various legs in a transport chain alongside corridors. These aspects will be further elaborate by business cases within the FEDeRATED Action. Italian and Swedish business cases will focus on creating visibility for improving the customer service from a logistics service provider perspective.

To achieve agility, resilience, and synchromodality, each individual end-user should only register itself once, integrate its IT back-office systems with the technology, and do business with any other relevant end-user with common data sharing arrangements. These latter should specify the rules providing trust (i.e. trust in the performance of another, not yet known end-user and trust in the federated network of platforms) and data requirements of the other users. The plug and play mechanism and additional rules should be specified by the Master Plan.

To ensure safe, secure, and compliant goods flows, authorities also should be able to trust the infrastructure and be able to formulate their data requirements (e.g. by milestones, data sets, infrastructure access rules, and data access policies like geofencing). Authorities should be able to monitor goods flows according to their requirement and in line with regulations and procedures.

## *4.4 The benefits of digitalisation*

Digitalisation offers a window of opportunities and benefits for both government and business. These possibilities need to be tested. In realizing the possibilities that digitalisation offers, existing culture, business models, organisational structure and legacy systems also play an important role.

### 4.4.1 Government benefits

For the government, digitalisation of freight transport and logistics offers new possibilities, such as:

1. Insight into actual goods flows and load factor (international and national);
2. The availability of accurate data on the use of the infrastructure (road, water, rail, airport, in time, based on historical data) for traffic management tasks; - under certain conditions and/or restrictions, this data can also be made available to companies for the planning of goods movements;
3. Sharing public rules and other relevant data for access and use of urban infrastructure by municipalities and regions for urban distribution;
4. Supervision and enforcement with risk analyses (with data analytics) on the available data, partly to ensure that the streamlined interoperability in the freight transport chain is not interrupted;
5. Providing (static) overviews for policy making and investment issues based on current data;
6. Insight into changes in goods movements (growth, decrease), for example, the calculation of effects on the use of the infrastructure and research into the causes of these changes;
7. Rapidly measurable effects of policy choices and government investments. Consider, for example, means for managing climate objectives and (re-)structuring, for example, city distribution;
8. Relaxation of cooperation between various government supervisory services by exchanging data, monitoring results and coordinating planning of controls;
9. Enable a more efficient and effective use of public resources.

### 4.4.2 Business benefits

For business, digitalisation of freight transport offers new possibilities, such as:

1. Visibility of data throughout the supply and logistics chain allows companies to plan more accurately and manage risk of loss, misplacement or delayed arrival of freight allowing them to manage and mitigate such risks;
2. The primary objective of private business is stakeholder return on investment. Digitalization of freight transport and logistics creates an opportunity for new ventures and business models that benefit from new and reliable business connectivity;
3. Customer service levels through more accurate and timely information can be increased;

4. A new and evolving ecosystem of platforms creates opportunities for competition and investment. Competition between digital solution providers will put downward pressure on cost of digital service delivery and provide an incentive for competitive innovation;
5. Digital competitiveness is increasingly important for logistics and transport providers. Their customers are shifting from traditional human-to-human interaction to online reservation and management systems, i.e. is human-to-machine and on to digital machine-to-machine business exchanges. The ability to deliver digital machine-to-machine services provides a competitive advantage to individual businesses and to the European business community as a whole;
6. Cost savings through the prevention of errors in retyping, automatic reading of data in systems, checks on the quality of sent and received data, etc.;
7. Process synchronization of different companies by inspecting deliveries and their expected time of arrival in order to prevent waiting times, to have personnel and (transport) resources available in the right place in time;
8. Transparency of goods movements and (availability of) transport capacity on the basis of which the load factor can be increased. This contributes to the government's climate objectives, both for city distribution and other forms of freight transport, as well as contributing to the revenue and profitability of the business community;
9. A transparent choice between different modalities through insight into available capacity, travel and route schedules, etc. This contributes to the realization of climate objectives and leads to higher revenues for the business community (synchromodality);
10. Proportional use of the capacity of logistical (sub) networks, through the availability of data about (future) use of that network, also in combination with route and travel information of vehicles. This can also prevent congestion;
11. The deployment of new forms of autonomous assets, such as self-driving trucks and robots in distribution centres, by freight forwarders, carriers, distribution centres and transhipment companies. This can bring about a reduction in costs. Self-propelled trucks, for example, can be used immediately after production;
12. The use of control towers by the business sector for the control and coordination of goods and transport movements to realize various forms of process synchronization and utilization of logistical (sub) networks;
13. Bundling of cargo flows. Studies show that supply chains coexist with sub optimization of each chain. Bundling of flows (horizontally and vertically) through data sharing can contribute to the capacity utilization of vehicles and logistical (sub) networks and to climate objectives;
14. Reduction of transaction costs.

In Annex 3 examples of data sharing in various transport modes are provided

### *4.5 Challenges*

The benefits of digitalisation have only partially materialized. Although, when transporting goods across borders, there is an increasing electronic exchange of information that accompanies the physical flows, these information flows are not fully seamless yet throughout the supply chain. The business and government operators in the logistics chain are challenged to overcome current bottlenecks that hamper interoperability and to find a common denominator to answer the emerging

powers of global operator technology platforms. This has to be realised through cross party collaboration and consensus, at the same time as creating the conditions for incentive for change.

The major bottlenecks that hamper digitalisation – seamless data flows - in freight transport and logistics are:

1. The lack of a coherent cross-party legal framework. At present not all legal provisions allow information transfer on the basis of digital data instead of paper. Also, the provision of digital versions of paper documents is not allowed in all countries and made possible by all laws. As a result, there is a fragmented transport market between the various parties in the various transport domains and between different countries. It is anticipated that these issues will be assisted through the foreseen eFTI Regulation however bottlenecks may still be present with e.g. non-regulatory information and the global marketplace. Further, questions on ownership, integrity and eventual liability still exist.
2. Impairment of the open freight system. An increasing accumulation of central power in the freight transport system is going to large market parties and technology companies. These parties may impose discriminatory and priority standards for data exchange and logistical chain arrangements on smaller parties in freight transport. This leads to an uneven playing field in transport.
3. No common digital language. The parties involved in freight transport do not all use the same language, i.e. the same standard, and, if they do use the same standard, they probably use it in different ways. A major cause of this bottleneck is insufficient coupling between the different standardization developments in the international (related to standardization in world trade) and national freight transport (related to standardization for individual transport modalities that often differ from each other), and the fact that standards replace paper documents and do not reflect business process choreography. In this way, a patchwork of solutions for digital information exchange arises, resulting in poor and lacking interoperability, often linked to high transaction costs, between the different transport modalities and between companies themselves.
4. Limited investment and availability of skilled resources or service providers are a challenge for all but the largest entities. Medium and small sized companies will most likely prefer to use platforms that provide them access to the digital networks, but this puts them behind the competitive curve while these platforms are being developed or upgraded.

### 4.5.1 The case for e-commerce logistics and transport

By 2021, e-commerce is expected to represent 17.5% of retail sales globally (according to the International Postal Corporation) This e-commerce freight represents vast volumes of small packages that are transported in bulk as mixed shipments. This presents an enormous challenge for customs & border protection and transport stakeholders whose systems and processes are not ready to track and treat each of these individual package movements which may include illicit, counterfeit, dangerous and underdeclared goods.

A second challenge concerns the magnitude of some of the leading e-commerce platforms. These platforms are essentially electronic marketplaces between sellers and buyers and may have virtual monopoly positions in markets that may span a continent. The absence of effective digital integration

of these platforms with the logistics, transport and government allows these platforms to control the access to information and dictate the terms of such access.

The development of regulation of digital data exchange and the recommended standards for such exchange platforms will allow governments to ensure that information access is not constrained unreasonably and provide them with the data they need to exercise their fiduciary role in cross-border trade.

From a logistics and transport perspective, the transport companies that cross borders with these goods are responsible for the provision of customs declaration and must also ensure that the freight they carry is safe and complies with regulations related to the goods carried. The ability to access data at piece level, i.e. for each e-commerce package movement will enable them to carry out their duties.

This is not to suggest that e-commerce platforms are unwilling to support seamless integration of their platforms with the international logistics & transport and government platforms. It is clear that any improvement in the exchange of data between all stakeholders is an enabler for continued growth in e-commerce.

These bottlenecks impede the realization of a streamlined multimodal transport chain - the fast and (cost) effective transfer of goods from one transport mode to another. It also blocks opportunities for innovation in freight transport and logistics based on digitalisation.

### 4.5.2 Technology applications

Digitalisation and automation in freight transport and logistics is an irreversible trend. Data is central to this. New technologies and their applications play an important role, such as Artificial Intelligence (AI), Machine Learning / Deep (Reinforcement) Learning, Software development and distribution, Internet of Things and sensors, Distributed Ledger Technology (DLT) or Blockchain and Robotization.

Digitalisation and automation in freight transport is an irreversible trend. Data is central to this. New technologies and their applications play an important role, such as:

- Artificial Intelligence (AI). AI offers the possibility to apply static algorithms for operational purposes in a different way, as a result of which these algorithms will take more and more decisions for people and organisations and can also be arranged for risk analyses of goods flows and dynamic synchromodal chain planning by companies.
- Machine Learning / Deep (Reinforcement) Learning. These applications are related to the design of AI algorithms to generate solutions for questions or challenges. Deep Learning requires a large amount of data in which people help to set the algorithms (to 'train'). With Deep Reinforcement Learning, the algorithm gets the basic rules of an application and the algorithm develops independently of human support. Examples are chain planning and medical diagnoses, with the ultimate goal that the algorithm performs better than a human being.
- Specific chipsets. The new chipsets offer the possibility for fast processing of a large number of data streams with small volumes and form the basis for the introduction of sensors in

freight transport for autonomous vehicles, intelligent cargo, etc., see also robotization. These chipsets may embed secure data encryption and IoT protocols.

- Software development and distribution. The current software can be developed on a large scale, and via co-creation, and quickly and easily get market applications that are immediately available to the end user with innovative distribution mechanisms. For example, applications are the continuous provision of software upgrades in cars to have the latest functionalities available - in this way these cars develop as "moving computers" for the transport of people (and goods).
- Internet of Things and sensors. Each package, container, vehicle gets an Internet address with a sensor. This sensor can combine various functions, such as location determination, temperature for perishable load, light for so-called Container Security Devices and movement for determining possible locations where damage has occurred. Expansion of the number of Internet addresses (IPv6) makes Internet of Things possible.
- Distributed Ledger Technology (DLT) or Blockchain. A technology with different properties, such as decentralized use, transparency for all users, not being able to change data and being able to withstand failure of a part of the infrastructure. This allows real-time data in chains to be shared with many users at the same time.
- Robotization. In addition to sensors for Internet of Things, it is also possible to incorporate special purpose computers with specific chipsets (see above) into assets, such as containers and means of transport, so that they can operate autonomously. There is then an autonomous asset that can also transport goods or people. This involves autonomous driving, autonomous sailing and truck platooning, as well as self-organisation, higher load factor and better routing as part of the so-called Physical Internet. This offers the possibility of completely new business models. Within ICT this is also called ubiquitous - or edge computing (-ubiquitous, everything has a computer in it - edge, calculations take place at the edges of the network).
- 5th Generation of mobile communication. The next generation of communication protocols. The use of certain bandwidths and the merging of different forms of communication into 5G leads to more possibilities for increased data volume, better targeting of signals and the further introduction of Internet of Things by the extension of battery life and robotization.
- Quantum Computing. A new form of data storage and computing power, so that data can simultaneously be present at two locations simultaneously and can be further developed into effective measures against cyber-attacks. The Netherlands is making major investments in this area, as well as in quantum storage of data.

Within the context of these new technologies, the development of pull based technology is emerging. Collaboration rules can be developed, whereby parties, for example a government agency, receives direct access to data from companies under conditions (pull) instead of or in addition to the transmission or reporting or duplication of data by companies within supply chains and with governments (push). These pull based mechanisms, based on legally binding agreements, could substantially reduce administrative burdens for business and allow law enforcement agencies to enhance their capabilities connected to risk assessment. Also, within the business process this would allow for substantial administrative reductions between business.

***The power of pull***

*Traditional EDI technologies where economic and administrative entities shared data via electronic messages, rely on 'data push'. This means that the party that has the data needs to take the action of sending it to the next party that needs it, at the right time and point in the data exchange process.*

*Data sharing creates a new paradigm: parties that have data that may be needed by other parties such as their private or public stakeholders will make this data available via a data-sharing platform. In concept this is like a website, i.e. their data is available to whoever needs it, provided that they have the digital security rights to access it.*

*This changes many things. The owner of the data still needs to make the data available but can do so generically and just needs to ensure that potential authorized parties are given the access rights. From there on, whoever needs the data can simply help themselves when they need to and get the data.*

*Why is this powerful? Think of the web again. Anyone with a web browser can access any of the 2 billion websites available today. The choice is theirs to 'pull', i.e. access data from these websites as they wish. Now imagine that we would be using the old 'push' approach? How would we make these 2 billion websites push their data to the right user that they may not even know? It can't be done at that scale.*

*Data pull facilitates data access in huge data networks with the least complexity and effort possible.*

### *4.6 Steps to take*

A suitable legal framework has to be developed on a cross-bordering level, i.e. on an EU and global level, to cover all legal restrictions for paperless transport – getting documents transferred into data, and the re-use of data by supply chain partners as well as authorities. Not all issues - cargo, transport modes and persons – are covered in a suitable legal framework. Increasingly, legal initiatives are being developed.

To deal with the need to counter the threat to close the current open system, various steps can be undertaken. Apart from the application of EU competition rules and additional legislative initiatives, the current information infrastructure needs to be improved to allow for good and rapid exchange of information between all parties in the chain. Therefore, an interoperable, trustworthy and open information infrastructure is required to allow the various actors in the logistic chain to better connect and allow smooth machine to machine data exchange.

To cope with the issues of establishing a common digital language, various steps have to be taken. These steps relate to establishing a common data set and rules for cooperation (protocols). Ideally, all data that companies and public authorities exchange should be developed as a common data set. The most important and innovative step is to derive data requirements from business services

and goals. These latter formulate for instance the type of cargo that needs to be transported, with their data features (e.g. a container of a size and type and with a container number and gross weight). It's a long road before these steps can be achieved. In general, attention is given to the semantics[11] and coherence of logistical concepts that are shared between companies and administrations (also amongst themselves). In addition, rules are laid down to share this data between business processes of any two stakeholders. Collaboration rules may also be developed, whereby parties receive direct access to data from companies under conditions (pull) instead of or in addition to the transmission or reporting or duplication of data by companies to governments (push).

To ensure that small and medium size enterprises do not get left behind in the transition to digital logistics & transport, adequate transition time needs to be factored in. This can be accelerated by stimulating innovation and competition in the area of platform services as a way of increasing the solution options and keeping access costs sufficiently low.

Preferably the following principles for digitalisation of freight transport and logistics should be applied, i.e.:

- Digital by default;
- Use of open source data and open standards;
- Legally anchored;
- Cost-effective solutions (in line with developments in the supply chain);
- Future-proof solutions, considering that every solution requires adjustment to new technological developments;
- "Decentralized, unless", with the emphasis on maximum use of existing IT legacy systems and not on the development of a new system;
- Financial involvement from government in IT developments leads to open source software and open standards that can be applied and further developed by governments and companies;
- Minimum administrative and transaction costs;
- International standards 'by default';
- Equal and international playing field.

### *4.7 Dealing with risks in removing the bottlenecks*

In removing the bottlenecks, sufficient attention will have to be paid to safeguarding risks in the areas of:

- Trust. Data has a high personal or commercial sensitivity. Unlocking this data makes it possible for third parties to generate an extensive, highly detailed and if required customized image and to base their business model on it. An important challenge is to guarantee the integrity of this type of new service of platforms, for example. Identity linked to rules of conduct for data sharing must also be guaranteed to create trust with regard to data sharing.

[11] Semantics helps make sense of all the information available by providing a universal framework to describe and link data. It adds contextual meaning around the data so it can be better understood, searched and shared, enabling both people and computers to see and discover relationships in the data. See Annex 2

In this context, the notion of “chains of trust” that exist between subsequent logistics & transport partners needs to be supported by technological solutions such that parties can retain control over their data

- Accessibility - (controlled) open or closed. Data must be accessible to those who need it, based on common agreements about data structures and meaning in accordance with the conditions of the provider of that data. This is about semantics, standards and their application, exchange techniques and platforms or systems. A concerted effort is aimed at tackling the problem of developing open or closed systems, the role of the government and the privacy issue should provide room for a strategy for using everyday digital services based on the trend towards an integrated platform of platforms in Europe, accessible worldwide.
- Legislation and legal framework. Legislation, such as privacy legislation (GDPR – General Data Protection Regulation) and goal binding, set requirements for data sharing. In addition, legislation also formulates requirements for data, whereby these requirements can change with changes in legislation, for example the consequences of 9/11. A legal framework must support the application of contractual terms such as accountability for data availability and accuracy, responsibility for data driven payments of dues and fees and liability for any consequential damages of decisions made with data from third parties.[12]
- Data quality and integrity. Many companies are still active in getting their data in order. The data quality in data exchange is therefore often focused on supporting a specific function, for example 'transport order' or 'import declaration'. Manual (re-) input of data also often takes place. It has also been found that government organisations often have data of insufficient quality for the performance of their duties. Customs has developed the 'data pipeline' concept for this; US Customs the term '10 +2’ for assessing security risks. The government and the business community will have to work together to share data of sufficient quality with the necessary integrity safeguards for performing various tasks, also in view of the possible further-reaching automation of decision-making (AI).
- (Cyber) Security. An environment for data sharing is needed, where business and government can trust that this environment will also remain available, data does not fall into unlawful hands and unauthorized participants cannot add data. This extends to the level of resources: a fully automated truck must not provide incorrect data, nor may anyone provide a non-existent resource and have that resource provide data. Data sharing and all components involved must be resistant to cyber-attacks.
- Operational management. The operational management of companies is geared towards entering into framework contracts for a guaranteed turnover. These framework contracts most often also address data sharing agreements, especially focused on orders and deliveries, which leads to high switching costs. This requires common, standardized agreements and approaches for data sharing.
- Sustainability objectives. Governments and the business community can work together to develop new systems based on data sharing that contribute to the climate objective by achieving a better load factor in a multimodal context based on the principles of synchromodality.
- From chains to networks. Digitalisation is decentralized and requires no centralized system

[12] Annex 2

solutions. Supply and logistics chains are created in a (global) organisational network. Chains constantly change due to changes in physical processes (e.g. delays caused by disruptions) and changing collaborations (e.g. alliances) of stakeholders. An organisational network can support these chains. Optimal functioning of all actors (things, people and organisations) with cooperation in their environment is central. This holistic approach requires a next generation of data sharing standards and - systems; current systems are aimed at optimally solving a (partial) problem.

- Accessing data at its source. Based on common standardized agreements, data is accessible from a multitude of things, people and organisations. New (demand-driven) services, algorithms and methods can be developed using this data. Having controlled access to relevant data at its source provides agility to government organisations and the business community to respond quickly to changes.
- Investments. Adoption of technology may require major investments. These are a barrier for (large) organisations with existing IT and SME organisations with no or limited IT (knowledge). There are (already) new companies offering services for this, but often this gives a so-called vendor lock in the case of a lack of (open) standards.
- Governance. All parties involved in a data sharing infrastructure will have to be involved in the process in order to achieve cooperation and buy-in. They must be able to individually discuss and understand the usefulness and necessity as well as propose changes towards improvement. This has to do with the fact that data sharing implies a form of cooperation in which the identity of the individual parties can merge with the whole. That is why parties in the development of this infrastructure must always have a positive feeling about " what's in it for me?"

### *4.8 The processes covered*

Data connectivity relates to various information flows. A2B, A2A, A2B and B2B.

1. B2A. This information flow relates to legal requirements to be fulfilled by business in order to accommodate public authorities to execute their tasks. The information relates to cargo, transport and potentially individuals. The information can be delivered to the Administration either through reporting or on request of authorities during physical inspections. In general, most of this information is on paper. DTLF subgroup 1 will make a repository of data requirements. Within the perspective of less administrative burdens there is a tendency towards less reporting and if so, only once. Thus, requiring public authorities to actively cooperate.
2. A2A. Various public administrations obtain information from business. The execution of their tasks is based on this information. Administrations sometimes also add their own data to the information they have obtained from business. Increasingly, in national and international settings, public authorities collaborate and start sharing data amongst each other. The principle of multiple use of data has emerged. Apart from possible legal restrictions - data to be provided by business to authorities are not always allowed to be used by various public authorities – the IT systems operated by various public authorities do not easily allow for data exchange. Agreements between law enforcement agencies to share data, and thus develop common risk management appreciations and interconnected and streamlined inspections, could be created on an eGovernment perspective.
3. A2B. Logistics & transport is often dependent on clearance and approvals from authorities.

Effective knowledge of the status on administrative aspects and possible inspections to be executed helps them plan and manage their operations or deal with issues rapidly and accurately. In many cases these administrative interventions are data driven and may be accelerated by improved data connectivity and access.

4. B2B. Although the movement of freight is and will be a physical process, the management processes of these movements are entirely information driven. The vast amount of information exchanged still uses the paper medium. The drive towards digitalisation is nothing other than a drive towards accelerated transport. Access to data between B2B stakeholders requires improved digital infrastructure and interoperability of freight platforms. This data concerns commercial, operational and compliance information and involves logistics and transport companies as well as financial services such as banks and insurance companies.

# 5 DEVELOPING A FEDERATED NETWORK OF PLATFORMS

Developing a federated network of platforms has to consider various aspects These aspects all provide requirements and constraints for the construction and realization of such a federated network of platforms. This section will address these various aspects.

## *5.1 Platform development*

In its policy choices, the EU will have to benefit optimally from the opportunities digitalisation provides and keep the risks to a minimum. New technologies play an important role in this. An important trend that responds to this is the development of platforms that act as marketplaces. The developments in the field of ICT make it possible to make data in a decentralized way accessible, directly at the source, which greatly benefits the speed, reliability and quality of data, and enables data sovereignty. This digital information infrastructure connects platforms and IT systems. It enables the mutual and secure availability of high-quality data between companies and governments and offers opportunities for structural innovations, new data driven business services and the ability to deal with data differently. Streamlining of processes is taking place to an ever-increasing extent and leads to efficiency benefits (such as improved use of infrastructures, increased load factor and reduced CO2 emissions). The accessibility of data leads to transparency and makes it clear where hidden costs and failure opportunities occur and can be reduced.

## *5.2 The information infrastructure*

The federated network of platforms concept addresses information infrastructure development. The federated network of platforms allows various information hubs and companies to connect and serve as an infrastructure distributing high quality data thus enabling companies and public authorities to develop services and new business. A metaphor for the developments that have taken place in digitalisation for transport and logistics was the readjustment of development within Western cities towards small, fragmented islands of infrastructures. These islands were integrated towards standardized, regulated networks designed to deliver predictable, dependable services across the metropole. In transport and logistics, the information hubs, or islands, comprising different networks do not connect, yet.

The federated network of platforms concept is about developing Europe as an integrated, digitalized metropole in the world for logistics and transport by capitalizing on existing investments. How to get there? To return to the metaphor of the city. The city became a space to be ordered, regulated and configured through managing the interplay of territory and infrastructures. What was discovered at that time was *the idea of society*. A unifying terminology like “society” to establish a federated network of platforms for transport and logistics has not emerged yet. For individuals, “internet” serves as the unifying terminology; some unified term like “World Wide Web of (Supply and Logistics) Data”, “Logistics WWW” or “Internet of Logistics” may propose a solution. The need for an integrated approach to manage the interplay of different transport movements in order to facilitate optimal use of the data available for all stakeholders is emerging.

The importance of infrastructures is in binding different geographical (time-)spaces, while highlighting the complex socio-political and socio-technical arrangements required for their

development. This is at stake developing a federated network of platforms.

### 5.2.1 A metaphor – data spaces

Within data interconnectivity one can either speak of data spaces or a data space that is interconnected or an information infrastructure managing the interplay of data spaces. The imagery of the "data space" like developed by Industrial Data Space seems applicable, initiated by the Fraunhofer Gesellschaft in the context of Industry 4.0. By way of example, those forms of manufacturing represent autonomous operating management systems that make decisions and implement smart production resources independently. The current spurt that China is making in the field of artificial intelligence (AI) and robotics, for example for use in smart factories, was prompted and made possible by the Germans' preliminary work. Meanwhile, two-thirds of the most important investments in artificial intelligence are in China, which means that this country is on the way to developing new AI standards.

The term data space comes from the field of data management and seeks to solve the problem that data from different sources, in this case several business data systems, cannot, or are difficult to, be exchanged as companies use different standards. According to the Fraunhofer Institute, International Data Space is "a data space that uses uniform standards and governance models, in order to specify the safe exchange and smooth linking of data across corporate ecosystems". In this way, a type of World Wide Web of Data is created: different corporate ecosystems are interconnected and interoperable.

This approach is not only applicable to industry but might also be useful for the transport and logistics sector. We also encounter the same basic issues in this sector, aimed at managing data from different sources. Only then will we have to talk about a World Wide Web of Supply - and Logistics Chain Data, or a World Wide Web of Data for Supply and Logistics Chains.

The Fraunhofer Institute provides the following basic elements of the Data Space:

- Data sovereignty. The data owner displays the general conditions under which his data may be viewed and used.
- Secure data exchange. Security with different levels of protection ensures that data is securely exchanged across the entire data chain.
- Decentralized approach. The data space is formed by the total of all data end points that are connected to the data space. There is no central authority responsible for data management for monitoring compliance with the "rules of the game".
- Data management. Possibly the data space is supplied with a distributed architecture and therefore has no central supervisory authority, data governance principles are usually developed as "game rules". These rules are derived from the requirements set by users and determine the rights and obligations that are required for data management.
- Network of platforms and services. Data providers can be individual companies, but also professional "things" from the IoT, from data platforms or digital marketplaces.
- Scale benefits and network effects. Scale benefits and network effects will be of major importance for the success of the data space. The more participants have the data space, the more it becomes the place for data providers, data users and data service providers.

### 5.2.2 Various aspects of a data space for supply chains

A data space for supply chains is primarily a digital business environment[13] in which business is and trade are conducted compliant with regulations, in which products and services are exchanged and financial transactions take place. For that reason, it may be called an economic or commercial space. In addition, it is also a technological space in which software determines the possibilities and limitations and which constitutes of interconnected and interoperable data spaces of individual stakeholders. Moreover, due to the great importance that is attached to liability in logistics and the legislation contained in legislation, it is a legal space. And finally, such a Data Space for Supply Chains can also be viewed as a geopolitical space due to its global size and the intimate interweaving of public and private.

## *5.3 Integrated information infrastructure*

A federated network of platforms and IT systems provides companies and governments with the procedural and technical links to share data of good quality in a decentralized, open and neutral manner. It acts as a basis of trust, so that parties can make data available from their own systems. This results in faster data exchange, multiple use of data, transparency and administrative burden reduction.

In order to be able to use the federated network of platforms, companies and governments will have to organize the functionality of their connection point in such a way that, for example, it is recorded which data they can share with each other. If they find it desirable, they can add additional functionality. They can also decide to share certain data in closed groups, while other data has a broader or more open character.

The development of this federated network of platforms is a process that has been started for a number of years but is impeded by the lack of perseverance power of an independent party. An active role of the governments is required. In this respect, this basic infrastructure is being pursued, both in the EU Member States as well as in the EU, regarding shape and interpretation and enjoying the trust of the market parties.

[13] In this document the term environment has replaced ecosystem that is often used

**To further reflect on the geopolitical aspect.**

To a certain extent, a trading space is always a battlefield, and the way in which government and industry join forces and arrange their affairs has geopolitical dimensions. To understand this, all we have to do is look at China, a country where the Communist Party is leading in practically everything that happens, including business. This means that a level playing field is not guaranteed in Chinese Data Spaces, and that they take it less closely with conditional conditions that we attach so much to, for example in terms of privacy. For the EU Member States and the EU, China is a systemic rival in terms of Data Spaces, a rival that creates its own domains, with rules that are not always in line with ours, and that, among other things through the rollout of the Digital Belt & Road Initiative, tries to attract possible parties within the ambit of its data spaces. These parties can impose discriminatory and priority standards for data exchange and logistical chain design on smaller parties in freight transport. That leads to an uneven playing field in transport.

It could be said that if data is a new oil, then data is also the new theatre of wars, in this case, economic & trade wars.

### *5.4 The platform game*

A federated network of platforms can perhaps best be characterized as a Digital Playfield for Supply chains. Because it is a business environment, the game that is played here will come down to "doing business" and "trading". But beyond this basic game there is another game that is being played in the world of these data spaces, and that is the platform game: which platform is going to control and dominate the business environment. It shows the importance of IT creating new entrants in traditional business and trade.

The platform game is not only played by traditional parties from the world of transport and logistics, such as Maersk or Kuehne + Nagel, but also by new logistics service providers such as Flexport and e-commerce giants such as Amazon and Alibaba. The last two categories in particular seek to change the supply and logistics game as a whole, by changing the way business is done. What they are after is to become the most important director of global supply chains. What they have to offer is primarily convenience, cost efficiency and real-time data integration. A growing concern is the development of monopolies, which mobilizes EU competition legislation.

In addition to the emergence of commercial technology platforms, there are more federated platforms, such as the port community systems. These are more neutral, non-profit-making digital marketplaces on which companies from port communities manage their logistics affairs digitally. Port Community Systems often collaborate with public authorities.

A "platform" consists of a backbone of hardware and software, but that is certainly not its most important aspect - it is primarily a business model. The companies that make use of this revenue model form digital marketplaces, the platforms, and facilitate data exchange between market parties. Every platform, every marketplace, uses its own language (standards) and has its own specific rules. For that reason, platforms can be interpreted as Data Spaces, in the sense as described in this

document.

Actually, the platform game now is the game for allowing as many companies as possible - customers and suppliers in a market - to do business via their own digital marketplace, their own data space. It is a game that determines who ultimately has the largest and most powerful marketplace. This is based on the motto the winner takes all, or, as an alternative, a constellation of many, smaller, autonomous data spaces that are interconnected and interoperable.

### *5.5 Foreseeable bottlenecks*

The international developments in the area of Data spaces for Supply chains are moving at the speed of light. After all, we are dealing here with the introduction of disruptive technologies. It is therefore important to keep moving and speed up the development. After all, global players in the field of transport and logistics are not standing still. Hence, it is advisable to make a brief estimate at this juncture of the expected bottlenecks on the way to a maturity.

As discussed earlier there are various aspects of Data Spaces for Supply Chains to be considered, namely:

- the commercial-economic aspect;
- the technological aspect;
- the legal aspect;
- the geopolitical aspect;
- the generational aspect; and
- the cultural and human aspect, including the threat of machines taking over control.

In which of these aspects of a data space are the most obstacles and stumbling blocks to be expected?

With regard to the *commercial-economic aspect*, the **trust** that is needed for a well-functioning digital marketplace must be emphasized. Trade only flourishes when the data infrastructure really has the confidence of market parties. Only in this way is there enough enthusiasm for such a federated network of platforms and can it get enough scaling.

With regard to the *technological aspect* of the federated network of platforms, one of the major bottlenecks is the current interoperability paradigm that will be implemented by innovative technology leading to less open solutions. The interoperability is based on bilateral or community agreements for applying open standards in practice. It is too time consuming and thus too costly to develop these agreements, which hampers supply and logistics innovations like agility, resilience and synchromodality. Either standardized data sharing agreements have to be constructed specifying (role based) data sharing and - access policies or a mechanism has to be put in place where each participant of the federated network of platforms will be able to formulate its data sharing and - access policies. The latter concept is developed by DTLF I SG2 and will be embraced and in more detail developed by FEDeRATED. There is, however, also the opposite risk: technology can develop disruptively and in unforeseen ways, and when federated network of platforms is set up on a specific technological basis, a next generation or other type of technology can cause the proposed approach to become obsolete. **An open and adaptive technological system with common mechanisms**

**for formulating data sharing and – access policies** will therefore have to be chosen.

***Making Europe stronger***

*To safeguard the further development of the four EU freedoms - movement of goods, persons, services, capital and services – the principle of digital by default is to be applied in freight transport and logistics: paperless transport. The EU Member States have agreed on EU legislation, EU Customs and transport legislation, to foster paperless transport. So far, neither an integrated nor cross sectoral EU approach to enable an interoperable global, EU and national digital supply chain to emerge is required. This integrated approach should not only remedy current bottlenecks as fragmented legislation and no common data language, but also prevent the closure of open market access for public and private operators to data. The EU Commission Von der Leyen is already speaking of the need for EU technology sovereignty. Antitrust issues are reawakening the political discourse when discussing the future of digital Europe. What matters is not a company's market share, but whether its' actions harm consumers.*

Most bottlenecks can be expected with regard to the *legal aspect* of the federated network of platforms. The new possibilities that the federated network of platforms offers come with new relationships and new ways of working, while the legislation is still based on the old situation. To give an example: it is still the case that transporters are legally obliged to pass on information about the goods they are transporting, which is mainly related to liability. When the information is retrieved from the source via a federated network of platforms, that is to say at the origin, the shipper, there is a discrepancy between legislation and reality, so the legislation in this area will have to be amended. The legislation must remain in line with the changing reality, and it looks like the reality is changing faster than the legislation can be adjusted. We are dealing with both national and European legislation, where legislation and the federated network of platforms need to be developed in close collaboration. Of course, the federated network of platforms needs to adhere to a number of commonly applicable Regulations, like GDPR.

No bottlenecks are to be expected with regard to the *geopolitical aspect* of the federated network of platforms. On the contrary, this aspect constantly nourishes the sense of urgency to offer a counterbalance to the "opponents" of Europe.[14]

As we are seeing a new generation of digital natives' progress through the education system, they will be leading the digital economy from a de facto position, i.e. everything that matters is digital. This *generational aspect* could create a new group of marginals in society, both as individuals, companies and economies that are excluded from the digital society. This goes beyond the simple lack of computer skills or understanding of social media, but it will touch the core of business, trade and national leadership. Therefore, a federated network of platforms is an important and urgent step in the digital emancipation of society.

[14] See also page 50

The *cultural and human aspect* relate to digital savviness as well as to the divide between cultures how to deal with digital progress and adaptability. Machine Learning and more specifically Deep Reinforcement Learning are AI algorithms to generate solutions for questions or challenges. Deep Learning requires a large amount of data in which people help to set the algorithms (to 'train'). With Deep Reinforcement Learning, the algorithm gets the basic rules of an application and the algorithm develops independently of human support. An example is chain planning, with the ultimate goal that the algorithm performs better than a human being.

Increasingly, it is becoming obvious that the users of machines are less in control of digital applications then previously assumed. In today's world, subject and object have switched places. The sites, the apps, the ubiquitous platforms: Computers seem to run the show now, and people — mere data subjects — are unaware of the practices behind what is driving their work. Software creates us, our ontic exhaust powering the megacorporate machinery. Perhaps the inevitability of the reversal was always there, coded in the words. The end user, in the end, are in jeopardy of being used.

Entering into the process of digitalization and applying data sharing infrastructure provisions it is important to be in control. Any provision should allow the user to be able to be in control. Also, to prevent worse case scenarios from happening, it is essential to empower the users with the capacities to effectively prevent third parties from taking control. Digitalisation offers a window of opportunities, but also some rather fundamental ethical issues that need resolve. Worst case scenario development should preferably accompany any reference architecture development.

**Towards human-centric data economy**

During its Presidency of the Council of the EU (second half 2019), Finland boosted the growth of the data economy and the utilization of artificial intelligence as part of developing the European single market. The data economy should be driven by the consumer, in other words by the user. A document, Principles for a human centric, thriving and balanced data economy, was issued.

Individuals are guaranteed access to their personal data and the means to manage the reuse of their data without lock-ins or impediments that inhibit access or portability (e.g. timeliness). Users should be given full control and portability of their data, while safeguarding their privacy. Additionally, transparency and clear terms and conditions should be guaranteed so users can understand how their personal data is used in services and automated decision-making (also by third-parties). All stakeholders need to be informed of decision-making employing algorithmic programming in order to understand how data is being used and to take action, for example when agreeing to terms of use or product liability. Empowering individuals to manage their data rights requires easy to use tools:

- to manage access to and the reuse of their data (e.g. consent)
- to increase findability and reusability of user-generated contents (e.g. metadata)
- to change service providers (e.g. relocate data)

# 6 THE FEDERATED NETWORK OF PLATFORMS AS THE FOUNDATION FOR COMPLETE DIGITALISATION

To construct the web of data as described in the previous chapter, where data is stored and can be shared between IT systems of various stakeholders, one global platform will not be the solution, since it might impose many non-functional constraints (e.g. performance, availability) and governance – and business issues. There are already many solutions available that need to be interoperable. The federated network of platforms that makes these solutions interoperable, can serve as the foundation to help realize the full digitalisation of freight transport for all enterprise and increase data quality for authorities. It can be described as a network of interconnected and interoperable platforms, in which all parties involved can share data with each other via their own systems in a controlled and where necessary protected environment.

The solution foreseen is to develop the (detailed technical) specifications of an infrastructure provision and its governance that prides a facility that enables data to be shared. A shared facility.

The major questions about the shared facility are:

- What does the facility do? What is shared? What is being done for that?
- What growth model is in service provision used?
- How do you innovate the service portfolio?
- How is the facility being implemented?
- What is the business case?
- What is the business model?
- What are the conditions of use?
- How is the governance organized?

These questions will be further elaborated and when available, answers will be provided that give direction to the project.

## *6.1 Functionality of the facility: what does the facility do?*

The users of this infrastructure are enabled to do business safely and confidently in line with laws and regulations that make digitalisation possible. Companies that are in the early stages of digitalisation can be involved. Specific functionalities and value-added functions are not part of this infrastructure. After all, it is a basic digital information infrastructure by providing primary functionality for constructing the web of supply and logistics chain data. This infrastructure gives companies the opportunity to create added value and develop new services that allow companies to differentiate and cover specific customer needs.

The facility provides a number of services (the service portfolio) to end-users, both enterprises and authorities. On the one hand the service portfolio supports business (B2B data sharing), on the other hand the service portfolio supports administrations (B2A, A2A and A2B data sharing).

## *6.2 Involvement of public administrations*

Within the concept of eGovernment, EU Member States try to improve the communication of

companies with governments and also between public authorities. It is necessary that the public authorities can operate as one entity towards the market and companies. The mutual availability of data is key. It has two dimensions:

1. Reporting - for the legally required reporting of information to Administrations, the principle that companies report data once and this data is used multiple times is applied.
2. Control - for the legally required information that business needs to present in case Administrations control, the principle is that data need to be available and accessible by the Administration before a control physically takes place.

In both cases, the data need to be presented in a harmonized and M2M readable format. A major requirement is application of the digital-by-default principle. The M2M readable format would allow a federated government platform approach to be developed, based on decentralized connected IT systems facilitating seamless data exchange between governments and with companies. This fosters cooperation between the authorities, including the various supervisory government organisations, and allows for the coordinated implementation of inspection and supervisory tasks and also improving services to companies (e.g. status information and one-stop shop treatment).

The federated network of platforms approach – also allowing interoperable government platforms to be developed - constitutes the overarching reference architecture for the implementation of the Customs legislation as well as the European Maritime Single Window environment (EMSWe) and electronic Freight Transport Information (eFTI) Regulations. Within the context of these EU legal provisions, but also in connection to other legal provisions as the Union Customs Code, the FEDeRATED Vision of providing for a data sharing infrastructure provision based of the need to enable business and public authorities to make data accessible to authorised users should preferably apply. This provision is based on a set of agreements and technical applications (e.g. API's) and a pull-based mechanism, called Publish and Subscribe. From this perspective, the implementation of the EMSWe or the eFTI should be rather perceived as services derived from such an infrastructure provision, than a stand-alone infrastructure provision. All these services enable a seamless EU multimodal freight transport/logistics chain to emerge.

The basis to enable a federated government platform is the (legally acceptable) reuse of data provided by companies for optimization of risk management, deployment of people and trade facilitation. To this end a dedicated access (or entry) point for the government with business and business with the administration is required to enable the exchange digital data (send, receive, retrieve, make available). It is a kind of IP address, which, just as in the Internet, must also be registered and findable.

In figure 4 hereunder, the concept of a dedicated visibility and access point is illustrated. This figure could also apply for the development of the eFTI Platforms allowing accessibility through visibility and access control rights to public authorities. The semantics for the upload and download functionalities are to be developed as well as the URI's (Uniform resource Identifier) to unique links in business data (e.g. CMR number, container number etc)

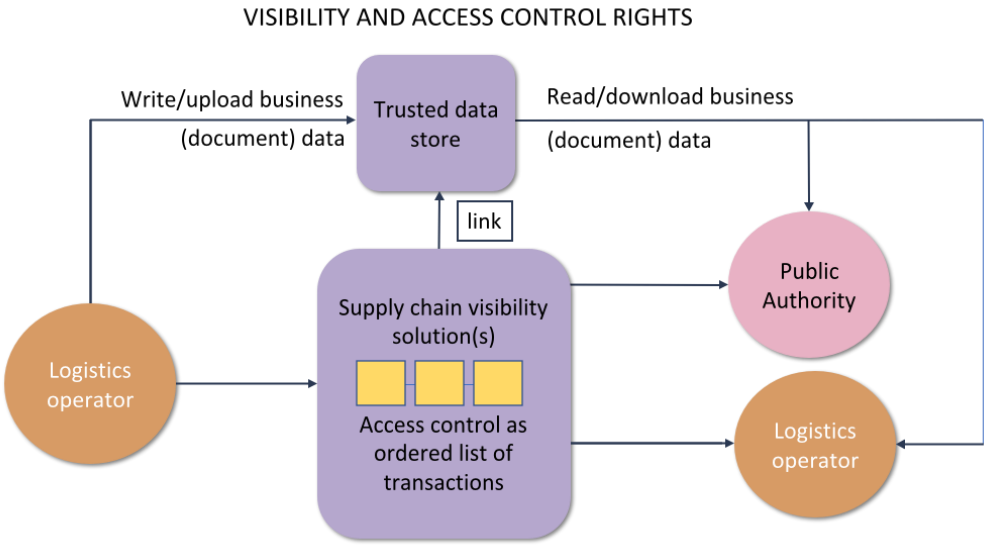



*Figure 4: Visibility and access of data through dedicated entry*

This access, terminal point, determines how you can share data, the syntax. Government agencies should be able to find the connection point of companies from their connection point to retrieve data or access data. This federated government platform will have to be designed in such a way that in the long run not only data between governments and companies can be shared but can also fit into a federated network of platforms that enables data sharing between companies. The design of the federated government platform should apply the general FEDeRATED reference architecture principles. This will also define the need for application of a publish/subscribe mechanism, the subscription structure and the event data structure for supply chain visibility.

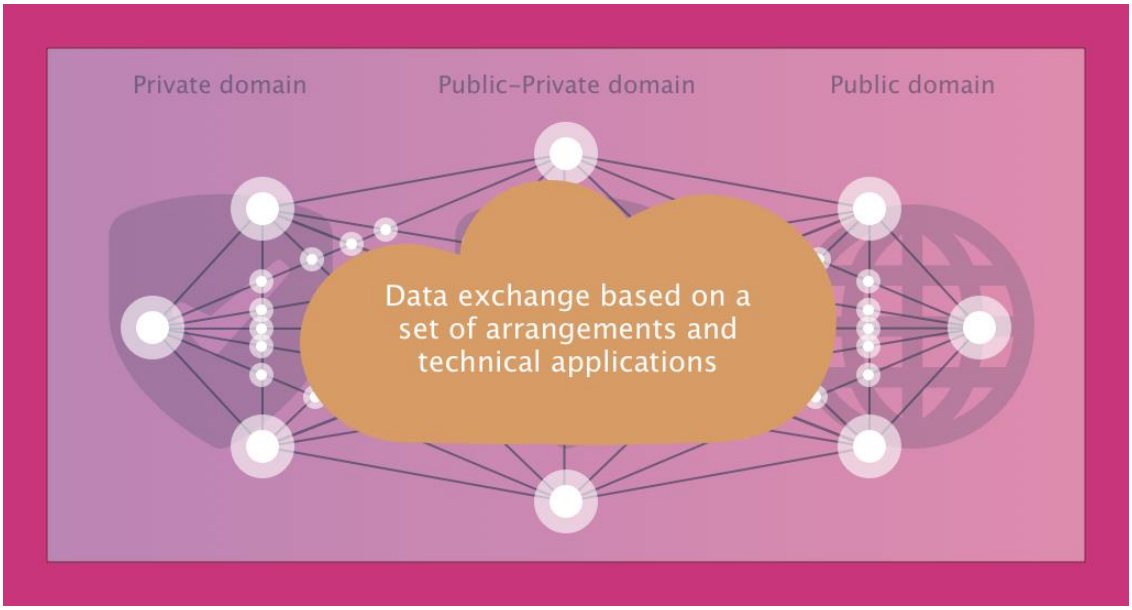



*Figure 5: The concept of a federated infrastructure provision approach*

In the figure above the A2A, B2A, A2B and A2B opportunities to allow open data-exchange for all based on a Core Operating Framework systematic application of data access rights is illustrated.

### 6.3 Growth model of the service portfolio

One of the strengths of the federated network of platforms is a gradual implementation of the services. The growth model of the service portfolio of the facility means that the interests of the parties are taken into account, that data sharing offers added value and sufficient account is taken of possible pitfalls and uncertainties. Such a growth model will have to provide any of the services that are not yet (widely) implemented by existing systems and solutions but have a clear business case. This implies that existing platforms will also be enabled to extend their existing service portfolio with new services.

Analysis of many EU funded and national projects, literature, and of the proposed Living Labs in FEDeRATED learn there is a real business case for supply chain visibility. Although there are already initiatives that develop and provide these services, visibility services are not widely implemented and used by relevant stakeholders. These visibility services can be the basis for sharing spare capacity for booking and ordering, thus contributing to sustainability goals.

From an authority perspective, new regulations like European Freight Transport Initiative (eFTI), European Maritime Single Window environment, and ICS 2.0 provide the opportunity to develop a service portfolio for compliance (B2A) with its roots in supply chain visibility.

Since the service portfolio developed for the shared facility will not address existing services from the start, there must be a migration strategy by, for example, supporting existing standards and integrating with platforms. A gradual transition of existing services to the service portfolio of the shared facility, which functions as a network of existing platforms and IT systems, is desirable. It offers companies and government the opportunity to transform, while new services and applications become available. It also provides a better integration of all modalities, thus enabling the multi-modal shift and synchromodality.

### 6.4 Service portfolio innovation

Another strength of the federated network of platforms is its preparedness for new services, the extension of the service portfolio (future proofing). Extension of the service portfolio is required from two perspectives, namely the introduction of new regulations requiring (access to) data and of new technology. Technology considers two aspects, namely the introduction of automation of assets and of innovative IT technology building upon the shared facility.

This strength is based on a distributed experimentation, development, and validation environment, where the results of innovations can be fed back into the service portfolio. FEDeRATED will provide foundational concepts and collaboration procedures that enable innovations of the service portfolio. Existing platform providers might need to innovate their technology or find other ways for rapid implementation of these new services of the service portfolio to address business and authority requirements.

In the figure 6 hereunder it is illustrated how a federated infrastructure provision allows not only seamless data exchange, but also service portfolio innovation.

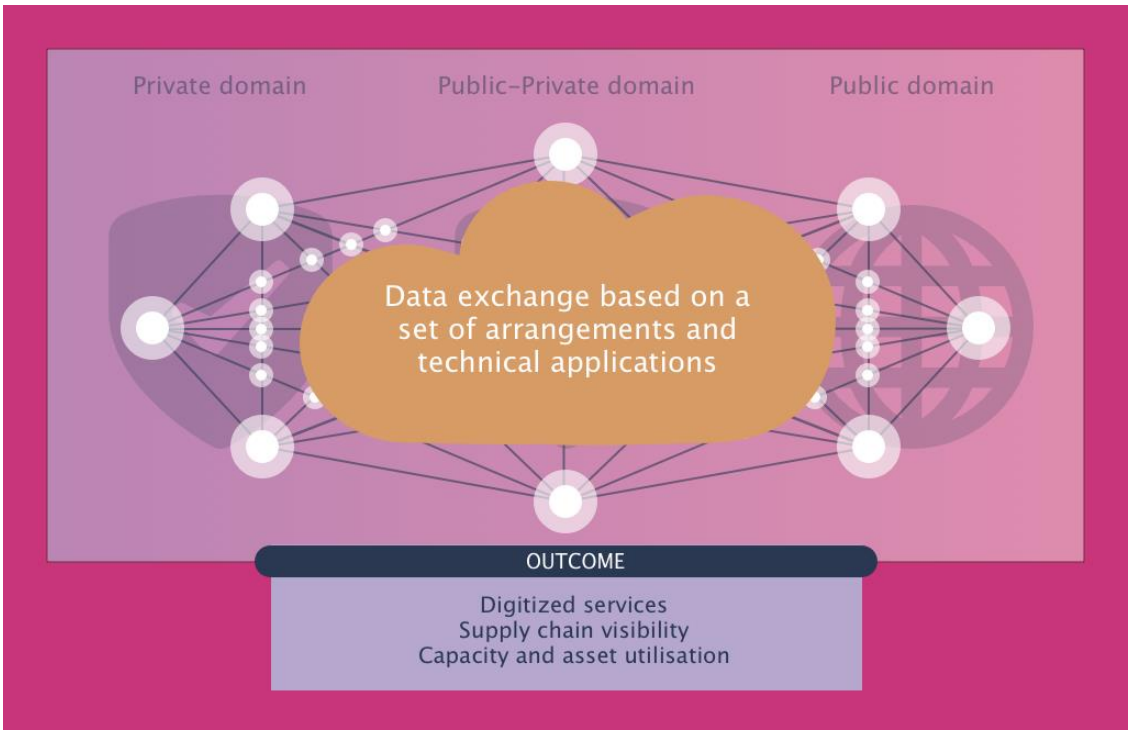



*Figure 6: The federated infrastructure provision allowing service portfolio innovation*

### 6.5 Implementation of the shared facility

As stated, the shared facility is a set of (detailed technical) specifications with a governance structure. The shared facility can be implemented by many existing platforms and solutions, including peer-to-peer data sharing, with existing or innovative technology. There can also be a distinction between private -, public -, and combined (public-private) implementations of the shared facility. These implementations are all about the governance (and business) model of platforms and solutions.

For instance, a public shared facility implements the compliance functionality (B2A) of the service portfolio, interconnecting via protocols to implementations of the shared facility with a private governance model, and may additionally implement data sharing between different administrations (A2A), for instance in the context of the Maritime Single Window and upcoming eFTI Regulations or ICS 2.0 of EC DG Taxud. The implementation requires protocols.

By distinguishing the service portfolio and the protocols, service innovation is enabled from different perspectives like in the private – or the public domain.

### 6.6 The business case of a federated network of platforms for the EU

A lot is at stake for the EU. The number of data flowing in and out is increasing. It is expected a tsunami of data will flood Europe and allow for interoperability.

In the context of the realization of an EU digital internal market, the EU is working on the development of a data sharing infrastructure. With the rise of digital power concentrations from North America –

'business model' market dominance and capital appreciation – and from China – 'business model' global expansion and national security for its internal market and society – the EU can position itself with its own 'business case and – model'. Digital resistance, level playing field, employment, sustainability, (cyber) security, and privacy protection are important elements in this. A federated network of platforms will thus also enable innovation in the EU, which develops and stimulates employment.

It is very unlikely that European companies will independently take the initiative to realize and implement this shared facility. Digitalisation requires major investments, both the shared facility and the digital transformation of companies and government. These are a threshold for (large) organisations with existing ICT and for SME organisations with no or limited ICT (knowledge). The 'business model' of this shared facility is based on the public interest that the government has, together with citizens and businesses, to allow the blood in the veins of the world economy, but especially of Europe, to flow freely and to 'everyone keep on board'.

### *6.7 The business model of a federated network of platforms for the EU*

To realize the objective of a shared facility, the public sector may take the initiative by developing and implementing the public part of the service portfolio in such a way, that the private part of the service portfolio only needs limited extensions and thus investments. The shared facility implemented by a basic data sharing infrastructure can thus also be used by business (B2B). There is a case for the public sector to consider i.e. public private partnerships in order to bring some order to the digital revolution that has been, and still is, driven by the private sector, often without shared goals and values.

### *6.8 Conditions for use*

A shared facility must be open to all stakeholders, providing a level playing field from the public, EU perspective and creating the EU digital single market. However, there will be conditions not only for its use but also for providing (part of) the service portfolio. Trust is at the core of the facility: trust in end-users (are they really who they say they are; identity), trust in platform providers (do they not sell or manipulate data), trust in value added service providers (do they adhere to rules of re-use of data), and trust in sharing the data between the various systems (security). These aspects of trust address issues like passive and active attack to systems, where passive attacks address unauthorized access to data and active attacks changing data, misuse of identity, etc.

In this context, the complete shared facility and its components has to be able to cater with other types of cyber-attacks, that have an impact on non-functional aspects of the shared facility like performance and availability. These will impose requirements to implementation of the shared facility.

On top of these aspects of trust, there is also the aspect where each end-user also behaves according business rules (enterprises) or governance rules (authorities). Reputation management can be a means to facilitate this type of trust; reputation management is currently not foreseen as part of the service portfolio of the shared facility.

In this context, it is up to all end-users to protect their data, where the data is stored in a secure

environment. Access control needs to be organized locally by each stakeholder. In case a stakeholder stores its data by an external (cloud) provider, the same conditions as for sharing data have to be applicable.

The eFTI Regulation already addresses a number of these trust related issues that might be implemented by a certification framework.

### *6.9 The governance framework*

Not only the specifications of the shared facility should be part of governance, but also all other solutions with functional and non-functional requirements need to be part of a governance framework. Such a governance framework also needs to address service portfolio innovation, see before. A governance framework might consist of an organisational structure with participation at various levels, national, association, international, but potential also regulations and standards for the technical specifications.

In general, the governance should cover:

- Defining Boundaries;
- Balancing the Benefits and Costs of Resource Usage Managing;
- Sanctioning resource to these users (i.e. by constitutional right holders);
- Devising and Modifying resource Usage;
- Conflict Resolution mechanism.

The legislators and standardizations bodies need to collaborate with end-users in this governance framework. The governance is one of the components to work out. It can vary from a simple system of agreements and some "gentlemen's agreements" to a highly regulated whole.

# 7 DESIGNING A FEDERATED NETWORK OF PLATFORMS

## 7.1 Towards a federated infrastructure configuration design

The long history of infrastructure development can be summarized in three configurations, in which stakeholder constituencies take different lead roles and responsibilities for IT decision making. IT decision making relates to the infrastructure, future development, and potential value-added applications based on data sharing. These configurations can be combined in any possible way. The infrastructure typology can be given as:

- Centralized (platform) configuration - IT decision-making authority concerns the infrastructure, applications, and development. A centralized solution supports more than one organisation in data sharing (we don't address centralized configuration within a (multinational) organisation). Development of value-added applications will depend on authorization of data owners using a centralized solution.
- Distributed (peer-to-peer) configuration - IT management and organisation management have the authority for the infrastructure, applications and developments. In this perspective, infrastructure, applications, and developments for data sharing only are in scope.
- The federal configuration - (a hybrid configuration of platform(s) and peer-to-peer solutions) where IT decision-making is done at various levels and overlapping functionality exists.

Advances in ICT have increasingly led into networked organisations, requiring a federal configuration of the infrastructure. Processes of social production have caused the creative splintering of infrastructures. Online horizontal networks have become a fundamental dimension of everyday life built around user-driven initiatives and interests. Currently, all the inputs necessary for effective productive activity are under the control of individual actors.

## 7.2 Infrastructure layers

In line with the European Interoperability Framework (EIF), an infrastructure consists of various layers. These will be discussed in this section. A layered approach is not only taken by the EIF, but also is the basis of the success of the Internet. Agreements on different layers can be made, enabling particular functionality that could be developed by individual organisations. The EIF is also the basis for the platform game.[15]

[15] **The EIF gives guidance**, through a set of recommendations, to public administrations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that existing and new legislation do not compromise interoperability efforts. COM(2015) 192 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, Brussels, 06.05.2015.

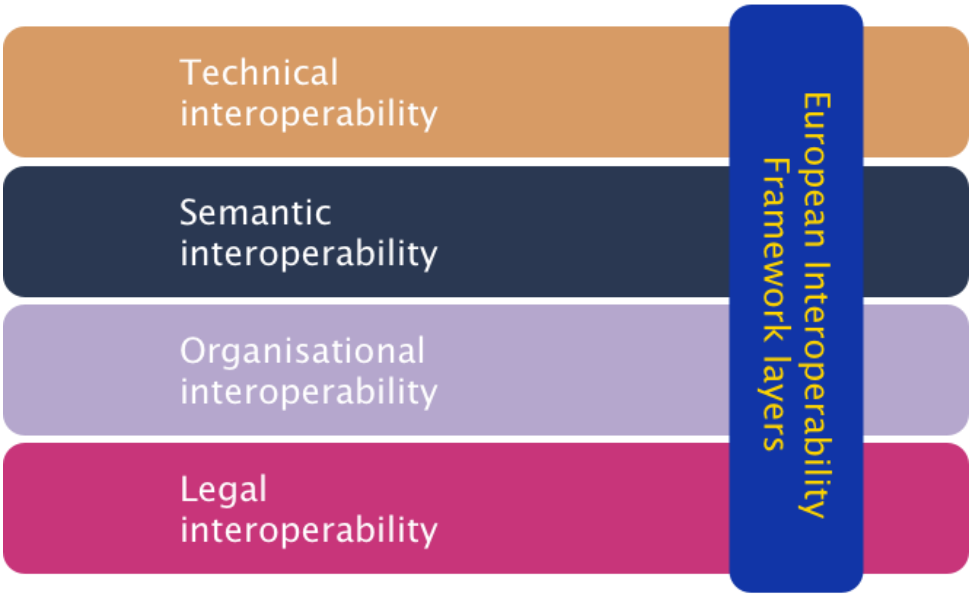



*Figure 7: The EIF four-layer interoperability approach*

The *technical layer* providing technical interoperability is the best-known. It supports functionality like push (messaging), pull (APIs – Application Programming Interfaces), (temporary) data storage, generating notifications supported by publish/subscribe, etc. These different mechanisms will have requirements regarding communication protocols. Most notably, also the syntax as data carrier, the technical structure for organizing data during its exchange, can be agreed upon. Well known solutions like XML, EDI, and JSON are mostly supported by the technical layer.

There are sufficient general-purpose functionality and technical protocols available to support the technical layer, for instance the eSens Delivery functionality for reliable and secure data sharing. Some functionality can also be (and is) offered as a service, e.g. transformation functionality. Thus, technical interoperability is about making choices as to which functionality and protocols will have to be implemented.

Agreement on *semantic interoperability*, the second layer, addressing the context and business processes for sharing data, will be more difficult to agree. It concerns the aforementioned processes such as ordering, visibility and all types of compliance (security, safety, VAT, etc.). This semantic layer will provide particular information services that support business services. These information services should be identical for all implementations participating in the federated network of platforms, independent of the configuration typology. Business services are part of the third layer specifying organisational interoperability.

Since we are facing a federated configuration, individual solutions (platforms and peer-to-peer) need to be able to share data; they have to be interoperable. This interoperability in a federated configuration can only be achieved by harmonization of the semantic layer across configurations.

With respect to solutions at the semantic interoperability layer, choices have to be made, based on the leading principles and supporting organisational interoperability. If for instance, a choice is to

specify only interactions between any two stakeholders as described in the DTLF I SG2 final report, business process choreographies have to be developed specifying interaction sequencing between those organisations.

The third layer, *organisational interoperability* enables data sharing from the perspective of business services, where value exchange according these business services, i.e. business transactions, has to be compliant with regulations. Information services specified by the semantic interoperability layer, support actual data sharing for business services. For large scale adoption of FEDeRATED, and its concepts and solutions developed by DTLF, the business service approach provides a common, innovative way of specifying one's data requirements only once and drastically reducing the time required to come to data sharing agreements. This time reduction is required to support all types of goals of individual organisations (e.g. agility, resilience, synchromodality) and of the society as a whole (sustainability, safety, security, etc.), thus enabling dynamic constellations of supply and logistics chains in organisational networks.

Organisational interoperability requires new components with interfaces to existing solutions. They need to interface with the semantic interoperability layer to be able to specify data requirements for business services. New components have to address the registration of business services of stakeholders, data – and process requirements or constraints stemming from legal interoperability, etc.

The fourth layer, *legal interoperability*, will need to be developed during the Action, integrating with various existing Regulation like the aforementioned GDPR. These can be privately governed legal code, e.g. Rotterdam Rules for shipping containers by sea, or publicly governed, e.g. the aforementioned GDPR and ICS 2.0 as an example. These can also be local regulations like city access restrictions controlled by a municipality. Authorities implementing these Regulation not only have to make these Regulations available in a means to have them rapidly and uniformly implemented in the federated network of platforms, e.g. data – and process requirements, but also have to formulate how they will monitor compliance, e.g. push (message) or pull (publish/subscribe and/or linked data).

Additional to these four layers, a *supporting layer* is required enabling trust, security, registration, and auditability of data sharing. Identity - and Authentication Providers are organisations that provide functionality that increases trust in the total solution. The supporting layer functionality will differ for each of the other layers, e.g. the semantic interoperability layer will require a data dictionary with semantics and the technical layer a dictionary of data carriers and their support of the semantic interoperability layer.

### *7.3 Technology – federated network of platforms*

The technology provides particular services (DTLF building block Technology Independent Services) that enable business benefits. To achieve this, the platforms have to become interoperable and IT systems of individual stakeholders will have to integrate with a platform of choice according the plug and play building block of DTLF.

The Technology Independent Services are specified in such a way that they provide business benefits. These business benefits might be specific to for instance a modality or a type of cargo (e.g.

dangerous, bulk, containers), which implies that the standards for data sharing also are specific to support these business benefits. The objective of FEDeRATED is to make these standards compatible to allow for interoperability amongst several modalities and cargo types, in line with DTLF. The plug and play is one way to achieve this, another way is to utilize standards at meta-level, according the following requirements:

- Meta-level standards shall allow the creation of mode, cargo type, or other specific standards
- Meta-level standards shall allow the re-use and extensibility of existing standards.
- Meta-level standards shall enable the utilization of tools of choice by specific communities or end-users

DTLF I SG2 proposes some of the meta-level standards like Ontology Web Language (OWL) for modelling semantics and Business Process Modelling notation – choreography (BPMn) for interaction modelling between any two stakeholders. These meta-level standards, which are used to create standards for data sharing in logistics, thus should be open standards supported by tools.

To enable compatibility of specific data sharing standards, there are four constraints:

- The standards have to be based on commonly used concepts. The concept 'business service' to reflect value propositions as defined by DTLF I SG2.
- A layering of semantics should be created where what one could call the foundational layers contain all relevant concepts that are independent of any specific application. The following layers could be identified (to be detailed in the master plan):
    - Technical Model. Common representation and restrictions for representing basic concepts at a technical level. Examples are the representation of weights and currencies, but also codes like country codes and codes for packaging types.
    - Common Logistics Model. The common logistics vocabulary should be derived from a core logistics model, specifying the core logistics concepts and their properties (data – and association properties). Examples of what could be in the core logistics model are concepts like 'cargo', 'equipment' and 'transport means', that can be further specialized.
      The Common Logistics Model has to contain the concept 'business service' that has to be independent of any domain specific model.
      Properties of common logistics concepts could be specified by the model reflecting the CCL and code lists. This separation allows to identify the minimal logistics vocabulary, building upon others.
    - Domain specific model, which contains concepts with their properties that are specific to a particular application area. A domain specific model can build upon the common logistics model or another domain specific model. Besides reflecting domain specific requirements like for a modality or cargo type, these domain specific models could also reflect data sets of business documents that serve as legal contracts.
- Embedding of compliance regulations. The above-mentioned models should contain all specific rules and data requirements for compliance to international and (potentially) national/local regulations. These regulations address for instance safety and security when using the infrastructure, improve the utilization of that infrastructure (e.g. traffic – or corridor management), and compliance to trade agreements and VAT. Local regulations could for

instance be on restrictions imposed by municipalities for city distribution.
These regulations lead to data requirements (push and/or pull) at specific milestones, or more general, on authority demands (e.g. geofencing for dangerous cargo movements).

- Re-use of existing standards. As much as possible, existing standards for data sharing should be re-used when creating the previous layers of models. These are for instance (to be completed in the master plan):
    - UN CEFACT Core Components Library (CCL). This contains a lot of technical representations that are the basis for the Technical Model. The CCL should be converted into an ontology representing the Technical Model.
    - UN ECE Recommendations. There are a lot of code lists (e.g. country – and packaging codes) that are used in practice. These have to be re-used an integrated with the CCL in the Technical Model.
    - UN Trade Data Elements Directory (UNTDED), which contains a number of agreed terms as a basis for constructing the Common Logistics Model.
    - Existing data models and ontologies. There is already a number of data models like WCO with quite a lot of concepts and their properties, and there exists already an ontology for data sharing in freight transport by air (OneRecord). Concepts and properties defined by those models should be as much as possible be re-used to construct the common model and potential one or more domain specific models.

Adhering to these constraints, communities should be able to specify their domain specific models. Procedures will have to be developed as part of governance.

The aforementioned semantic models should support the interaction types identified in a choreography. The master plan should identify how these interaction types should be represented, for instance by a set of rules (e.g. a transport booking should contain at least two places, dates and times and an indication of the cargo to be transported) or by an ontology of their own (e.g. an ontology representing a transport booking).

The aforementioned semantic models should also be the basis for (see also DTLF I SG2):

- Generating APIs to support the choreography. This requires that for each interaction type identified by a choreography, one or more APIs have to be generated. The Master Plan should specify examples of APIs for particular applications (e.g. supply chain visibility) and provide rules for generating these APIs.
- Data validation and – quality assessment. The APIs should come with a technical representation for validating the data shared by an API. These validation rules can be given by an XSD (for XML data) or by SHACL (for RDF data).
- MyOntology. Individual organizations should be able to define their view upon existing models by selecting a particular model for support of their business services. They could select for instance domain specific model and generate their specific ontology.

# 8 THE CORE OPERATING FRAMEWORK

In the preceding sections much has been said on how digitalisation has structurally initiated a transformation in the way in which freight transport and logistics will operate. Numerous examples have been provided on how digitalisation offers a window of opportunities and benefits for both government and business.

It has also been shown that there are several bottlenecks that have to be overcome, mainly focused on interoperability issues, if seamless data flows and a level playing field is to be realized.

Further, it has been shown that the “solution of choice”, i.e. the federated network of platforms, has the potential to address the limitations afforded by current capabilities and practices. However, the federated network of platforms relies on a sound development that considers all interoperability issues in a consistent and coherent manner. Further, if boundaries are required, e.g. regarding scope (or extent) of such a federated network of platforms, then this can be inferred from the points addressed in the Vision, in particular chapter 2.

To achieve this ultimate goal of interoperability at different layers, certain basic “rules”, agreements or requirements need to be agreed by data users and IT providers. The overarching conditions needs to be set. This is done in the Core Operating framework.

The “Core Operating Framework” sets out:

- within the given context of the Vision, key principles that need to be adhered to in order to ensure that the interoperability issues are safeguarded in such a way as to enable a federated network of platforms approach.
- the high-level requirements that should be applicable to the interoperability layers and be constraints to formulating the leading principles as part of the Master Plan.

The next stage is to further elaborate upon the high-level requirements.

The Core Operating Framework will also be used to derive a number of the validation criteria for the FEDeRATED Master Plan and Pilots/Living Labs.

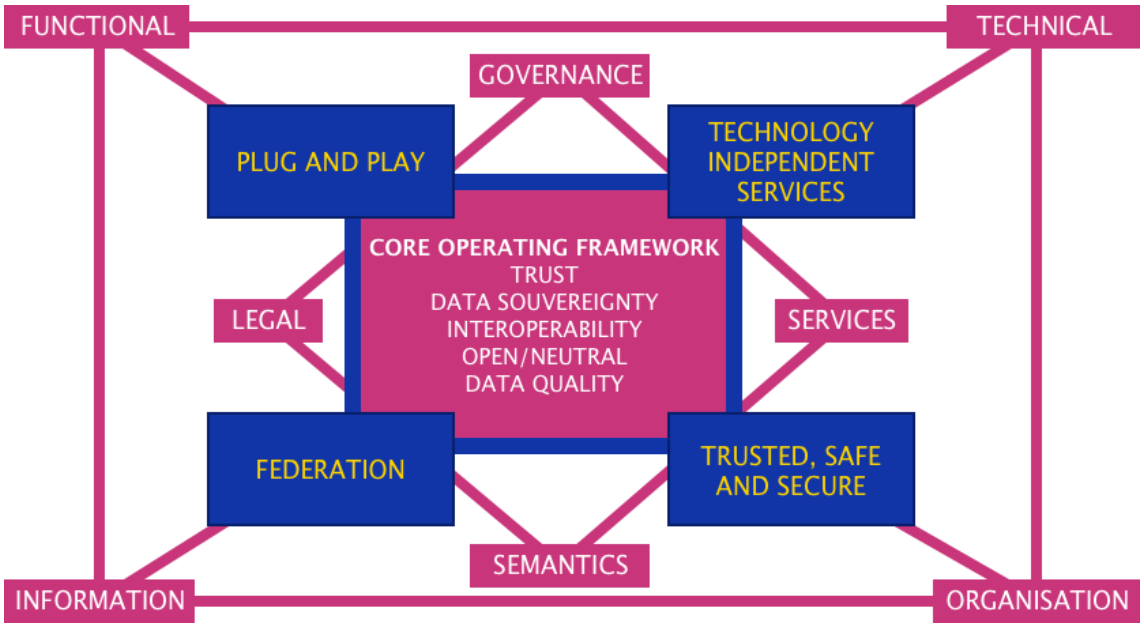



*Figure 8: The DTLF design principles in relation to the Core Operating Framework to be elaborated on the Master Plan Leading principles*

The further development of a federated network of platforms has to rely on the comprehensive consideration of certain definable design requirements as well as legal and organisational boundaries, constituting the following key principles:

1. ensure data sovereignty and data quality;
2. create trust among platforms and participants;
3. provide a framework to enable interoperability;
4. be open and neutral to any participating party;
5. rapid deployment of new IT services to support business processes.

Within the context of these key principles of the Core Operating Framework the following issues have to be developed:

- coherent and comprehensive legal interoperability requirements;
- governance;
- organising principles;
- layering approach;

The above forms the high-level “Core Operating Framework”. In general terms, this Framework is further elaborated in this Chapter. More in specific the Core Operating Framework will be further developed through the leading principles. These principles will be elaborated and validated through pilots and testing beds in the FEDeRATED Master Plan.

## *8.1 Ensure data sovereignty*

The data that is exchanged by the infrastructure is made available by the owner of the data through a push/pull mechanism. The data is then consumed based on pull/subscription mechanism or received as a push by any authorized recipient. A data owner grants access to the data then to the

authorized recipient. It is also worth noting that the data is not retained by the infrastructure as the data is only available at the source through a reference/Unique Resource Identifier (URI) or pushed by messages, unless this is required as a temporary solution for data sharing. For instance, temporary data storage is required in case a data owner submits data (publish) and a recipient is only able to receive messages.

Data sovereignty should be further explored in the semantics interoperability layer, where this layer supports the organisational interoperability layer. There might be a particular classification of data, where data can be considered open (I.e. publicly available), for instance timetables, traffic data, and voyage schemes, data is only shared in a commercial relation between any two stakeholders, e.g. order data, or data has to be made available to one or authorities. Yet other data will be classified as internal data that is subject to internal authorization rules. Data classifications are driven by for instance legal and commercial constraints.

Each stakeholder will formulate its own data sharing and – access policies, using the aforementioned classification that needs to be developed in the FEDeRATED Master Plan.

### *8.2 Create trust among platforms and participants*

The infrastructure should contain various mechanisms, service and solutions that contribute to trust in using the infrastructure. Not only should users be identified, but also particular active attacks to the complete infrastructure should be prevented. There are various issues to be addressed, depending on user requirements with respect to data sharing. Data privacy should also be respected, and data sovereignty should be adhered.

### *8.3 Provide a framework to enable interoperability - seamless interoperability*

The federated network of platforms will have to enable interoperability amongst all stakeholders, providing a level playing field. Interoperability should be seamless, meaning that each user of the federated network of platforms should be able to do business digitally without making any additional data sharing agreements. There should be a mechanism during registration at which each organisation will be able to formulate its data sharing policies, expressed in their business services, timetables, voyage schemes, distribution patterns, and what you have. These mechanisms should be supported with results of the semantic interoperability layer (see before).

### *8.4 Be open to any participating party*

The infrastructure for data sharing in supply and logistics should be open for anyone to use. The FEDeRATED Solution should be easily accessible for any parties, where each party can make the choice to implement the FEDeRATED Agreements themselves or connect to a platform that implements these agreements.

This requirement results in the Technology Independent Services (or standards for the Information Services of the federated network of platforms Agreements) and requires platform interoperability, two of the four design principles agreed in the DTLF.

## 8.5 Rapid deployment of new IT services

Technology allows for a rapid deployment of new IT services (APIs) to support business processes. Many examples are available for consumer-based applications on smart devices; the concept of rapid deployment of IT services for business process support is not yet implemented. Examples of this type of rapid deployment are in crypto currencies such as BitCoin; another one would be Connected Logistics Chain developed by Ericsson. It refers to a layered architecture (see further on) where once agreement is reached on a relevant IT service by a user community, they are able to deploy this new IT service almost instantaneously. It requires a governance structure with agreed procedures that support the various user communities and/or (modality specific) associations.

## 8.6 Data quality

Data quality has different dimensions, for instance completeness, correctness, and consistency. Data quality also needs to be considered from different views. For instance, authorities like customs would like to have a full view of supply and logistics chains, which includes parties involved and cargo objects with its movements (place and time). This also involves consistency: inconsistency between data received from different stakeholders may give rise for actions, both from an authority and a business perspective.

Data quality is required to meet all goals in supply chain synchronization, innovation, and other opportunities. Thus, it is crucial to improve data quality. Data correctness might be enforced based on more technical representations that can be implemented by IT systems. Enforcing data correctness will increase data quality but might decrease the data volume that is shared and made available to for instance authorities.

## 8.7 Supporting elements to the key Core Operating principles

### 8.7.1 Set out coherent and comprehensive legal interoperability requirement

Legal aspects need to be developed especially for data sharing and interoperability, also considering any legal constraints that need to be implemented like the aforementioned GDPR. Potentially, new regulation has to be developed or other regulations developed for more generic data sharing issues needs to be adopted by supply and logistics. Issues like liability need to be addressed, re-use of data, etc. Since much data is re-used in logistics chains, also data ownership needs to be established. Depending on the delivery terms in these chains, ownership of data might also be transferred from one stakeholder to another. The main question arises the identification of the stakeholder that is in the end responsible for the data that is shared with others.

### 8.7.2 Ensure governance

Given the increasingly large-scale nature of information infrastructure projects, it is essential that individuals (and the communities they represent) at multiple level are engaged in the decision-making process. A key objective of the governance is to ensure synergies to occur and associated benefits are reaped.

In general, the governance principles for a network-based infrastructures development should

contain:

- Defining Boundaries – The boundaries of the information structure and those individuals or groups with rights to infrastructure resources should be clearly defined;
- Balancing the Benefits and Costs of Resource Usage – Operational rights specifying the types of infrastructure resources that a user can access should be directly linked to local needs and conditions concerning work practices, available technologies, information, and/or money inputs;
- Managing and Sanctioning resource– A system monitoring resource image should be implemented by the users themselves. Users who violate rules should receive gradual sanctions (depending on the seriousness & context of the offence) from other users and/or official accountable to these users (i.e. by constitutional right holders);
- Devising and Modifying resource Usage – Users should have rights and modify the rules determining the use of infrastructure resources. These rights should not be imposed by external authorities (e.g. the state);
- Conflict Resolution mechanism – Users and their officials should have rapid access to low-cost, local area arenas to resolve conflict among users, between users, and between their officials, and infrastructure providers.

### 8.7.3 Organising principles

It may be required to further investigate structural - and emergent properties of for instance the Internet might be applicable. These properties are:

- Organising principle - layering of IT capabilities, where a layer can be provided by multiple platforms, IT capabilities, and social groups that design, implement, and maintain its functionality. A distinction can be made between end-user functionality and data sharing functionality, where this latter is for instance developed by International Data Spaces or as open source by development of Distributed Ledger Technology. It also implies that data is shared syntactically by an open standard like GS1 EPCIS, WCO, or UN CEFACT and semantics is shared by another technology.
- Control - the design is distributed among a large set of designers, user communities, and forms of governance. In Internet, there are several communities contributing to the design like IETF (Internet Engineering Task Force), W3C (World Wide Web Consortium), ERA and IANA (Internet Assigned Numbers Authority), RIPE NCC (Réseaux IP Européens Network Control Centre) and OASIS each with their own governance structure but agreed coordination mechanisms. Similarly, the end-user functionality might be developed by organisations like IATA (air transport), WCO (customs), and IMO (sea transport), also with common agreed coordination mechanisms (see the governance section).
- Shared - the infrastructure is used by an increasingly growing number of heterogeneous user communities, designers, regulators, and other social actors. These user communities, etc. should be enabled to specify and implement their specific requirements. This requirement is for instance supported by the app store of Apple, where particular rules are defined. These types of rules should also be specified in the Agreements to participate in a federated network of platforms and be implementable by a platform.
- Open - any new IT capability, designer or user group can be added as long as it conforms to

the architectural principles (of the Internet) and thus abstracts data transfer into a transfer of data streams to a specified set of IP addresses (or endpoints/URIs). This requirement of openness differs from the previous one, it sets rules for extensibility and flexibility of the solutions that have to be addressed by the federated concept of platforms Agreements. It identifies various stakeholder groups that specify interoperability solutions/standards for their community, e.g. IATA for air transport and ERA for rail transport.

- Heterogeneous - it is a socio-technical network involving several layers of technical components, humans, organisations, institutions, and so on. The challenge is to find a solution that is acceptable and can be implemented in this network.
- Evolving - the set of IT capabilities grows significantly during the evolution of the proposed federated network of platforms Solution, integrating new users and design communities. In the Internet, these IT capabilities can be listed as mail (smtp - simple mail transfer protocol), browsing (http - hypertext transfer protocol, widely applied in eCommerce applications) and file transfer (ftp - file transfer protocol). These IT capabilities have been extended over time by adding application specific ones like notifications (a primitive publish/subscribe mechanism) and sharing links to data (linked (open) data via so-called uri's - uniform resource identifiers). The solution should enable the integration of sensors (IoT - Internet of Things) and the Physical Internet with data sharing between autonomous operating assets, their users, and their owners (see trends). The properties and the principles in the core operating framework are not only part of the design, but also provide input to governance.

### *8.8 From layers and core operating framework to leading principles*

The leading principles will act as a guide for the development of the federated network of platforms in the Master Plan. These leading principles, rooted in ICT architectural approaches (TOGAF), are required to formulate the system boundaries, services, and functionality of the federated network of platforms.

Whereas normally leading principles in ICT architectures will be specified by individual organisations, the FEDeRATED leading principles have to be applicable for the shared facility, where this shared facility is implemented by many organisations. Thus, the FEDeRATED leading principles will have to address the interfaces between individual organisations, as if these principles are applicable to a virtual organisation. This adds complexity to the way of defining them in the Master Plan.

Leading principles have to be defined at various levels:

- Legal – what legal constraints should be considered or what regulations should be supported;
- Organisational – which organisations/roles are involved that function as end-users of the shared facility and how could the federated network of platforms add value to data sharing between those roles. A holistic approach needs to be taken for constructing supply and logistics chains in networks. This will require for instance to define 'business service' and 'business process choreography'. One of the most important principles at this layer might also be 'seamless interoperability' - being able to share data based on a common approach – and governance;
- Services and information – identification of the services provided by the shared facility, related to one of the aforementioned interoperability layers. The services, that support the

business process choreography between any two organisations, require data to be shared that is specified by a semantic model. This principle will have to define how these services and their semantics (information) will be specified;

- Functional – basic principles with respect to functionality are on components providing services with their information and interfaces. From a functional perspective, also the supporting layer functionality will have to be taken into account;
- Technical - choices on the technical layer have to be made, but also as regards to (temporary) data storage.

The development of the Leading principles within the concept of the Master Plan will develop the FEDeRATED reference architecture for a federated network of platforms: the FEDeRATED House.

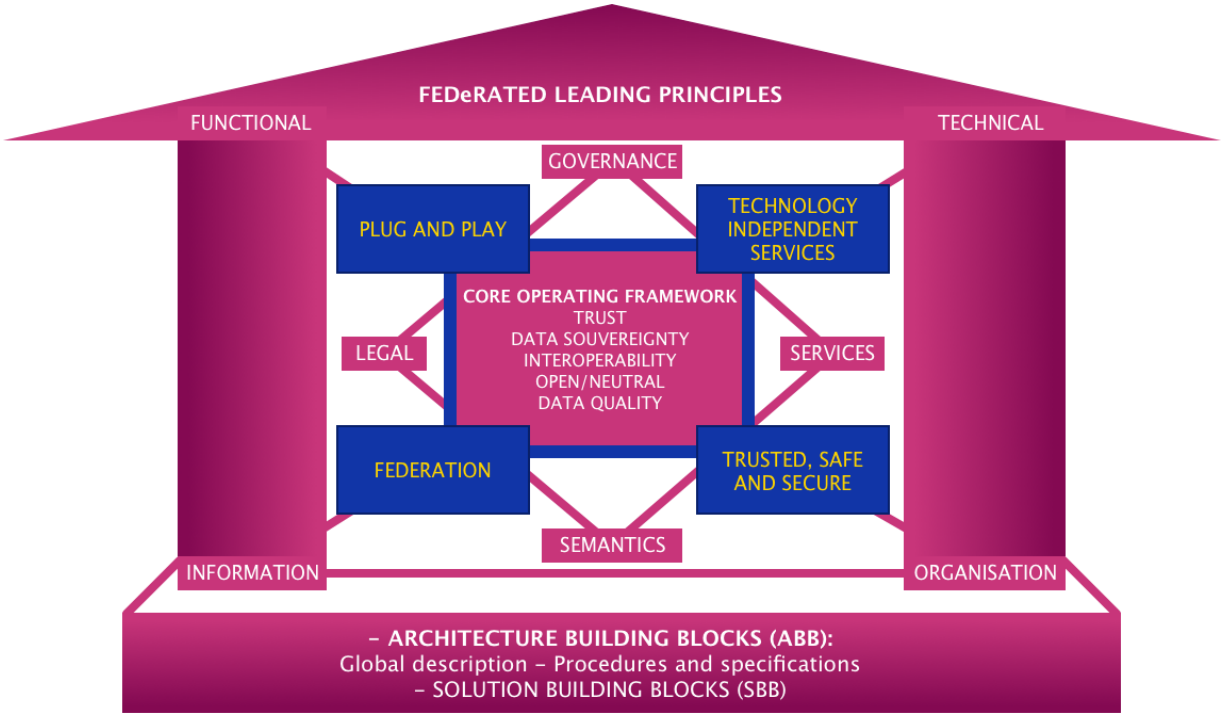



*Figure 9: The FEDeRATED House for developing a reference architecture*

On top of these leading principles, the Master Plan has to provide various implementation options, based on the typology presented at the start of this section. These implementation options will for instance visualize which organisations can provide particular services. For example. As the FEDeRATED Action is a Member State driven Action, this implies that the main focus will be on data sharing between business and government (B2G). Thus, any solution developed by FEDeRATED will interface with solutions in the private sector. However, since FEDeRATED also addresses level playing field, a public solution might also support particular B2B data sharing. The latter will enable digitalisation by SMEs, which increases data quality of authorities and large enterprises and reduces costs for manual data processing.

The B2B functionality in the public domain will be such that it increases data quality of authorities. Any type of B2B functionality otherwise required can be developed using the services provided by the public domain facility. These issues will have to be addressed in the Master Plan.

# 9 QUESTIONS AND ANSWERS

Q and A often allow the opportunity to be as clear as possible on what one is dealing with. Therefore, several questions have been put on the table.

## *9.1 A federated network of platforms, what does that mean exactly?*

This is an information infrastructure provision for sharing data in transport and logistics. It offers a set of agreements and technical applications, including the following components (necessary, probably not yet sufficient / exhaustive):

- Data models for various modalities, including data definitions;
- Value lists (such as country codes, item codes, rates, etc.);
- Standards for exchange, such as protocol standards and other technical exchange standards: REST, JSON, HTTPS, OAUTH2, API / URI standards, security, etc. Including interpretation of minimum required common components;
- Directory services with which data can be found (also depending on chosen URI standards);
- Joint implementations and domain-specific standards: iSHARE, OneRecord PMD, DLF, legacy messaging standards;
- Connection conditions and quality requirements / agreements regarding data and services;
- Governance of the system: who determines what and how it is implemented, entry and exit / granting and withdrawing of access, etc. This also includes a legal track;
- (Optional) agreements on data enrichment for one of the other "squares";
- Monitoring functions for monitoring the system - this is a real technical layer;
- Agreements about management, maintenance and expansion (and who will pay for it and implement it, or how you determine that);
- Rapid deployment of new IT services to support business processes.

## *9.2 How would a federated network of platforms function?*

There are a multitude of examples of how a federated network of platforms could function. To give four examples:

- This federated network of platforms could regulate that public authorities has access to certain streams of data;
- Port Community Systems could request data from other 'squares' (data corridors) on behalf of public authorities;
- Operators and stakeholders can combine and enrich data on behalf of each other, and subsequently exchange data with each other via the federated network of platforms;
- Various parties can offer a multimodal service package for parties that also operate multimodally (for example, almost all trucking companies).

A good example is how the energy market has regulated itself. If you switch from an energy supplier, the registration and deregistration process will take place "naturally". The new supplier cancels on your behalf and the "switching" of the electricity and gas is fully handled. This has regulated the energy market by agreeing on a number of messages and establishing a central link (EDSN) that

carries out these central processes.

### 9.3 Who should participate?

This depends on the ambition level. There are two angles. The public authorities' perspective and from the business site.

*Public authorities' perspective*[16]*:*

If the federated network of platforms were to be set up from a public authorities' perspective a very likely approach would be that a limited group should participate in the set-up, namely the parties that are seen by the Ministry responsible for data infrastructure in transport and logistics as "critical infrastructure for the transport sector".

The approach would be different is various countries. Any EU Member State that has already established a Maritime Single Window might be easily be tempted to develop this one single data entry point for maritime transport into a data hub to various other transport modes than maritime data only. In addition, to make optimal use of the available data a data sharing, instead of a data distribution mechanism, should be established.

Operationally, so once the system "runs", anyone can purchase data and services for their logistical role, within the governance and the connection conditions.

*From the business perspective:*

There are well identified touchpoints between business and authorities in the logistics and transport space concerning cross border transport, goods compliance, taxes & duties and safety & security. These touchpoints can act as the scope of participation of business in this network of platform. Each of these areas are deeply integrated in the internal data operations of business and the private sector networks they operate in and some of these data operations are more advanced than other others. Goods compliance for example still requires paper documents in many cases whereas transport documents are either digitized already or that development if in progress. From a pragmatic perspective, business involvement in a federated platform would be driven by existing capabilities as a starting point.

### 9.4 What does participation in a federated network of platforms imply for the systems of the participating organisations (financial, technical, legal) that participate?

The systems themselves will become somewhat simpler from a technical point of view, because they can connect to a (if we do well) universally decentralized data landscape. This gives them access to a great deal of well-defined and managed data. It can even happen that systems can be phased out

[16] See Annex 6 for public authorities responsibilities

because, for example, some joint functions only have to be implemented once (i.e. within the green area, which I see as a system) - depending on how far the parties dare to go.

It is therefore a major step in efficiency and in a "level playing field" for all parties. From a legal point of view, there will be a clearer division of roles and rights and obligations for affiliated parties with regard to the use of (each other's!) Data, something that is now mainly regulated in many bi / multilateral agreements (if it has already been arranged ...).

### *9.5 Is it the intention that participating organisations no longer have their own systems?*

No. On the contrary. The federated network of platforms concept ensures the continued validity of legacy systems and that data remains with the data originator, thereby requiring that data originators have their own systems (or that of a platform service).

### *9.6 How do already developed data sharing mechanisms fit into this story?*

Various data sharing mechanisms have been developed the last five years. Most of them cover part of the issues that need to be resolved. To mention a few: iSHARE, OneRecord, AEOLIX/SELIS, TAF-TSI. These initiatives exist and that they can act as a source of inspiration, experience and lessons learned but do not necessarily constitute integral part of the federated platform nor constrain its designs.

**iSHARE** is one of the Identity and Access Management frameworks. When OAuth (version 2 is now common) is chosen as the authentication standard, then in principle interoperability with other frameworks (Google, Facebook, Apple, Microsoft) is possible. It is very important to be able to establish the identity of a party in the system at all times. iSHARE offers a framework for this as well as a sharing data mechanism with unknown parties including a way to establish the identity of a party in the system at all times.

**OneRecord** is a standard for data sharing in the air cargo sector. It specifies data security and identity standards and management, a standard from a single common API and a data model for airfreight based on an ontology (semantics) which inherits they key elements from the air cargo XML standards which in turn are built on air cargo EDI standards known as Cargo IMP. The purpose of ONE Record is to migrate from EDI push technologies which are constraining and limiting digitalization of air transport to a pull-based data sharing approach that facilitates digital cargo and the emergence of digital twins in logistics for the purpose of automated and smart logistics and transport.

### *9.7 What are the short-term benefits for the organisations that start to participate in developing this infrastructure facility?*

Efficiency, shorter / no waiting times, access to more data, higher / guaranteed quality of data.

### *9.8 What does a federated system entail? And what are the advantages and disadvantages?*

Federated means that you do not have to do or know everything yourself, but that you let someone

else do or determine parts of a process and - very importantly - that you trust that.

The information architecture in many EU Member States is built on this principle, but also payment systems. For example, almost all government road services rely on identification by means of. National approved Authorisation and Identification system. As a result, these services do not all have to figure out for themselves how to identify and check a person's identity. This makes a huge difference in costs and efforts (and greatly reduces the number of errors).

### *9.9 What does the governance look like? How complex or simple does it look?*

That is precisely one of the components to work out. It can vary from a simple system of agreements and some "gentlemen's agreements" to a highly regulated whole. In general, the governance should cover:

- Defining Boundaries;
- Balancing the Benefits and Costs of Resource Usage Managing;
- Sanctioning resource to these users (i.e. by constitutional right holders);
- Devising and Modifying resource Usage;
- Conflict Resolution mechanism.

### *9.10 Can we develop our own solutions? Can we join in the discussion? How?*

Before starting your own data sharing project some lessons learnt form data exchange projects relating towards a hub-and spoke perspective are:

1. Explore for each party a recognisable and quickly achievable advantage in having the node;
2. Organise based on trust between the parties and start the growth core of the node;
3. Do not start with a design, but initiate a process;
4. Place the node in the hands of a party who does not benefit from the exchange.

The question about joining the discussion refers to three layers, local, national and for the EU.

1. On the EU level, also in connection to the global level, the DTLF is acting as a consultation platform, together with the CEF projects. In addition, various European Commission Services are actively engaged, like DG TAXUD and DG Connect and DG Digit.
2. To organise the work nationally, the best thing is if there is a defined client where a few coordinating and commissioning / decision-making tasks are arranged (program management, architecture, functional specifications) that can then be worked out together with the aforementioned parties.

# ANNEXES

Annex 1: Lessons Learnt

Annex 2: Legal Issues

Annex 3: DTA Exchange and Semantics

Annex 4: Data Exchange and Business Cases

Annex 5: The Various Roles of Public Authorities in Freight Transport and Logistics and the Use of Data

# ANNEX 1: LESSONS LEARNT

Many data exchanges projects between business and also administrations have been developed the last 10 years in transport and logistics. What is striking about most cases is that they developed other services and control structures than originally intended during the start-up phase. The nodes have grown to the positions they now have. It was clearly indicated in all cases how central the role of trust is in starting and growing the node. Trust between parties is something that can of course exist before the node arises. In a number of cases it is also clear that the node is in fact a translation of a number of mutual trust relationships that have existed for years between administrators and / or organisations.

## 1 The major lessons learnt

The major lessons learnt are

1. *Development of services.* As the node becomes more trusted, complex services can emerge. This means that the form of organisation and the services provided by the node are a result of the degree of trust that has been established. A service of the node that is seen as completely unfeasible at the start can be made later, after more trust in the node suddenly emerged, desirable and even requested by the affiliated parties.
2. *Equal or different.* Of course, trust is also something that can be lost, so that certain services can suddenly no longer count on support and financing. Trust evolves more easily between parties that have the same degree of influence on the node. Maintaining trust is a continuous point of attention. We also see a number of cases actively looking for variants where the parties can once again sit at the table as equal.
3. *Trusted third parties.* Trust is also a reason why affiliated parties would like the node itself to be managed by an independent intermediary. It appears to be important that the node does not fall under the direct control of a party that itself benefits from the exchange. Especially with Exchange-type cases - trust is difficult to maintain if the largest party, for example a government party that must be supplied to, is also the owner of the node. The affiliated market parties will then not use the node to also exchange information among themselves, while this could be possible and desirable.
4. *Hook up later.* Trust is something, once the node, which also radiates to new parties and attracts new parties, acquires it. We see in the cases that new parties who connect to an existing and trusted node ask much less difficult questions than the original parties who were at the cradle of the facility. Where the original parties wanted guarantees about influence and control, the new parties that connect later have long been pleased they can participate and have much less need to contribute to the management of the node itself. The trust and proven utility of a node greatly simplifies the complexity of the management required over time.

## 2 Resistance to change.

Most data exchange projects have very long timespans between development and adoption. In

general, it is the scale of these projects that is the cause of this, in particular when the stakeholders concern an entire territory or industry. Typically, the adoption is measured in decades which is why 1970's EDI is still the standard in data exchange today. The pressure of digital transformation today will require a different approach to adoption that is measured in years, not decades.

# 3 Development scenarios

The guidelines of the lessons learnt can be applied in two development scenarios. One based on cooperation between market parties and one scenario with the Government as initiator. This is then step by step a Warehouse function for different parties. The starting point is then an Exchange facility for equal parties.

The cooperation between the market players

- Ensure that there is a clear financial business case. Although there will be more reasons to start a node than financial issues, clear cost savings make decision-making on connection easier. For example, a financial business case can be sought in lower costs of communication facilities since they are now shared with other parties. But there are also often direct financial benefits in the primary process through information from to switch. It is important that the parties involved immediately have a feeling they deserve through the exchange.
- Start with an Exchange facility supported by a small group of parties of a similar nature. A coalition of the willing. Foundations and cooperatives are appropriate legal forms.
- Facilitate the parties as far as possible when connecting. Go very far in this. For example, by not imposing requirements on delivery formats but by translating everything from and to the node. This makes connecting easier.
- Communicate through Manifests and the joint PR that the parties are sitting here as equals now.
- Allow more types of parties to connect and adjust the Governance structure accordingly. See the Governance structure as temporary and the provision as the fixed element. Proven utility and saving for the Exchange also allow the management or legal form to change along the way.
- The more trust in the node develops, the more growth will be achieved through the centralized storage of frequently exchanged data. This makes the exchange more efficient. Now there are also consultation structures available to jointly determine meaning and value. Parties are used to the node and are therefore prepared to adjust their own processes to the central warehouse. For example, by 'specifying' your own information collections and using those from the node. The growth rate must also allow parties time to make adjustments to this process. Graduality is the motto here.
- Start enriching that central data into value-added services, but only at a pace that matches the demands of the affiliated parties. The joint questions of the affiliated parties remain the guiding principle at all times. Innovation is also started on the basis of these questions. This also makes a decrease clear and makes it easier to position new services immediately in response to questions from affiliated parties.

# 4 Cooperation with the Government as initiator

The same development can also be started by a government organisation that is willing to show owner behaviour, even though the facility will, in time, have shared ownership. The growth model could then be:

- Start with a government party that has direct financial benefits from the exchange of information from and to other parties. For example, because parties now have a legal obligation to register or retrieve certain information in a central register.
- Create a facility to facilitate that exchange by a party that is not the launching government is the customer itself. It is now essential that the government organisation does not arrange the exchange itself but seeks a trusted third party for this. Not so much because of their own demand for exchange, but because this exchange over time must become a junction with a much broader objective.
- Allow the affiliated parties to share other information with each other, not just the information that is required for the government party. Now it is important that the existing one connection, originally intended for delivery to the government organisation, will also be used for mutual exchange between the parties. The government organisation, at this stage often also the leading party for the node, must stimulate this use even if it is independent of the original objective and the legal obligation. It is important that the vision of the government organisation must go further than strictly its own task.
- Open the Governance structure to allow more types of parties and give the market more control options as the information exchanged becomes more and more of a market character. As the nature of the use of the node changes, the Governance structure must also change. Here too, the proven utility of the facility is the leading factor. Governance is a temporary choice depending on the mix between market and government that comes together at the junction.
- Finally, as a government, say goodbye of the steering role, but only after the continuity of information provision to the government is guaranteed. At a certain maturity level of the facility, the government can take a step back.

# ANNEX 2: LEGAL ISSUES

## 1 Introduction

Other than technical barriers, such as data interoperability, a number of potential legal barriers are widely cited as restricting the further use (adoption) of digital data and data sharing. These concern both perceived and actual ambiguities or uncertainties relating to the primary, and interrelated, barriers:

- Re-use of data;
- (third-party) liability (for both data providers and (new) stakeholders in the chain, i.e. platforms).

Intrinsic to these two are related (secondary) barriers concerning clarity and (re-) alignment on the following:

- Acceptance of electronic data (by authorities);
- Data ownership;
- Permissions and access rules;
- Fit for purpose (of data use);
- Contractual obligations (initiated from the original transaction);
- Confidentiality and competition (impacts of increased visibility);
- Data storage;
- Data reliance;
- Data quality;
- Security.

Whereas the anticipated eFTI Regulation will go some way to alleviate the potential barriers concerning acceptance of electronic data by public administrations, namely through cross-sector alignment, other aspects on re-use and liability remain of primary concern.

All of these barriers have bearing on the liberalisation, further harmonisation or creation of a common playing field with respect to data sharing.

However, many contractual arrangements already exist in both the A2B and B2B spheres. On a one-to-one basis, under current arrangements, the disruption faced by the different stakeholders in respect of these barriers can be considered limited. The data originator, user, purpose of use, liability, etc. are well-defined and specific. These contractual arrangements may vary; some are based on “industry standards” or models; others are established for a specific (one time) purpose and others are to enable an “intermediary” service; however, they are all valid for the intended purpose.

Under the federated network of platforms concept there is a need for a common understanding and application. For example, the federated network of platforms concept relies on the re-use of data throughout the chain and not just between two contractually bound stakeholders.

The success of the federated network of platforms is reliant not just on technical solutions but on **securing trust**, on the basis of a sound **legal and regulatory framework** that establishes clear grounds and rules towards **re-use of data** and **potential subsequent liability**.

# 2 Securing Trust

FEDeRATED aims to "deliver the foundations for a trustworthy and interoperable business and administrative data sharing infrastructure for freight transport and logistics". Trust is key. Trust is required both in and within the federated network of platforms. There has to be trust between stakeholders to be able to use the data and trust between the platforms to be able to handle the data.

For data sharing in transport and logistics, trust for users means that the data users have sufficient belief and confidence in the quality, usability and availability of the data that they and (only) their counterparts in the chain need to conduct their tasks and responsibilities. In effect, this means that all stakeholders require assurance that:

- The data is of appropriate quality for the intended purposes;
- The data is only made available and used for the intended purpose, and only by and for those that require it (thereby protecting any commercial sensitivities);
- The data is available when needed;
- The data can be made available, processed, distributed and received in a format that meets both administration and commercial requirements and processes;
- The "system" is secure and not open to unwanted or malicious misuse.

Many of the efforts in FEDeRATED are centred around realising the technical infrastructure for ensuring interoperability. The technical means should cause minimum disruption to existing processes and systems. The FEDeRATED Master Plan will develop the ways and means for delivering a federated network of platforms. These ways and means will be validated through the Living Labs. The Living Labs will demonstrate trust within the "system" and for selected (participating) users by showing that it "does what it says on the tin".

However, these Living Labs are for particular business cases, with pre-selected, like-minded stakeholders sharing a common goal. For a federated network of platforms to be accepted and adopted across the board it is necessary to show and convince the wider audience that they can also be assured of similar reliability, capability and integrity for their purposes.

These purposes are varied and range from formal reporting requirements through to optimising business processes and opening up new markets. Some are governed by strict legislative measures, others are market-oriented and not subject to direct legislation.

The same data is often of interest to both administrations and business. There needs to be a robust governance structure that instils a high level of confidence in the solution(s) to all of the stakeholders. Central to the governance structure is ensuring a transparent and substantial set of "rules of the game". These "rules" can be either explicit or implicit.

One of the drivers for change is an overriding ambition towards reduction in the administrative burden. This is to be achieved in part through technological advances however also through ongoing moves towards deregulation. A condition to change is that it should be as non-disruptive as possible towards existing processes, procedures and systems.

Therefore, for the good functioning of a federated network of platforms it is essential that a robust **legal and regulatory framework** is set up that ensures minimum disruption to existing organisations, systems and regulation but supports maximum trust. It is necessary to remove uncertainties.

# 3 Legislative and Regulatory Frameworks

## *3.1 Legal Regime*

Data and Data exchange can be subject to international, EU, national, regional and/or local legal and regulatory rules and requirements. These rules and regulations pertain to both administrations and business and have the potential to impact both A2B and B2B data exchange.

As such the international community have set out internationally binding standards, regulatory frameworks, Agreements and Conventions, exchange and application of best practices etc. through e.g. UN Specialised Agencies (ICAO, IMO, etc.), other UN bodies (such as UNCTAD, UNECE (incorporating UN/CEFACT), etc.) and other independent intergovernmental organisations (such as WCO, WTO, etc.).

Many of these measures involve provisions for data exchange at some level or another. Sometimes they pertain to minimum requirements, but sometimes also maximum (e.g. in the case of FAL).

Where EU member States have ratified or signed up to these measures, the EU has in the majority of cases incorporated these into their own Directives and Regulations.

EU Regulations and Directives may provide for further requirements, beyond the internationally agreed minima and maxima, where this does not conflict with international arrangements. The EU Regulations and Directives effectively become national law once transposed and implemented by the individual MS. National law may also then be subject to yet more elaboration depending again on what is agreed on international and EU levels. Finally, requirements for data can be set at the local level (e.g. port) depending on particularities however normally according nationally agreed means.

In addition to existing legislative and regulatory measures there are numerous ongoing (drafting) initiatives, especially at international and EU level, concerning digitalisation which can also have a potential impact on and by the federated network of platforms approach.

## *3.2 Legislative and Regulatory Frameworks*

Legal aspects are wide-reaching and require consideration of both legislative and regulatory frameworks. Whether considering the applicability (and compatibility) of existing sectorial legislative

frameworks[17] or determining the potential cross-sector impact of regulatory frameworks within, on and by the federated network of platforms approach.

Examples of cross-sector regulatory frameworks having a wider potential impact on digitalisation include:

- General Data Protection Regulation (2016/679/EU(GDPR));
- Network and Information Security Directive (Directive (EU) 2016/1148);
- Directive on the re-use of public sector information.

A distinction should be made between legislative and regulatory frameworks as well as on the types of legislative and non-legislative measures and instruments available.

The following provides a short overview of these frameworks in the EU context.

Whereas EU Regulations generally lead to a harmonised implementation across all MS, EU Directives can lead to fundamental differences between the MS, especially when IT is involved. This is phenomenon is further compounded when considering apparent inconsistencies or diverse approaches between different transport modes and sectors, e.g. one mode may be subject to an EU Regulation (e.g. electronic reporting - Inland Waterways) and another to an EU Directive (e.g. Single Windows - maritime) for essentially the same (or very similar) purpose. This can then lead to further IT incompatibility or divergent end-results.

### 3.2.1 Legislative Frameworks

The legislative framework comprises the laws on what is to be achieved and consequences for not doing so. It is put in place by governments.

Within the EU, the legislative framework is set out through EU Treaties and EU Directives. EU Directives are goal-oriented and open (to some extent) to interpretation when individual MS devise their own laws on how to reach these goals. This can lead to inconsistencies when implemented, as was recently the case with the implementation of Single Windows in response to the (maritime) Reporting Formalities Directive. Therefore, especially when technology is involved, it is not uncommon that the EC will draft accompanying Regulations.

According art. 249 of the TFEU: “A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.”

### 3.2.2 Regulatory Frameworks

The regulatory framework sets out the standards and rules on how the goals of the laws are to be achieved, monitored, adhered to or enforced. It is put in place in the first instance by the same

[17] A listing of existing EU sectorial legislative provisions is provided in the appendix.

governments in order to help implement the laws (these are then enforceable).

Within the EU, the legislative framework is set out through EU (Delegated) Regulations. They are generally prescriptive and not open to interpretation. They apply automatically and uniformly to all EU countries as soon as they enter into force and do not need to be transposed into national law.

According art. 249 of the TFEU: A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.

### 3.2.3 Supplementary Measures

The above can be supplemented by further non-legislative measures covered by self-regulation and concerted actions through, for example, codes of conduct, standards, procedures, model contracts, agreements etc. as deemed necessary or useful by the (private) sector.

Within the EU, supplementary measures can be provided in the form of Guidelines, Recommendations and Opinions.

According art. 249 of the TFEU: Recommendations and opinions shall have no binding force.

### 3.2.4 DTLF approach

Under its first mandate the DTLF recognised that further legislative measures were required in support of the federated network of platforms.

It is recommended to further investigate the development of a Regulation/Directive (legal code) that is supported by the technical code of the federative platform, and the application of this technical code in the implementation of other relevant policies in the area of supply and logistics."

This was followed by the recognition for the need to pursue and develop supporting "soft measures" as well as implementation guidelines/recommendations for the technical code.

The measures foreseen by the DTLF vary in rigidity. Regulations and Directives serve different purposes and, although mandatory in nature, offer varying degrees of freedom in eventual implementation. Guidelines and Recommendations, as their names suggest, are non-mandatory as a standalone document; however, for the purposes of trust they are essential.

Integral to all of these are the use of e.g. standards, codes of conduct, service agreements, etc.

It can be concluded that the DTLF supports a mix of measures that are fit for purpose and support the correct balance of restrictive (mandatory) and non-restrictive (non-mandatory) instruments.

# 4 Transport and Logistics Sector

International trade is a series of commercial transactions between trading partners whereby both the types of goods and their values are tracked for the purposes of customs procedures. The physical

realisation of trade is performed in the transport chain organised by a series of logistical activities.

Within the transport and logistics sectors legal and regulatory frameworks have been developed to ensure certain data are available to authorities and administrations and/or business for conducting their roles and responsibilities in both ensuring the safe, secure and efficient movement of transport means, goods and persons as well as facilitating trade requirements such as Customs (incl. taxation) in general. These frameworks go beyond just EU Regulations or (transposed) Directives. Underlying the legislative measures are sets of agreements and codes entered into by public and/or private entities, either contractually or in good faith.

However, each sector has developed legislative and regulatory frameworks (including standards) that are fit for their own purpose. They have made allowance for existing procedures, processes and infrastructure within their sector (and to a lesser extent other related sectors). They may be subject to different constraints and opportunities due to the nature of their activities, e.g. through geography (access to means) or timing. It can be expected therefore that aspects of data sharing, for example re-use of the same data for different purposes, may be subject to constraints under existing measures.

FEDeRATED concerns B2A, A2B, B2B and A2A data sharing. Both business and government foresee benefits in change towards enhanced data sharing capabilities, both for their own processes and for the sector at large. This change is facilitated through a transition towards a federated network of platforms approach. However, the drivers for change as well as the roles and responsibilities within the sector vary. The expectations may vary and ultimately the consequences of change for each stakeholder will vary.

The need for technological change is self-evident and organisational change is unavoidable however what about legal change? Can a federated network of platforms function within the current legislative framework?

Therefore, when considering the legal aspects, it is also necessary to determine the impacts of existing measures on underlying principles such as re-use of data, system availability, data storage, etc.

# 5 FEDeRATED Framework

Within the context of the FEDeRATED Master Plan, the Action should:

- Identify the (perceived) roles, responsibilities, processes and obligations as identified through the FEDeRATED Vision and business cases;
- Examine the Leading Principles;
- Account for the existing legal and regulatory framework.

Based on this, the work on legal aspects within the FEDeRATED Action should further:

- Assess the Vision, Core Operating Framework and Leading Principles of FEDeRATED to identify the scope (area) of laws and regulations that are relevant and pertinent to FEDeRATED solution(s);

- Identify all existing (and planned) legislative and regulatory instruments having the potential to impact on, or be impacted by, the FEDeRATED solutions(s);
- Identify potential conflicts and/or shortcomings in these existing (and planned) legislative and regulatory frameworks(s);
- Evaluate the extent to which current legislative and regulatory frameworks(s) aid or restrict the implementation of the federated network of platforms;
- Develop a FEDeRATED legal framework.

FEDeRATED should endeavour to express the legislative and regulatory framework on the basis of least burden and most appropriate for each aspect of the federated network of platforms. It should at the least:

*Develop a Common Liability Framework:* Create an agreed-upon framework for apportioning liability related to data sharing among financial institutions, data aggregators and financial technology companies that can be shared and replicated in contracts between the different parties.

*Facilitate Market-wide Adoption:* Ensure that standard data-sharing approaches can extend to all entities.

*Provide recommendations for Regulators:* Clarify existing regulations that impact data sharing and determine where there is potential to remove regulatory overlap and form shared cross-sector viewpoints.

# 6 Core Legal Aspects

Private stakeholders are legally and/or contractually obliged to provide data to other stakeholders, whether in fulfilment of a legal obligation towards an authority (e.g. notification) or contractual obligation to another stakeholder in the chain (e.g. shipper to carrier). These obligations are often formed on a one-to-one (bilateral) basis whereby one party is responsible for ensuring delivery of the information (data or document) to another for a specific purpose. The data must not only meet timeliness and accuracy criteria but also be handled (or processed) in a manner conducive with overriding legislation on e.g. privacy, commercial sensitivity, storage, security, etc.

The federated network of platforms concept relies on a number of pre-requisites concerning availability of and access to data. It also promotes the ethos of the re-use of data and therein introduces factors such as data ownership, data sovereignty, data reliance and integrity (for all purposes) and confidentiality. Thereby additional issues arise concerning the ability (or not) to transfer responsibility and/or liability to third parties in the case of specific or explicit requirements concerning data provision in existing legal formalities and contracts.

According the authority-based legislative measures for A2B reporting and business-related data provision for B2B reporting stakeholders are responsible for (and therefore liable in case of fault) on a “named” basis. It is certainly not the case that the same stakeholder is always responsible for delivering the same data.

In the DTLF SG2 report on “Enabling organizations to reap the benefits of data sharing in logistics and supply chains”, which supports the use of the federated network of platforms approach”, the

word platform is used as a synonym for “node”. A node is defined as “IT system providing (a subset of) the federative infrastructure services to their end-users and implementing the protocol for those services.” It is also stated that a node can be further specialised into a Registry, (Distributed) Storage Node, or Infrastructure Service Node. The (existing1) platforms are in general subject to governmental, (port) community, commercial or private governance structures.

In developing the FEDeRATED Vision, a number of core concerns or questions arose regarding the legal sensitivities (and (potential) constraints) foreseen due to the underlying principles (or pre-requisites) of a federated network of platforms and the (proposed) Core Operating Framework.

The following legal sensitivities form the crux of the issues to addressed when considering potential (legal) boundaries towards the federated network of platforms:

- Changing responsibilities towards data provision, access and (re-) use (including reliance, authenticity and integrity);
- Liability, both in terms of protecting existing (transaction-oriented) rules and required (platform-focused) regulations;
- Extent and need for regulation concerning the design and operation criteria of such a decentralised trust-generating mechanism.

The two fundamental legal matters to be addressed relate to:

- Re-use of data
- (third-party) liability (for both data providers and (new) stakeholders in the chain, i.e. platforms)

Integral to these premises are the additional matters related to:

- Acceptance of electronic data (by authorities)
- Data ownership
- Data reliance
- Data quality
- Confidentiality and competition (impacts of increased visibility)
- Contractual obligations (initiated from the original transaction)
- Permissions and access rules
- Security
- (Fit for) Purpose of data (use)
- Data storage

Following is a short outline on the primary concerns.

### *6.1 Re-use of data*

FEDeRATED considers B2A, B2B and A2A data exchange and sharing. Opportunities and constraints for re-use of data within these areas vary.

Re-use of data for B2A data sharing is generally supported through existing legislative acts whereby

administrations are encouraged or obliged, through implication, to re-use data (A2A) already submitted (by business) in response to e.g. reporting formalities under single reporting or "reporting once" provisions.

Re-use of data for B2B data sharing is in the main not covered by legislative acts. Where re-use is allowed then this is normally covered under explicit (commercial) contractual arrangements. However, as a general rule, commercial entities are not forthcoming in openly sharing (certain) data, this being often due to maintaining their competitive advantage. Other reasons are linked to uncertainty in "ownership" and related liability aspects.

### 6.2 (Third-party) liability (for both data providers and (new) stakeholders in the chain, i.e. platforms)

The national and European legislative frameworks that apply to contracts in the data eco-system face multiple challenges. Firstly, they are based on concepts – ownership, intellectual property, personal data, consent, liability – which do not necessarily apply clearly or unambiguously to a complex business model where data is automatically collected, combined, enriched, updated, modified, exchanged, (re-)used and deleted.

Secondly, existing laws may not sufficiently take into account the different positions of market players, notably the situation of SMEs, entrants and start-ups, as well as inequalities in bargaining power, etc. More specifically, while the legislation as such is objective, it can have repercussions that are unfair to some market players, or that simply result in a market situation that is suboptimal from a societal perspective.

In this way, the legislative frameworks may hamper the smooth performance of the data value chain contract, e.g. through legislative gaps or inadequate provision, or simply fail to achieve results that are optimal for society as a whole.

Issues of (limitation of) liability within the transport and logistics sectors have been dealt with extensively for many years. International Conventions and Rules have been established setting out the (limitation of) liability placed on carriers, shippers, terminal operators etc. Questions of liability relate to eventual loss, damage or delay of goods. These same Conventions and Rules also set out the obligations regarding for example the provision of timely and accurate data (documentation) on the goods so that e.g. the carrier can reasonably perform their obligations to e.g. authorities in respect of reporting requirements.

Due to the emergence of different "contracts" for different transport modes and places in the supply chain efforts have been made to introduce all-encompassing door-to-door rules (e.g. the (yet to be ratified) Rotterdam Rules where a sea leg is involved) which also provide specific reference to the use of, and obligations concerning, "electronic transport records".

There are examples where certain stakeholders don't want to share data due to liability issues. For instance, if a stevedore or carrier have knowledge of the actual product that is handled, they could be liable for its value. These restrictions are formulated and agreed upon by all stakeholders, e.g. Rotterdam Rules, The Hague-Visby Rules, CMR convention, etc.

Liability needs to be considered on a number of different levels, namely:

- Liability on data originator (“owner”) for accuracy, availability, timeliness, setting of access rights etc.
- Additional liability on data processor (platform) for correct handling, application of authorisation and access rights etc.
- (Additional) liability on data processor (platform) in case of (necessary) modifications
- Liability on data receiver (data user) concerning data confidentiality and commercial sensitivity

Other contract forms also incorporate differing (limitation) of liability clauses. These contracts generally relate to the physical transport or (facilitation) of the management of the movement of goods. These may also be bound and/or impacted by overriding and underlying legislation, regulations, codes of conduct, stewardship and service agreements etc.

Examples of contracts related to physical transport include:

- Charter parties
- Bills of Lading
- Multimodal Bill of Lading FBL
- (Air and Sea) Waybills
- CMR
- CIM consignment notes
- letters of credit (L/C)

Examples of other arrangements, terms and certificates related to movement of goods include:

- Freight Forwarders' Standard Terms and Conditions
- Packing List
- Delivery Note
- Irrevocable Letter of Credit L/C
- Cargo Insurance Certificate
- Certificate of Origin
- Phytosanitary Certificate

The liability perspective differs depending on the role in the supply chain, not only for ensuring the physical movement of the goods but also concerning the provision and availability of data. Following some examples of liability perspectives:

*Consignor (Shipper):* Limited to obligations to e.g. describe the goods honestly and accurately.
*Consignee:* A straight bill of lading by land or sea, or air waybill are not documents of title to the goods they represent. They do no more than require delivery of the goods to the named consignee and (subject to the shipper's ability to redirect the goods) to no other. This differs from an "order" or "bearer" bill of lading which are possessory title documents and negotiable,
(Shipping) Agent:
*Liability of the transport terminal operator:* The United Nations Convention on the Liability of operators of transport terminals in International Trade states in art.3 that: “The operator is

responsible for the goods from the time he has taken them in charge until the time he has handed them over to or has placed them at the disposal of the person entitled to take delivery of them". The operator is liable for "loss resulting from loss of or damage to the goods, as well as from delay in handing over the goods (art.5)." This liability is not only related to the actions of the operator but is extended towards any "servants or agents or other persons of whose services the operator makes use for the performance of the transport-related services".
*Liability of the "platform" provider:* Data processing as a service - similarities can be drawn from provisions in e.g. the GDPR. In this case the data controller and data processer enter into an agreement (contract) whereby the obligations are set out. In the case of liability, the data controller will normally be held liable in the first instance, with recourse then being made towards the data processer (for breach of contract) in the case that the data processer has neglected an obligation. This represents a specific form of contract whereby liability is limited.

However, within transport and logistics there are many other forms of contract that exist having differing responsibilities and obligations, each having some recourse to data, data sharing and liability.

### 6.3 Additional

*Acceptance of electronic data (by authorities)*: It is anticipated that the eFTI Regulation will go some way to alleviate the potential barriers concerning acceptance of electronic data by public administrations, namely through cross-sector alignment. However, aspects on re-use and liability remain of primary concern and require alignment.

*Data ownership*: Recognising a lack of legal definition concerning "data ownership" the DG Connect "Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability" (Deloitte, 2017) developed the following working definition:

*'data ownership' is "understood as an alienable legal construct permitting one or more persons (the 'owners') to control access to or use of a single piece or set of data elements to the exclusion of others."*

It was found that at present there is a lack of common understanding between the different MS on the concepts of data ownership and data access/use rights. It was noted that "the concept of 'ownership' often relates to a very diverse set of claims, which may or may not combine aspects of intellectual property rights, data protection, trade secrets, contractual restrictions and other legal claims". Where ownership of data is considered, this normally falls under intangible assets (e.g. IPR). The majority of MS have no specific provisions in relation to the ownership of data.

However, provisions such as contractual "rights of access" and "rights of use" are generally recognised.

It may therefore be more appropriate to consider the rights and obligations of the "data originator" rather than the "data owner".

However, consideration also has to be made on the distinction between data originator and responsible party for provision of data. In A2B reporting this is clearly stated, but not always the

same party, and in B2B this can be subject to separate arrangements depending on e.g. INCOTERMS used or other measures.

# 7 Non-exclusive listing of Legal Measures

Following is a listing of EU Directives and Regulations that have a (potential) impact on, or may be impacted by, the federated network of platforms approach. The impact may be direct (in scope) or indirect (i.e. relevant but out of scope). They have been sorted according the following:

- Transport specific;
- Customs specific;
- Cross-sector non-specific.

## *7.1 Transport Specific*

### 7.1.1 Rail

*Interoperability of telematic applications for freight of the rail system in the EU*

Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (Recast)

Commission Regulation (EU) No 1305/2014 of 11 December 2014 on the technical specification for interoperability relating to the telematics applications for freight subsystem of the rail system in the European Union and repealing the Regulation (EC) No 62/2006

### 7.1.2 Air

*Commercial air transport operations*

Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council

*Harmonisation of civil aviation requirements and procedures*

Council Regulation (EEC) No 3922/91 of 16 December 1991 on the harmonization of technical requirements and administrative procedures in the field of civil aviation

Regulation (EC) No 1592/2002 of the European Parliament and of the Council of 15 July 2002 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency

Regulation (EC) No 1899/2006 of the European Parliament and of the Council of 12 December 2006

amending Council Regulation (EEC) No 3922/91 on the harmonisation of technical requirements and administrative procedures in the field of civil aviation

Commission Regulation (EC) No 8/2008 of 11 December 2007 amending Council Regulation (EEC) No 3922/91 as regards common technical requirements and administrative procedures applicable to commercial transportation by aeroplane

Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC

Commission Regulation (EC) No 859/2008 of 20 August 2008 amending Council Regulation (EEC) No 3922/91 as regards common technical requirements and administrative procedures applicable to commercial transportation by aeroplane

*Montreal Convention on air carrier liability*

2001/539/EC: Council Decision of 5 April 2001 on the conclusion by the European Community of the Convention for the Unification of Certain Rules for International Carriage by Air

Convention for the Unification of Certain Rules for International Carriage by Air (the Montreal Convention)

*Safety regulation of aerodromes*

Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council Text with EEA relevance

*Liability insurance of air carriers*

Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators

*Computerised air ticket reservation systems*

Regulation (EC) No 80/2009 of the European Parliament and of the Council of 14 January 2009 on a Code of Conduct for computerised reservation systems and repealing Council Regulation (EEC) No 2299/89

*Statistics in respect of the carriage of passengers, freight and mail by air*

Regulation (EC) No 437/2003 of the European Parliament and of the Council of 27 February 2003 on statistical returns in respect of the carriage of passengers, freight and mail by air

Commission Regulation (EC) No 1358/2003 of 31 July 2003 implementing Regulation (EC) No 437/2003 of the European Parliament and of the Council on statistical returns in respect of the

carriage of passengers, freight and mail by air and amending Annexes I and II thereto

*Air traffic management: Organisation and use of airspace in the Single European Sky*

Regulation (EC) No 551/2004 of the European Parliament and of the Council of 10 March 2004 on the organisation and use of the airspace in the single European sky (the airspace Regulation)

Regulation (EC) No 1070/2009 of the European Parliament and of the Council of 21 October 2009 amending Regulations (EC) No 549/2004, (EC) No 550/2004, (EC) No 551/2004 and (EC) No 552/2004 in order to improve the performance and sustainability of the European aviation system

*Air traffic flow management*

Commission Regulation (EU) No 255/2010 of 25 March 2010 laying down common rules on air traffic flow management

*Interoperability of the European air traffic management network*

Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation)

*Occurrences in civil aviation — reporting, analysis and follow-up*

Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007

*Obligation of air carriers to communicate passenger data*

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data

### 7.1.3 Maritime

Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC

Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC

### 7.1.4 Inland Waterway

Directive 2005/44/EC on harmonised river information services (RIS) on the EU's inland waterways

Commission Regulation (EC) No 414/2007 of 13 March 2007 concerning the technical guidelines for the planning, implementation and operational use of River Information Services (OJL L 105, 23/04/2007)

Commission Regulation (EU) No 164/2010 of 25 January 2010 on the technical specifications for Electronic Reporting in inland navigation (OJ L057, 06/03/2010)

### 7.1.5 Road

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

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

Commission Delegated Regulation (EU) 2017/1926 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

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

Regulation (EU) 2015/758 of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC

## 7.2 Customs Specific

### 7.2.1 A paperless environment for customs and trade

Decision No 70/2008/EC of the European Parliament and of the Council of 15 January 2008 on a paperless environment for customs and trade

Commission Implementing Decision (EU) 2016/578 of 11 April 2016 establishing the work programme relating to the development and deployment of the electronic systems provided for in the Union Customs Code

Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (recast)

Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee — A simple and paperless environment for customs and trade (COM(2003) 452 final, 24.7.2003)

Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code

### 7.2.2 CIS system

Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs or agricultural matters

Regulation (EC) No 766/2008 of the European Parliament and of the Council of 9 July 2008 amending Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters

### 7.2.3 International convention on the simplification and harmonisation of customs procedures

WCO International Convention on the simplification and harmonisation of customs procedures (Revised Kyoto Convention)

Decision 2003/231/EC on the EU's accession to the Protocol of Amendment to the International Convention on the simplification and harmonisation of customs procedures

### 7.2.4 Elimination of controls at frontiers in road and inland waterway transport

Regulation (EC) No 1100/2008 of the European Parliament and of the Council of 22 October 2008 on the elimination of controls performed at the frontiers of Member States in the field of road and inland waterway transport

## *7.3 Cross-sector non-specific*

### 7.3.1 Information Society

*EU Digital Strategy*

Directive (EU) 2019/1024 on open data and the reuse of public-sector information

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS EU eGovernment Action Plan 2016-2020 Accelerating the digital transformation of government COM/2016/0179 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a thriving data-driven economy (COM(2014) 442 final of 2.7.2014)

*Electronic Commerce*

Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services

### 7.3.2 Data Protection

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)

### 7.3.3 Internal Market

*Single Market for Services*

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

### 7.3.4 Enterprise

Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L 149/22 ("Unfair Commercial Practices Directive")

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services

Council Directive 93/13/EEC on unfair terms in consumer contracts

Regulation (EU) 2018/1724 establishing a single digital gateway to provide access to information, to

procedures and to assistance and problem-solving services

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling unfair trading practices in the business-to-business food supply chain (COM(2014) 472 final of 15.7.2014)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council

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) ----- and associated Commission Regulations

### 7.3.5 Competition

Regulation No 19/65/EEC on application of EU treaties to certain types of agreements and concerted practices between companies

Regulation (EU) No 330/2010 — application of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices

Commission Regulation (EU) No 1218/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of specialisation agreements.

Commission Regulation (EU) No 316/2014 of 21 March 2014 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of technology transfer agreements.

Regulation (EC) No 169/2009 — competition rules with regard to transport by rail, road and inland waterway

Council Regulation (EEC) No 4055/86 of 22 December 1986 applying the principle of freedom to provide services to maritime transport between Member States and between Member States and third countries

Council Regulation (EC) No 487/2009 of 25 May 2009 on the application of Article 81(3) of the Treaty to certain categories of agreements and concerted practices in the air transport sector

# ANNEX 3: DATA EXCHANGE AND SEMANTICS

The expected growth in freight transport urges for harmonized data interoperability and technical applications to connect data between various IT systems. In order to be able to cope with these challenges, an improvement of the information infrastructure is necessary: good and rapid exchange of information between all parties in the chain is an essential condition for an EU internationally competitive logistics system. In the logistics sector, the government is an important partner in that chain: when transporting goods across borders, there is a lot of digital exchange of information traffic that accompanies the physical flows.

Electronic exchange of information between parties means here:

"The automatic exchange of structured data between computer systems of different parties, whereby the standardization and structuring of syntax and semantics of the message and of the associated reference data makes it possible for the computers to process and possibly interpret the meaning of the messages.

A good and fast exchange of information between all parties in a chain is an essential condition for being able to compete internationally. In the logistic chain, the government is an important partner.

## 1 Exchange model

A number of levels regarding information exchange can be distinguished:

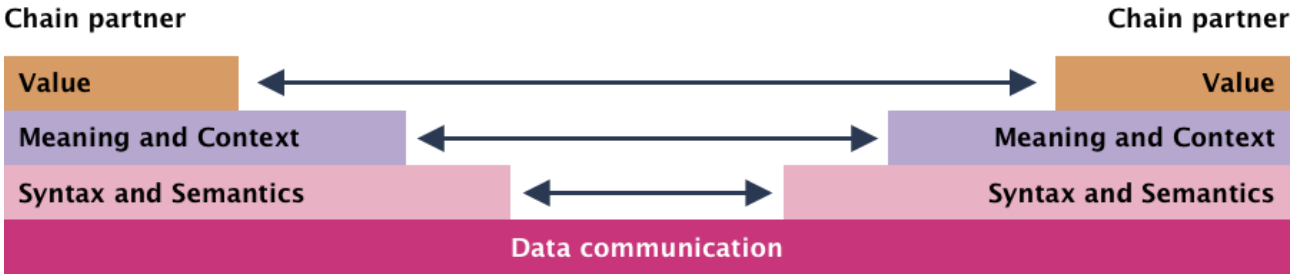



*Figure 10: Information exchange levels*

## 2 Data communication

The basic condition for electronic communication is that the parties are connected to each other via data communication networks, and senders can send digital messages error-free to the correct recipient(s) via an agreed communication protocol. For example, a node can ensure:

- Data goes to multiple recipients.
- There is an unambiguous address of senders and receivers, whereby the identification (who is who) and authentication / authorization (can the recipient receive this message?) from all parties is assured.
- The traceability of data flows is guaranteed, for example for audits and billing.
- The systems are disconnected by means of data queuing technologies (e.g. "Store and forward" function): temporary failure of a system at the data client (for example for

maintenance purposes) has no effect and reduces the costs of availability.

# 3 Syntax and semantics, reference data

Standardization of the structure of a message ensures that the parties can translate data communication consisting of a series of bits (message in binary data form) into information (and vice versa).

This standardisation relates to:

- Syntax: how can the series of bits be chopped in pieces that each have a meaning, what is that meaning, what are the variants of structure that are allowed, and how do you recognize which structure applies.
- Semantics: how should an individual piece of data be interpreted? For example: if the data represents a length, which length measure applies? Kilometres or millimetres? Is a “name" a first name, last name, company name or designation of an item?
- Ontology: how is the meaning of data related to other data? The world of logistics, transport and government have a language with a clear grammar and context. Ontologies provide this context. In the previous example, “name” has many meanings but in the context of a person or a company or a vessel, that meaning becomes clear.
- Reference data: In practice, often uses codes that refer to an agreed meaning. A home-garden-and-kitchen example is a zip code table that links codes to groups of homes and other buildings for mail delivery. Sender and receiver must use the same reference data to be able to interpret the codes correctly.

There are already many (partly overlapping) syntaxes and semantics that have grown from the time that administrative automation was started as an island in a paper sea. Every sector or company had its own variant. Harmonizing all these variants is a long-term and costly affair. After all, every adjustment requires new IT investments.

Practice shows that differences in syntax and semantics form much larger barriers than is often assumed. For example, a node can ensure that messages with different syntax and semantics are automatically translated to each other, so that users do not have to make costly adjustments. Making the correct version (s) and updates of reference data available is another function.

Meaning (contextual) → Ontology

The significance of receiving or not receiving data at a given moment, in a certain situation is driven by the context of sender and receiver. Even the lack of data can have great significance in a certain context.

That context is specific for a combination of sender and receiver: many context combinations can exist simultaneously, while it concerns the same data.

For example, a node can combine data from different message streams and stored message data using business rules. This allows automatic filtering the extent to which something can have meaning. Another example is the assessment and enrichment of raw data (removing false and

erroneous data) so that the output is clean and good.

# 4 The value of the meaning

The value of the meaning is also very situational and specific to the receiver or the sender. The value can be very unequal: the transmitter can attach very little value to it, but the receiver can place very much, or vice versa.

There are two dominant dimensions: services and parties.

1. Services:

a) the extent to which the node only facilitates data exchange, Exchange, or
b) the extent to which the node itself defines, adds, collects and distributes data, Warehouse.

2. Parties:

a) the extent to which the affiliated parties are Equal in role and their degree of influence at the node, or
b) the extent to which the affiliated parties are Different in their role, and each party clearly has its own role and rights.

The Service dimension is about the nature of the service provided at the node. With this type of node, the process for the participant proceeds as follows:

- Log in at the node, and bring one interface in the air
- Node checks and mediates between affiliated parties
- Share (= send via the node) data with one (or more) other affiliated party / parties.

# ANNEX 4: DATA EXCHANGE AND BUSINESS CASES

In this Annex various business cases for transport modes relating data sharing are provided:

1. Air cargo
2. General warehousing and Terminal Operator
3. Rail Intermodality
4. Freight forwarding Groupage
5. Contract Logistics
6. General truckload/full carload (FTL/FCL)
7. Short sea / Ocean cargo
8. Inland waterways

## 1 Air cargo

Within the EU, air cargo refers to international air transport and even among European member States, much of the air cargo is transported by Road Feeder Services with trucks that transport goods with an Air Waybill as part of the air transport.

Air cargo has a standardized transport chain that is: Consignor or Shipper, Export Forwarder, Export Ground Handler, Export Customs, Airline, Import Customs, Import Ground Handler, Import Forwarder and Consignee. In many cases air transport involves multiple flight segments to route freight via the global “hub & spoke” network of airports and airline routes. This process follows an IATA standard known as the Master Operating Plan.

International air transport is highly regulated such as the right to pick up and deliver freight in a country, known as Traffic Rights as well as specific documentary and handling requirements for types of freight such as dangerous goods, live animals, perishables, valuables etc. These regulations are either set by the United Nations through the International Civil Aviation Organization (ICAO) and managed by its industry counterpart, the International Air Transport Association (IATA), or set and managed by IATA altogether.

### *1.1 Starting point/challenges*

Digitalisation of air cargo at an industry level has been coordinated exclusively through IATA. The exclusivity stemming from the early days of international air transport when it was one of the first globalized industries that needed interoperable standards in order to provide a seamless experience to the traveller, i.e. one ticket and one service level delivered by multiple airlines. That legacy has translated, among many other standards, into data standards for air cargo using EDI technologies using Cargo IMP standards and later Cargo XML. This so-called “e-freight” program has set the foundation for the digitalization of air cargo and the e-AWB is now used for more than 2 out of 3 shipments worldwide.

e-Freight refers to message-based technology using electronic documents that represent paper documents. Message technologies are push based, i.e. electronic documents are pushed from one party to the next. There is a lot of common data in these documents, such as shipper, consignee

and freight details which has led do data duplication, inconsistencies, data re-entry and associated errors. These push-based message technologies are unsuitable for massive digitalization of logistics and transport and the air transport industry.

The current challenge is still in the reduction of the amount of paper documents accompanying cargo flights. Push-based messaging has not been able (yet) to tackle these challenges and innovative solutions driven by for instance shippers have to be explored.

Air transport requires effective integration with other transport modes. Most air cargo arrives and is dispatched by road, rail and sometimes sea as well. This is driven by sustainability needs and optimal use of transport infrastructure. The requirement for efficient interoperability of multimodal infrastructure, including data exchange and information platforms is self-evident. This issue, however, cannot be solved by IATA alone and needs further alignment with developments in other transport modes.

### *1.2 Solutions/Outcomes*

IATA is developing a flexible data sharing standard, named ONE Record, based on ontologies and driven by large shippers. This standard for data sharing creates a single record view of the shipment based on linking data that is stored by different data providers. Rather than each party in the logistics and transport chain having to maintain data that allows them to transport goods by air, the data sharing approach allows them to (authorized) access all the data from its source and have a direct an accurate view of all the data related to their shipment based on shared links (URL – Uniform Resource Locator).

This standard is based on mature but progressive data sharing technologies that are well aligned with the best practices used by leading airlines. Ontologies, RDF (Resource Description Framework) and RDF- or triple stores are examples of this innovative technology. This makes it directly usable to IT teams and service providers.

In practice, the data sharing solution focusses on///////;

- Data model specification provides the air cargo industry with a standard structure for data exchange;
- API specification specifies the interface allows airlines and their partners to connect their system directly to each other;
- Security & Identity specification: ensures data privacy, confidentiality and sovereignty for all parties.

### *1.3 Benefits*

This provides the air cargo industry with important benefits as it:

- Drives data quality and sovereignty: Data is shared by a data owner who is in full control of data quality;
- Provides data transparency: Data sharing covers the end-to-end transportation chain, from the shipper to the consignee thus ensuring enhanced visibility and transparency;

- Facilitates Plug & Play connectivity: It facilitates the direct connectivity between all the cargo stakeholders. This will lead to new cooperative IT solutions and innovation;
- Enables a future of digital cargo: It creates the foundation for true digital air cargo where airlines, their partners and service providers will be able to develop collaborative and automated digital services.
- Welcomes a new generation: It provides a technology platform that is ready for a new generation of digital natives who will be leading the logistics and transport industry within a decade.

# 2 General Warehousing and Terminal Operations

The main target of every port Terminal is to maximize as much as possible the use of the areas at its own disposal, in order to increase the rotation of the cargo and, therefore, be able to handle as more goods as possibile.

To achieve this target, a port Terminal has mainly to:

- Improve its productivity, by using appropriate and suitable equipments;
- Reduce stop times of the cargo in the Terminal areas.

Needless to say, the last issue is mainly effected by the coordination existing between Shippers/Consignees - Forwarders – Terminal – Shipping Lines, which could be basically improved through a safe and efficient port community system.

In particular, Terminal San Giorgio is mainly focused on Short Sea line services and is especially involved in the”Motorways of the Seas” traffic, which consists in RORO cargo services connecting the north (Port of Genoa) with the south of Italy (Salerno) and also islands (Sicily and Sardinia).

This type of transportation is alternative to road transport, which is clearly faster than sea transport (even if more polluting); therefore, in order to keep this transport competitive it is important to reduce as much as possible travel and stop times of the cargo.

It is moreover important that all stakeholders involved receive basic informations in real time in order to be able to speed up operations.

## *2.1 Starting point/challenges*

Actually, all the stakeholders involved in the sea transport (Shippers/Consignees - Forwarders – Terminal – Shipping Lines) use specific softwares to organise their own activities, but generally these softwares are not interconnected with each other. As a consequence thereof, each stakeholder has now reached a good level of optimization regarding its specific part of activity, but – since information are not shared between all the players involved – the other stakeholders do not have any substancial benefit thereof.

Therefore, data sharing is absolutely important in order to save time by avoiding multiple data entries, reducing mismatches and giving to all the other players proper information to organize proper actions and operations.

Thus, as already pointed out, since a sea transport always involves many different stakeholders it is clear that a proper information stream allows all the players to be ready to properly perform their part of activities.

### 2.2 Solutions/Outcomes

Cargo tracing could be the starting point. The possibility for all the stakeholders involved in the transport to know exactly where a cargo is in each moment and to have all the documents regarding this cargo digitalized will allow the stakeholders to carry out in advance some operations and to execute their actions in a faster and more economic way.

In particular, geolocalization of trucks and vessels will be very useful for port Terminals in order to organize gate in/gate out operations of cargo and to maximize the use of the areas, without considering that also land carriers, by knowing exacly when a cargo is expected to arrive, could plan transport (custom formalities) in advance and in a more functional way.

### 2.3 Benefits

The possibility for all the stakeholders involved in the transportation to carry out their own operations in a coordinate manner based on reliable and real time information has a lot of easily imaginable benefits. In particular, it must be considered that data sharing allows the companies to save many considerable costs, for example the ones for idle personnel and, in the meantime, it has the effect to increase the global performance of a transport.

# 3 Rail Intermodality

This segment is focused on the intermodal transport of freight carried out through the modal shift between road and rail transport (and vice versa). This freight is being moved using loading units (ILU – Intermodal Loading Unit) such as trailers, swap bodies, containers or tanks without intermediate break-bulk or consolidation from “dock-to-dock”. These loading units are handled with gantry cranes or reach stackers. An important feature of this segment consists in transporting several loading units with a unique loco on the longer stretch of the route, combining the flexibility of the road transport on the last mile to reach all the customers in the area.

### 3.1 Starting point/challenges

This segment of market is characterised by a low visibility of the goods especially when they are travelling on the railway network. The Railway Undertakings and the national railway Infrastructure Managers manage their data internally in order to prevent the leakage of information and industrial espionage due to the high level of competition on this market. In addition, the priority system of the railway paths is, for the great part of the day, unbalanced in favour of the passenger transport, slowing the railway freight flow in case of simultaneous passage on the same line (during daytime, the contrary happens during night-time). All these factors are hampering an efficient management of the railway terminals since there is a lack of information of the real position of the train. The FEDeRATED approach has to take into consideration the impossibility/extremely high difficult to receive data from these players. It causes inefficiencies along the entire European intermodal chain,

affecting both the operators' activity and the customers' market. These negative conditions influence the decisions of the actors involved that sometimes prefer to use road solutions instead of intermodality. In addition, the lack of information reduces the productivity of the terminals that have to manage internal congestions caused by the delayed trains. Consequently, the surrounding road of the terminal are often crowded because the heavy vehicles like trucks have to wait more than expected to carry out the pickup or drop off activities. Compared to a simple road transport, intermodality involves at least the following players: shipper, one freight forwarder, first carrier, first terminal, train operator, second terminal, second carrier and shipper's costumers.

### *3.2 Solutions/Outcomes*

The railway operators' involvement in the digitalisation process is a key aspect to be faced in this segment of the logistics chain in order to enhance B2A cooperation. Data sharing is problematic when the majority of the MTOs (Multimodal Transport Operators) decide to keep the information about their trains internally, creating inefficiencies along the multimodal chain. B2B relations need to be improved as well, considering that the freight forwarder should have all the information available to proper coordinate the chain.

A heavy improvement of the sector can be reached through investments in ICT solutions able to prevent the leakage of information, making smoother the exchange of information. Unfortunately, there is a scarcity of time, financial resources and competences, which are slowing the digitalisation process. Therefore, an integration of the existing IT tools can be a good starting point for the realization of shared data system in which all the operators of the chain can get precious information about the real time conditions of the trains travelling on the network. The different IT systems available in the market must be set in order to communicate each other, sharing only the essential data necessary for operation management. The achievement of this objective can be pursued through a deep review of the IT network architecture that must be improved especially on the collection of the proper information and on their correct handling. Only in this way, the operative systems of the different players can launch specific queries in order to get only the necessary information. The data obtained will be merged in order to make a comparison that is necessary to get a smooth result. An essential mandatory condition is to produce a no disclosure agreement that must be signed by all the partners involved. This document will guarantee a safe exchange of information.

### *3.3 Benefits*

Currently, the approach of players operating in the intermodal chain is far from a cooperative system. Therefore, a federation of platforms that allows a safe sharing of data can enhance the visibility of the freight along the entire chain. This information flow is essential to improve the overall efficiency of the intermodal chain. The most important is certainly the possibility to increase intermodal flows compared to diesel. In order to provide some practical examples, the dispatchers will be able to optimize the daily routes of their trucks that can reach the terminal area only in the precise moment when the handling operations (pick up/drop off) will actually take place. It means to reduce the long queues outside the terminal gates, decreasing the congestions in the surrounding roads of the nodes. In addition, the terminal managers will have the opportunity to reorganize promptly all the terminal assets, comparing the scheduling to the daily forecasts provided by the IT system. In this

way, the personnel shifts and the use of the equipment is directly influenced by the effective railway traffic so the waste and the inefficiencies will be reduced to the minimum level. Lastly, the customers will be able to follow their goods in every moment, understanding if the delay in the shipment is caused by a wrong management of the freight by the operators or is due for force majeure (bad weather conditions, disruptions on the line, accidents, etc.).

# 4 Freight forwarding LTL/Groupage

LTL (less than truck loaded and groupage) transport refers to the market for individually labelled dry or staple goods from industrial or consumer goods sectors in consignments weighing between about 30 kg and two to three tons, very often being tendered in palletized forma. This market segment also includes the so-called “groupage”. The architecture of the transport considerably differs from FTL/FCL. It cannot be economically carried directly from sender to consignee but require consolidation through networks of regional collection and distribution depots and terminals, sometimes involving intermediate sorting hubs.

## *4.1 Starting point/challenges*

The complexity of the architecture of the segment which requires to organise and consolidate different shipments on a single trailer has determined the creation of a limited number of regional, national and European networks. Nonetheless, the critical elements affecting the FTL are even more exasperated in LTL segment. The consolidation of several shipments means un undetermined number of customers with different characteristics on a single trailer. The lack of capacity in collecting, managing and sharing data is the main cause for the lack of exploitation of transport capacity. For the large part of the companies, the consolidation of the cargo is managed manually without IT support or any other device. The companies which own a TMS (Transport management system) can count on a partial support which in most of the cases can be translated in collecting basic information shipment per shipment. The low level of digitalisation affects the large part of the companies in the market with the exception of the biggest and structured companies. So, the application of the data sharing concept seems difficult to be applied.

## *4.2 Solutions/Outcomes*

The first step to be considered and solved is the lack of digitalisation of the heavy and volume of the shipments to be executed. In some cases, the operation is done directly by customers but without the necessary accuracy. The market is already provided the possibility to digitalise such data. Nonetheless, further tests have to be promoted in order to improve the reliability of such systems and to allow a concrete deployment. The share of data should be direct and automatic between the IT systems of shippers and transport companies in order to set in a certified way the volumes and heavy of every shipment. Such a solution will be also necessary to avoid problems in case of controls performed by police officers on the transported cargo. Another key topic is the availability of reliable track&trace systems that should share information directly with the shippers’ systems and the consolidation/deconsolidation points. This would make easier the difficult management of the booking procedure for cargo’s slot.

In consideration with the last development of the digital tachograph, the determination of the truck

position to be integrated with a TMS could be definitively solved. Nonetheless, the management of the drivers' private data should be taken in a careful consideration.

The digital knowledge of the road segment is quite low and would need to be properly supported starting from a culturalization process.

### *4.3 Benefits*

The benefits can be summed up as follow:

A proper data sharing among shippers and transport companies could support an automatic saturation of trailers capacity. Once the shipments would get into a consolidation point the sharing of information would allow to properly verify and validate the consistency of heavy and volume of every shipment. Such a support would allow also LTL to think in a predictive way and to establish transport relations based on the exploitation of intermodal solutions.

# 5 Contract logistics

The segment of contract logistics requires a complex bundle of several logistical services such as transportation and warehouses as well as a potentially wide range of value-added services. Generally, the segment determines long-term contractual relationships tailored to an individual customer's requirements. The "contract logistics" segment is differently identified and determined by the companies dealing with it. The segment can be further divided in two sub-subset logistics on the base of the services required to the logistics provider: "strategic outsourcing" or "warehousing".

While the warehousing is simply describable as a rent of spaces, the strategic outsourcing complies ad hoc project which integrate the logistics providers with the supply chain of the production company.

### *5.1 Starting point/challenges*

The lack of consistent growth of the European economy has a negative effect on the transport business nonetheless the contract logistics segment has recorded in the last year a clear growing rate from the provider point of view. The reason has to be linked to the increased number of companies which externalize the logistics services looking for specific competences and know how that they cannot internally guarantee. The research for added value services can be considered a potential boost for the digitalisation of the whole logistics chain as for data sharing. Indeed, the trust on a logistics provider is strengthened by its transparency in managing customers' commodity. Such characterisation of the market concentrates a great know how in 3PL providers making them innovation drivers of the sector. The boundaries for a full transparency of the logistics chain managed by 3PL and 4PL providers are the lack of digitalised procedures within warehouses and the capacity to collect and managed big amount of data. Indeed, most of the companies dealing with this segment declare that their focus is their capacity to analyse and use the data collected. Not enough emphasis can be deducted to the importance of data sharing concept. The IT system characterising the contract logistics provider is generally called warehouse management system (WMS). The market provides different kind of WMS and most of the companies work with such technological support.

### 5.2 Solutions/Outcomes

The application of the concept of data sharing has to comply intermediate steps as processes and procedures optimisation, digitalisation, data collection, data processing and just finally data sharing. For a 3PL a key aspect of competitiveness is its capacity to personalise its own WMS on the base of different customers characteristics providing the data requested in a coherent and usable way for the customer. The adaptability of procedures and processes has to be coherently mirrored by the IT tools. Furthermore, it has to be highlighted that the relationships with the customers is just one element of the logistics chain managed by 3PL providers. Managing hubs with a complex mix of operations, the WMS digital cooperation has to be extended to the companies working within the warehouses and transport companies dealing with the hubs.

A clear evidence to the goods stocked within a warehouse and its movements have to be improved and recorded automatically in the WMS. This step can be obtained by technological solutions such as IoT devices or true regular and standardised stocking rules.

### 5.3 Benefits

The transparency of the logistics operations managed by the contract logistics providers could determine several benefits for the all chain. Starting from the possibility to have a clear overview of the different companies working in a hub, the logistics providers could have and demonstrate the respect of social rules and better monitoring safety and security issues. The automatic connection of information with the customers will further enhance the idea of the strategic outsourcing of the logistics chain benefiting the market growth and the importance of the transaction from an asset base market to a knowledge base one.

Introducing a clear and transparent digital cooperation, a short logistics chain not complying international transport would be able to test and deploy a dematerialised transport chain.

# 6 General Truckload / Full Carload (FTL/FCL)

This segment includes the carriage of dry goods that can be carried and stored in truck equipment such as box-type railcars, standard ISO-containers and standard swap body units. The shipment weights typically range from two to three tons per shipment up to about 28 tons (if complied rail transport). FTL cargo is moved without intermediate break-bulk or consolidation from “dock-to-dock”, resp. “ramp-to-ramp”. A special characteristic of this segment is the relative “openness” of the market for any type of cargo that may be handled with standardized equipment.

### 6.1 Starting point/challenges

This segment of market is characterised by a high level of fragmentation. The relatively simplicity of the architecture of the transport missions (point A loading – point B unloading) and the lack of economic barriers to get in the market are the main elements which have determined the current situation. The presence of many small companies and the low marginality determine a difficult engagement of these players in the digitalisation process. The FEDeRATED approach has to take into consideration the impossibility to collect data in a digitalised way from these players. This determines a strong inefficiency of the whole European transport system both from the market and

public perspectives. Some examples can better clarify the concept. Intermodal solutions cannot be applied if there is not a proper concentration of volumes in the market managed by one player or more players in a coordinated way. Small players without the capacity to share information among them will always prefer the road solution then intermodality. This condition affects also the capacity of the public to take decisions on the base of data collected on traffic flows. Small companies not connected and not crossing any border cannot be easily traced.

It has also to be noted that the conceived IT platforms generally called TMS (transport management system) are thought for internal use and never declined as tool ready to establish cooperative solutions.

### *6.2 Solutions/Outcomes*

The SMEs involvement in the digitalisation process is a key aspect to be faced in this segment of the logistics chain. Data sharing cannot be concretely promoted and become a regular practice if many players are excluded by the process.

A cultural improvement of the sector can be reached simplifying the messages and clearly presenting the advantages of investing in IT solutions. This cannot be sufficient considering the lack of availability of financial resources. Exploiting major companies as integrator of transport capacity available is certainly a good option to consider. The phenomena are already present in the market since in most of the cases small carriers do not interact directly with shippers, but they work for them through freight forwarders that can offer added value services to the customers.

IT tools available in the market have to be redefined following the logical framework of the digital cooperation. This new way of thinking has to start from answering to the following basic question: how to collect the right data, how to process them, how to share them. Considering the peculiar condition of the market, a focus just on data sharing will not support a real digital cooperation framework.

### *6.3 Benefits*

Being able to collect, process and share data in a proper way along the logistics chain will determine a better transparency of the flows of the commodities along the European transport corridors. In the short term, counting on the availability of integrated IT tools and more cooperative transport systems will reduce the inefficiencies and support the modal shift. In the long run, the automatic data sharing will path the way for a full automation of the transport system. Shippers will be able to fully exploit the transport capacity available in the market by directly booking shipments on providers TMSs. Such providers will be able to automatically dispatch the shipments exploiting the most sustainable solutions available considering not just their own assets but all the integrated partners in their logistics offer. Independently by the number players involved in a specific shipment or the different modes of transport used, data should be available by all the players in the chain on the base of their operational and commercial needs.

# 7 Short sea / Ocean Cargo

Short sea shipping is the movement of cargo and passengers by sea over short distances. The

European Commission describes short sea shipping as follows: “short sea shipping includes domestic and international maritime transport, including feeder services, along the coast and to and from the islands, rivers and lakes. The concept of short sea shipping also extends to maritime transport between the Member States of the Union and Norway and Iceland and other States on the Baltic Sea, the Black Sea and the Mediterranean. Regarding Ocean Cargo segment, the core business is the Atlantic trades: between North Europe, West Africa and South America; between South America and West Africa; and also, between North America and West Africa. Most of the shipowner fleets are deployed on these routes. It includes a substantial number of Ro/Ro-Multipurpose Container Carriers (extremely flexible in carrying large volumes of cars, rolling cargo, containers, project and oversized cargo as well), and large Pure Car and Truck Carriers (PCTC).

### *7.1 Starting point/challenges*

As the globalization of world trade accelerates, the importance of achieving operational speed without sacrificing accuracy is becoming paramount to the success of all stakeholders in the international trading system, from shippers to logistics service providers, terminal operators, and carriers, to retailers, consumers and end-users of the transported goods. Shipping industry needs better data sharing and collaboration. The maritime industry and broader ocean supply chain are suffering from major and costly inefficiencies, due to ineffective data sharing and poor cross-industry collaboration. Importers, exporters, container carriers, terminal operators, vessel owners and other stakeholders suffer from poor visibility and predictability around shipments and are losing money, due to a lack of partner synchronization and insufficient data insight. Route and voyage planning data is becoming increasingly valuable to e-navigation developments while improving navigational safety and facilitating regulatory compliance.

### *7.2 Solutions/Outcomes*

The solution could be the potential path to real-time collaboration across the industry, including cultural and operational challenges facing adoption. Real-time data access and information sharing will be important to increasing the efficiency and performance of the shipping industry. Shippers are pushing for better operational visibility; alliances will demand better ways for their carrier members to share information to improve efficiencies and customer service; and terminals and port authorities will be under pressure to increase utilization and optimize existing infrastructures. Will be necessary an open-source digital maritime domain in order to facilitate secure information exchange, not only within e-navigation but the maritime domain at large. Will be necessary to enhance communications, share information and to tackle the new commercial realities of stricter environmental regulations, tighter logistics schedules and squeezed margins. Shipping companies must adopt greater levels of digitalisation and in the longer term become a facility for storing information for autonomous shipping.

### *7.3 Benefits*

The performance metrics will improve by at least 50 percent if we could share real-time operational information. The advent of cloud-based, collaborative data-sharing platforms will enable automation of different of global supply chain processes and management of electronic booking, digital transmission of shipping instructions, and real-time container-status tracking. With the expansion of collaboration and data-sharing into the foundational end-to-end container planning processes, from stowage planning and execution to berth window management and port call optimization, the ideal

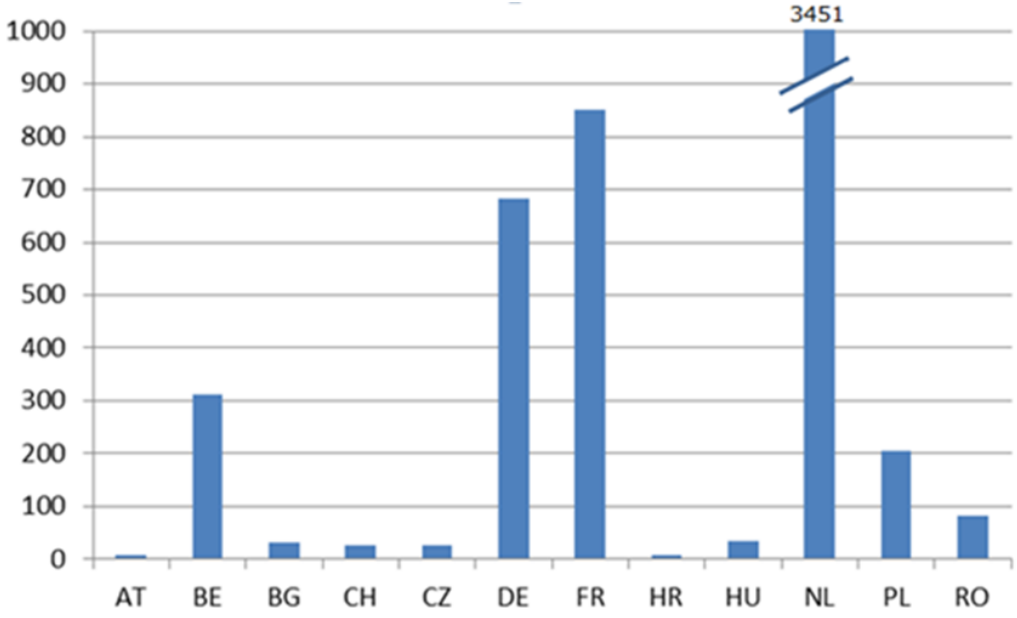
of “working as one” will appear to be within reach. Vessel owners who will share data with equipment suppliers will see improved vessel efficiency and maintenance cost reductions by transferring engine performance and other vessel condition data from ships to shore-based centres for analysis. Vessel owners in multiple sectors over time will be required to disclose information on emissions to demonstrate efficiency improvements to the IMO, regional authorities, such as the European Union, and national organisations, including the US Coast Guard.

# 8 Inland waterways

From the perspective of FEDeRATED, inland waterways is the transport of cargo via canals, rivers and other types of inland waterways such as lakes by barge (the perspective of passenger cruises is outside scope). Inland waterways are used for transport of different types of cargo, like sand for the building industry and waste that can be considered internal EU or flows of chemical products and containers in and out of Europe via (main) ports. European rivers like the Rhine and Danube are major inland waterways, but also Member States like the Netherlands utilize inland waterways for transport of non-time critical bulk cargo flows.

## *8.1 Starting point/challenges*

Like the road sector, this sector is highly fragmented. It consists of many SMEs (owning between 1-3 barges) and a small number of inland waterways shipping lines with a fleet of barges. The Dutch fleet of barge operators (over 3400) is the major one, followed by France (some 850), German (almost 700), and Belgium (around 300), see figure (2014), with in total some 22.000 employees.




Data sharing initiatives in inland waterways focus on ‘sailing’: safety – and traffic flow improvements with reduction of waiting times. RIS COMEX is the major initiative in this context, building upon the RIS Directive. Other improvements focus on handling of barges in ports and hubs: reduction of traffic flow and waiting times at terminals and hubs. These initiatives are mostly taken by ports and

terminals. The various initiatives for 'sailing' are not aligned, resulting in various applications (apps on smart devices) to be used by skippers. 'Logistics' is considered the other perspective for data sharing: visibility, reliability improvements, and better capacity utilization by customers of barge operators. The 'logistics' aspect is considered by EC DG Move DINA, but is as of yet not sufficiently tackled. The challenge for the logistics perspective is the creation of a market for integrated logistics applications that can be developed by (innovative) IT service providers. It requires standardization of APIs addressing both 'sailing' and 'logistics'.

### *8.2 Solutions/Outcomes*

Like in road transport, SME involvement in digitalisation is a key aspect to be faced in this segment of the logistics chain. However, these SMEs lack the knowledge and expertise for developing solutions. They require standardized, integrated solutions that are easy to use and support data sharing according the core operating framework.

There are two aspects to a solution. First of all, a cultural improvement of the sector can be reached simplifying the message of digitalisation and providing integrated IT solutions. These IT solutions have to be integrated in the daily operations of these barge operators/skippers, so they can use them easily during their sailing. From a cultural perspective, barge operators/skippers are used to travel solutions, but not yet integration with their customers. This needs a change.

From an IT perspective there is a lack of availability of financial resources. Thus, a market for integrating solutions has to be created. Since the inland waterways sector is basically too small for real investments in IT development (see before) and only port-hinterland corridors are considered of relevance, solutions need to be modality and cargo type independent and have to be configurable to requirements of end-users. These solutions have to be based on APIs, Application Programming Interfaces, and address all relevant areas of data sharing (from capacity booking to visibility, including collaborative types of applications on inland waterways and in ports/hubs. Instead of the development of systems and solutions, APIs that enable IT service and solution providers to develop integrated solutions have to become available. Innovative IT services will have to be developed supporting for instance ETA prediction from various perspectives (to the next lock, to the next hub, and for delivery of the cargo at the intended hub). Potentially, the perspective of PortCDM and STM has to be taken, where relevant APIs are (or will be) integrated in travel systems based on ECDIS map information for sea.

### *8.3 Benefits*

Short-term benefits are to be found in reduction of waiting times for barge operators/skippers, improved safety and traffic flow on inland waterways, and synchronisation of inland waterways in the total transport chain. The latter might reduce any unnecessary fines imposed by a consignor or consignee to a forwarder for late delivery at the final destination.

Long-term benefits are to be found in creating a predictable and reliable service building upon the short-term benefits that contributes to sustainability by better capacity utilization. Applying synchromodal planning, logistics services providers could contribute to a multi-modal split. Future investments are in (semi-)automated sailing, resulting in less employees and even more improved safety, predictability, and reliability.

# ANNEX 5: THE VARIOUS ROLES OF PUBLIC AUTHORITIES IN FREIGHT TRANSPORT AND LOGISTICS AND THE USE OF DATA

## 1 Public authority tasks

The government fulfils various tasks in its involvement with freight transport, such as:

- Infrastructure management and traffic management - drafting and monitoring rules for safety, the use of infrastructure (such as access regimes for cities) and integrating logistic data of (water) road managers (traffic jams, incidents, preferred route, loading and unloading locations) for optimal accessibility and safety. This can prevent incidents, stimulate modal shift and promote the optimal use of the physical infrastructure (roads, railways, water);
- Corridor and chain management - involvement in the streamlining of information from shipper to delivery address, so that traffic flow processing, for example intermodal transport at hubs, can take place seamlessly;
- Import duties and security (security) - generic Customs duties at entry, departure import and export of goods with all kinds of detection (terrorism, fraud, smuggling, etc.);
- Intelligence - all kinds of monitoring of illegal actions of people by police, Coast Guard and other enforcers in cooperation with for example Customs (smuggling of people, drugs and weapons, stolen goods, etc.);
- Safety and Security – developing and implementing policy, regulation, measures and infrastructure;
- Sustainability - developing a set of instruments so that the sector can realize sustainable mobility objectives (less CO2 emissions, better load factor etc.).

These tasks are performed by the government for all kinds of goods such as bulk goods, containerized goods and parcels (e-commerce). Different requirements apply to each of the types of goods, laid down in legislation, based on the social objective of safety, liveability and climate.

## 2 Use of data

Digitalisation can play an important role in the execution of government tasks. The linking of databases, internal and external data files, for example, provides the government with new insights to monitor the goods transport chain and to effectively implement risk management. In addition, digitalisation offers opportunities for the development of integrated traffic management systems, which can provide tailor-made solutions for logistic operators, and can also work on the development of autonomous transport systems. Thanks to digitalisation, efficiency gains in the performance of duties by the government can be realized in freight transport, which can also lead to cost reductions for governments and companies.

Digitalisation contributes to the realization of the sustainability agenda. Examples are the faster linking of transport modalities among each other, fewer waiting times at terminals, anticipating - and thus the possibility of preventing - congestion by real-time information systems, and the possibility of making more conscious choices for the use of sustainable transport modalities.

FEDeRATED
NETWORK OF PLATFORMS

Co-financed by the Connecting Europe Facility of the European Union