Governance-oriented analysis

Table des matières

PoA 1: Creation of the Legal Framework of ST4W - MULTITEL, LiW, TUE/e, SPB/EICB, INLECOM, TUL

In this first Point of Action, the different rules and regulations applicable for ST4W will be identified and more precisely those that can have an impact on the project.
At the beginning and from the objectives of ST4W project, the IDIT has identified eight themes related to ST4W:

- Electronic Data Regulations (personal data, commercial data, digitalization, network and information system security, …)
- Transport Information Systems (RIS, AIS, ITS, Maritime Single Window environment)
- Freight forwarding
- Maritime and Inland Terminals
- Carriage by Inland Waterway
- Carriage by Road
- Customs regulation (including "Authorized Economic Operator (AEO) status)
- Cargo community systems

For each theme, IDIT will explore and enumerate relevant International/ European, national and regional regulations (if they exist –Multitel, LiW, TUE/e, SPB/EICB, and INLECOM).
This First POA constitutes a fundamental basis for our report. This collection phase will then allow us to be able to identify the legal impacts on the development of waterway transport (we mean by legal impacts, the legal requirements and the legal obstacles which could put a brake on such development).

NB: We have used in particular the information and regulations that will have been sent to IDIT by the project partners.

Finally, IDIT focused on a more specific scope whose themes are the followings:

→ Electronic Data regulations
- Personal data and privacy
- Commercial data / Trade secrets
- Electronic commerce (identification, trust services and dematerialization /Dematerialization of goods related transport documents (in inland and road carriage)
- Transport information system (RIS/AIS)
- Cyber security : Protection of information systems

→ Reporting formalities
- Single Maritime Window
- Customs

→ Carriage by inland waterway
→ Carriage by road

Each regulation will be briefly presented, in particular with regard to its link with the ST4W project.

1.1 Electronic Data Regulations

1.1.1 Personal data and privacy

1.1.1.1 International level

IDIT : **Governance-oriented analysis**

• *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28th of January 1981*

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection"). The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors. Moreover, appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination. It also provides additional safeguards for the data subject. This Convention is applicable to Belgium, Germany, Netherlands, UK and France.

1.1.1.2 European Union

• *The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*

It requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

• *The 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)*

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

• *Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data*

• *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, 29 may 2019 – COM(2019)250*

This guidance aims to help users - especially small and medium-sized enterprises - understand the interaction between the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation.

1.1.1.3 France

• *Law n°2018-493 regarding the personal data protection – 20 June 2018*

It facilitates an effective application of the RGPD and the directive (UE) 2016/680.

1.1.1.4 Germany

• *Federal Data Protection Act (BDSG) - 30 June 2017*

This Act shall apply to the processing of personal data by public and private bodies.

1.1.1.5 Belgium

• *Law relating to the protection of individuals with regard to the processing of personal data – 30 July 2018 (I.e. the Privacy Act)*

The Privacy Act both transposes the Directive for Police and Criminal Justice Authorities in Belgian law and supplements or specifies some specific provisions of the GDPR.

• *Law amending the Law of 2 October 2017 regulating private and particular security with regard to the processing of personal data – 9 may 2019 (Brussels)*

1.1.1.6 Netherlands

• *The Dutch GDPR Implementation Act (AVG) - 22 may 2018*

The Act contains rules on the implementation of Regulation (EU) 2016/679.

1.1.1.7 United-kingdom

• *The Data Protection Act - 23 may 2018*

The Data Protection Act 2018 achieved Royal Assent on 23 May 2018. It applies the EU's GDPR standards and makes provisions about the processing of personal data. It also implements the EU Law Enforcement Directive.

1.1.2 Commercial data / Trade secrets

1.1.2.1 European Union

• *Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*

It aims to standardize the national laws in EU countries against the unlawful acquisition, disclosure and use of trade secrets. The directive harmonizes the definition of trade secrets in accordance with existing internationally binding standards. A trade secret is a valuable piece of information for an enterprise that is treated as confidential and that gives that enterprise a competitive advantage.

1.1.2.2 France

• *Law n°2018-670 relating to the protection of trade secrets implementing the Directive (UE) n°2016/943 – 30 July 2018*

It transposes the directive 2016/943/UE.

1.1.2.3 Germany

• *Law transposing the Directive (UE) 2016/943 (« Gesetz zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung »)*

1.1.2.4 Belgium

• *Law transposing the same directive relating to the protection of trade secrets – 30 July 2018*

1.1.2.5 Netherlands

• *Law on the protection of Trade Secrets (« Wet bescherming bedrijfsgeheimen ») transposing the Directive – 17 October 2018*

1.1.2.6 United-Kingdom

• *Intellectual Property the Trade Secrets Regulations – 9 June 2018*

1.1.3 Electronic commerce

1.1.3.1 Electronic identification and trust services

1.1.3.1.1 International

• *The UNCITRAL Model Law on Electronic Commerce 1996*

It purports to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce.

• *The Model Law on Electronic Signatures 2001*

It aims to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures.

• *UNCITRAL Model Law on Electronic Transferable Records 2017*

It aims to enable the legal use of electronic transferable records both domestically and across borders. The MLETR applies to electronic transferable records that are functionally equivalent to transferable documents or instruments.

1.1.3.1.2 European Union

• *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market*

The Electronic Identification and Trust Services (eIDAS) Regulation creates a new system for secure electronic interactions across the EU between businesses, citizens and public authorities. It aims to improve trust in EU-wide electronic transactions and to increase the effectiveness of public and private online services and e-commerce.

1.1.3.1.3 France

• *Law n°2000-230 adapting the law of evidence to information technology and relating to electronic signature – 13 March 2000*

Adapting the law of evidence to information technology and in relation to electronic signatures, it recognizes the legal value of electronic documents and signature.

• *Article 1367 of the Civil code (Decree n°2017-1416 on electronic signature – 28 September 2017)*

A signature which is required in order to perfect a juridical act identifies its own author. It demonstrates his consent to the obligations which stem from that act. Where it is placed on the act by a public official, it confers authenticity on it.
Where it is in electronic form, it must use a reliable process of identification which guarantees its relationship with the act to which it is attached. The reliability of the process is presumed in the absence of proof to the contrary where an electronic signature is created, the identity of the

signatory is ensured and the integrity of the act is guaranteed on the conditions fixed by decree of the Conseil d'État.

1.1.3.1.4 Germany

The national regulations required for this Regulation adopted the "eIDAS Implementation Act= eIDAS - Umsetzungsgesetz" on July 29, 2017, in particular the Trust Service Act (VDG) issued together with Article 1. The trust regulation for the VDG was issued on February 15th, 2019. The previous Signature Act was expired on 29th of July 2017.[1]

1.1.3.1.5 Belgium

• *Law relating to electronic identification – 18 July 2017*

1.1.3.1.6 Netherlands

1.1.3.1.7 United-Kingdom

1.1.3.2 Dematerialization

• *Proposal for a regulation of the European Parliament and of the Council on electronic freight transport information COM/2018/279 final/2 - 2018/0140 (COD)*

This initiative is part of the Third "Europe on the Move" Package, which delivers on the new industrial policy strategy of September 2017, and is designed to complete the process of enabling Europe to reap the full benefits of the modernization of mobility. It will enable the use of electronic means for transmission of regulatory information on cargo transport to the authorities not just at the point of entry and exit of the EU, but also on the entire EU territory.

• *Inception Impact Assessment Ref. Ares (2017), European Commission, 15 december 2017 – Digital tools for inland waterway transport*

The initiative will aim at developing digital tools to facilitate compliance and enforcement of IWT legislation.

• *Dematerialization of Goods related transport documents* (Inland waterways and road carriage)

[1] https://www.buzer.de/s1.htm?g=eIDAS-Durchf%C3%BChrungsgesetz&f=1

1.1.4 Transport information systems (RIS/AIS)

1.1.4.1 RIS

1.1.4.1.1 International

• *Guidelines and recommendations for RIS (Translation and adaptation adopted by the CCNR RIS Working Group on August 30, 2012)*

These guidelines set out the general principles and requirements for the planning, implementation and operation of inland navigation information services and related systems. In particular, they contain the definitions and explanations of terms relating to RIS. In 2002, the CCNR adopted the guidelines and recommendations for inland navigation information services (RIS Directives) and updated them in 2012. These guidelines and recommendations are reproduced in the same way in Regulation (EC) No. 414 / 2007 of the European Commission.

• *CCNR Protocol (30.5.2012) adopts the CCNR strategy for the development and implementation of river information services on the Rhine*
• *Rhine Police Regulations (RPR) RIS (art. 4.07)*
• *Rhine Vessel Inspection Regulations (RVIR) RIS (art. 7.06, chiffre 3)*

1.1.4.1.2 European Union

• *Directive 2005/44 on harmonised river information services (RIS) on inland waterways in the Community (7/09/2005)*

The legal framework for RIS is based on Directive 2005/44/EC which sets binding data reporting rules and a minimum level for river information services. The Directive provides a European-level framework for the harmonized implementation of RIS and the compatibility and interoperability between current and future information systems in Europe. It specifies, for example, which waterways RIS are mandatory (cross-border corridors, etc.)
The directive and its regulations of the commission in its application describe the general principles and conditions for the planning, implementation and operation of river information services and associated systems. They are applicable to cargo, passenger and pleasure craft vessels. The three regulations of the commission (CEC, 2007a, 2007b and 2010) define the technical specifications of the main RIS technologies.

River Information Services (RIS) are harmonized IT services that support traffic and transport management on inland waterways, particularly at the interface with other modes of transport. They are designed to improve the safety and efficiency of inland waterway transport by optimizing traffic and transport processes. The exchange of information takes place through a rapid electronic data transfer between water and the coast, demand-driven, through real-time information exchange. The information is used in different systems and applications to improve the traffic and transport process. The information is shared on the basis of harmonized information and communication systems.

The purpose of RIS is to streamline the exchange of information between all stakeholders involved in inland water transport. Since 2005, the EU Framework Directive has established minimum requirements for the implementation of RIS and RIS standards agreed to allow cross-border compatibility of national systems.

Through the exchange of information, transport operations (such as trip planning or lock opening times) can easily be optimized and enable inland navigation to be better integrated into intermodal logistics chains.

- Commission regulation (EC) No 415/2007 concerning the technical specifications for vessel tracking and tracing systems referred to in Article 5 of Directive 2005/44/ (13/03/2007)
- Commission regulation (EC) No 414/2007 concerning the technical guidelines for the planning, implementation and operational use of river information services (RIS) (13/03/2007)
- Commission regulation (EC) No 416/2007 concerning the technical specifications for Notices to Skippers as referred to in Article 5 of Directive 2005/44/ (22/03/2007)
- Commission regulation (EU) No 164/2010 on the technical specifications for electronic ship reporting in inland navigation (20/01/2010)
- Commission Implementing Regulation (EU) No 909/2013 Inland ECDIS (10/09/2013)

1.1.4.1.3 France

• *French legal framework of RIS: Articles D.4411-1 to 8 of the Transport Code (supplemented by a Decree 2008-168 of 22 February 2008 on harmonized river information services (RIS) on Community waterways*

France has transposed Directive 2005/44/EC by Decree 2008-168 of 22 February 2008 on harmonized river information services (RIS) on the inland waterways of the Community, which has been codified by Decree No 2013-253 of March 25, 2013 relating to the provisions of the fourth part of the Transport Code. The French legal framework for RIS is now part of Articles D.4411-1 to 8 of the Transport Code. They are supplemented by a Decree of 18 March 2008[2] .

Voies Navigable de France (VNF) provides coordination for the implementation and interoperability of RIS on the French network (Article D.4411-5 of the Transport Code). VNF ensures the exchange at the national level, as well as the treatments made necessary by these exchanges, with the managers and users of RIS. It is the same at the international level with the authorities in charge of river information services notified to the European Commission. The modalities of these exchanges are fixed by order of the Minister of Transport. The waterway managers (listed in Article 1 of the Decree of 18 March 2008) set up and manage the river information services, they are responsible for (Article D.4411-3 and Article 3 of the order of 18 March 2008):

- Implement RISs so that their application is efficient, scalable and interoperable to interact with other RIS applications and, if possible, with other modes of transportation. They must also provide interfaces with transport management systems and commercial activities;
- Provide RIS users with all relevant data regarding navigation and travel plans on these waterways. These data are at least provided in an accessible electronic format;
- Provide users of RIS, in addition to the data referred to in the previous paragraph, electronic maps adapted to navigation for all their waterways;
- Providing, in the form of standardized, encoded and downloadable messages, notices to skippers, including information on the status of the waterway, water level, headroom

[2] Decree No. 2008-168 of 22 February 2008 on Harmonized River Information Services (RIS) on Community Waterways (Official publication: Official Journal of the French Republic (JORF), Date of publication: 2008-02-24); Repealed by Decree No. 2013-253 of 25 March 2013 on the provisions of the Fourth Part of the Transport Code (Decrees in Council of State and Single Decrees) - Order of 18 March 2008 pursuant to Article 2 Decree No. 2008-168 of 22 February 2008 on Harmonized River Information Services (RIS) on Community Waterways (Official publication: Official Journal of the French Republic (JORF), Date of publication: 2008-03-23)

and freezing. The standard message contains at least the information necessary for safe navigation;
- Provide RIS users with a service for tracking and tracing boats on the inland waterways referred to in Article 1. For the purpose of the use of this automatic identification system, the Regional Arrangement for the Radiotelephone Service on Inland Waterways concluded at Basel on 6 April 2000 under the Radio Regulations of the International Telecommunication Union (ITU) is applicable.

1.1.4.1.4 Germany

• *Inland Waterways Act (Binnenschiffahrtsaufgabengesetz – BinSchAufgG) 15.02.1956 (last amended by article 1 of the law of 25 April 2017)*

Under the Binnenschiffahrtsaufgabengesetz - BinSchAufgG, the controlling authority in charge of RIS in Germany is the Wasserstraßen - und Schifffahrtsverwaltung des Bundes (WSV)[3] . In so far as this is necessary for the operation of the inland navigation information services, in particular for traffic and traffic information, the services of the Bundes Wasserstraßen und Schifffahrtsverwaltung may collect, process and use the following data:
- Identification marks of a registered vessel or association
- Identification of the owner, the supplier, the charterer, the tenant, the debtor or the guide of a ship (last name, address ...)
- from the port of departure and arrival, route, last departure and next port, estimated time of departure and arrival, also on the inland navigation facilities, position at the time of data collection, speed, direction of the journey, status, number of blue cones or lights and draft,
- Cargo data, including type of cargo, HS code, port of loading, port of destination and size of cargo (in tonnes) and, in the case of dangerous goods, name of the cargo, cargo code, class , packaging code and UN number.

1.1.4.1.5 Belgium

• *Royal Decree amending the Royal Decree of 19 March 2009 on the technical requirements for inland navigation vessels (transposition of Directive 2005/44) of 26 December 2013*

• *Order of the Walloon Government transposing Directive 2005/44 of 7 September 2005*

The Walloon Government Decree of 7 September 2005 lists in its Article 2 the inland waterways concerned by the RIS. It concerns all the waterways of the Walloon Region of class IV and higher as well as in the ports situated on these waterways.

The regional administration service responsible for the management of waterways is designated as the Walloon competent authority for RIS applications and international data exchange (Article 4). This competent authority is responsible for taking all necessary measures to implement RIS effectively, scalable and interoperable. It also provides interfaces with transport management systems and commercial activities. In accordance with the guidelines defined by the European Commission, the competent authority:
- Provides RIS users with all relevant data concerning navigation and travel plans on inland waterways. These data are at least provided in an accessible electronic format. The data are listed in the appendix of the decree;
- Ensure that RIS users have, in addition to the data, electronic maps suitable for navigation for all its waterways;

[3] Inland Waterways Act - BinSchAufgG of 15.02.1956 as last amended by article 1 of the law of 25 April 2017

- Empowers the competent authority to receive electronic records of the data to be provided by the vessels. For cross-border transport, this information is transmitted to the relevant competent authorities concerned before the arrival of the vessels at the border;
- Ensure that notices to skippers, including information on the water level (or maximum allowable draft) and freeze on their inland waterways, are provided in the form of standardized, encoded messages and downloadable. The standard message contains at least the information necessary for safe navigation. Notices to Skippers are at least provided in an accessible electronic format.

• *Order of the Government of the Brussels-Capital Region transposing Directive 2005/44 / EC of the European Parliament and of the Council of 7 September 2005*

The Order of the Government of the Brussels-Capital Region of 7 September 2005 lists in its Article 3 the waterways and ports concerned by the RIS. These are all Class IV or higher inland waterways connected by a Class IV waterway or above to a Class IV or higher waterway of another Member State and ports on the inland waterways. The RIS application is efficient, can be expanded and is interoperable, so that it can be coupled with other RIS applications, other transport management systems and business activities, and possibly systems for other modes of transport (Article 4).

The Port of Brussels is the competent authority. He is responsible for the performance of RIS obligations and the exchange of data (Article 5). The competent authority shall provide security measures and procedures to safeguard RIS messages and archives from untoward events or misuses, including illegal access, changes or loss of data. It ensures, among other things, that this data is not accessible to unauthorized staff members and external staff.
For the setting up of RIS, the competent authority:

- Provides RIS users with all relevant data concerning navigation and travel plans on inland waterways. These data contain at least: the river axis with kilometric indication; restrictions on vessels or convoys in terms of length, width, draft and draft; the schedules of the limiting structures, in particular locks and bridges; the location of ports and trans-shipment sites; reference data on water level gauges for navigation;
- Ensure that RIS users have navigable electronic maps for all their class Va and higher waterways in accordance with the European Inland Waterways classification;
- Ensure, as far as national or international regulations require the notification of ships, to be able to receive electronic records of the data to be provided by the vessels. For cross-border transport (when the border with a neighboring Member State is crossed, when the border with a neighboring Region is crossed, when the border with a neighboring waterway manager is crossed) this information is transmitted to the competent authorities of the Member State concerned. Neighboring Member State, Neighboring Region or Neighboring Waterway Manager, before the arrival of the vessels at the border;
- Ensure that nautical publications, including information on the water level (or maximum allowable draft) and freeze on their waterways, are provided in the form of standardized, encoded and downloadable messages. The standard message contains at least the information necessary for safe navigation. Nautical publications are at least provided in an accessible electronic format.

• *Flemish Government Decree on River Information Services on Inland Waterways of 19 December 2008 / Order of the Flemish Government implementing the Decree of 19 December 2008*

The Decree of the Flemish Government of 19 December 2008 lists in its Article 4 the navigable waterways and the ports concerned by the RIS. These are all Class IV or higher inland waterways connected by a Class IV waterway or above to a Class IV or higher waterway of another Member State and ports on the inland waterways. In accordance with Article 6 of the Decree, the Flemish Government has designated the competent authority responsible for implementing the obligations of the Decree and the exchange of information.
"De Scheepvaart" (The Navigation), "Waterwegen en Zeekanaal" (Inland Waterways and Sea Canal), the Navigation Assistance Division of the "Agentschap voor Maritieme Dienstverlening en Kust" (Maritime Service Delivery Agency) and of the Coast) and the port authorities ", act as competent authority within the framework of the article 3, § 1, 1 ° of the decree (article 2 of the decree of the Flemish Government executing the decree of 19 December 2008 relating to River Information Services on Inland Waterways).
The tasks of the competent authority designated by the Flemish Government are the same as those listed in the Order of the Government of the Brussels-Capital Region of 7 September 2005 (see above)

1.1.4.1.6 Netherlands

• Law of 21 July 2007 amending the law on maritime traffic as part of the implementation of Directive 2005/44/EC - Decree of 2 October 2007 setting the date of entry into force of the law of 21 July 2007 amending the law on maritime traffic September 2005 laying down rules on the receipt, storage and supply of transport data by organizations and persons not involved in the transport and application of river information services to Inland navigation

• Regulation of the Minister of Infrastructure and Environment of 27 April 2012 laying down additional rules for navigation and non-navigating organizations and persons with regard to notifications and communication (notification regulation) and maritime communication)

• Regulation of the Secretary of State for Transport, Public Works and Water Management designating the competent authority and providing data relating to navigation under the Merchant Shipping Data Decree 2007.

The Netherlands has transposed Directive 2005/44 by amending the Maritime Traffic Act and the Secretary of State Circulation[4] , Public Works and Water Management Regulations containing the designation of the competent authority and the transmission maritime transport services data related to the 2007 Shipping Data Decree 2007 (supply regime for 2007 maritime transport data)[5] .

Several organizations have been designated as competent authorities under the Maritime Traffic Act. The management of the shipping lanes is entrusted to various governing bodies. These are the government (invested via the Rijkswaterstaat), the province, the municipality and / or another public entity, including for example the harbor masters[6] . Rijkswaterstaat is responsible for the management of the waterways at national level.

In accordance with Article 40 of the Inland Navigation Act Harbor Masters of Port of Amsterdam NV and Rotterdam NV have also been designated as competent authorities.
The Coast Guards are managers of the waterways for the coast of the Netherlands.

[4] Official publication: Staatsblad (Bulletin of laws and royal decrees); Number: 287; Publication date: 2007-08-28
[5] Staatscourant (Dutch Official Journal); Number: 192; Publication date: 04/10/2007;
[6] Art. 2 paragraph 1 of the maritime traffic law

The waterways managers are responsible for ensuring the safety and the fluidity of the traffic; Receiving, storing and providing shipping data by organizations and persons not involved in the navigation[7] and for the proper implementation of river information services (RIS), and therefore the AIS regarding the processing of personal data[8].

1.1.4.1.7 United-Kingdom

The Directive 2005/44 has not been transposed by the United Kingdom. With regard to River Information Services (RIS), the United Kingdom uses ECDIS for navigation purposes, but for cargo and ship information the approach is still conventional (in paper form). There is no Electronic Reporting Information.

[7] Art. 4 paragraph 1 of the maritime traffic law
[8] Art. 4 (4) of the Maritime Traffic Act

1.1.4.2 AIS

1.1.4.2.1 International Level

• *SOLAS Chapter V safety of navigation, 1st July 2002*

The SOLAS Convention is published by the IMO (International Maritime Organization). SOLAS Chapter V refers to the Safety of Navigation for all vessels at sea.
Regulation 19 of SOLAS Chapter V - Carriage requirements for shipborne navigational systems and equipment - sets out navigational equipment to be carried on board ships, according to ship type. In 2000, IMO adopted a new requirement (as part of a revised new chapter V) for all ships to carry automatic identification systems (AISs) capable of providing information about the ship to other ships and to coastal authorities automatically.
The regulation requires AIS to be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size. The requirement became effective for all ships by 31 December 2004.

Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.
A flag State may exempt ships from carrying AISs when ships will be taken permanently out of service within two years after the implementation date. Performance standards for AIS were adopted in 1998.
The regulation requires that AIS shall:

- Provide information - including the ship's identity, type, position, course, speed, navigational status and other safety-related information - automatically to appropriately equipped shore stations, other ships and aircraft;
- Receive automatically such information from similarly fitted ships; monitor and track ships;
- Exchange data with shore-based facilities.

1.1.4.2.2 European Union

• *Directive 2005/44 on harmonized river information services (RIS) on inland waterways in the Community*

The Directive 2005/44 does not impose a formal obligation to introduce AIS. It dictates, however, that member countries must use transponders in accordance with the Inland AIS standard if they want to implement the automatic announcement of boats on their inland waterway network. The European Union has also published technical specifications for Inland AIS, the system used for inland navigation.

• *Commission implementing regulation (EU) 2019/838 on technical specifications for vessel tracking and tracing systems and repealing Regulation (EC) No 415/2007 ; Commission Regulation (EC) No 2019/838 of 20 February 2019 concerns the technical specifications applicable to the systems for monitoring and locating vessels as referred to in Article 5 of Directive 2005/44/EC on harmonized river information (RIS) on Community waterways. It repeals Regulation (EC) No 415/2007.*

According to this text, the use of AIS for automatic identification and for monitoring and locating vessels in the context of inland navigation has the following characteristics. AIS is:

- ✓ a marine navigation system introduced in accordance with the IMO provision requiring all SOLAS vessels to have one,

- ✓ a system operating both in ship-to-ship mode and in "ship to land station" or "land-to-ship station" mode,
- ✓ a security system meeting strict criteria in terms of availability, continuity and reliability,
- ✓ a real-time system through the direct exchange of ship-to-ship data,
- ✓ a system operating independently and self-organized without master station. A central control intelligence is not needed,
- ✓ a system based on international standards and procedures in accordance with Chapter V of the IMO SOLAS Convention,
- ✓ a system approved to improve the safety of navigation according to a certification procedure,
- ✓ An interoperable system.

Inland AIS is based on maritime AIS according to the IMO SOLAS regulation. It includes the main functionality of the IMO SOLAS AIS while taking into account the specific needs of inland navigation.
Only tracking, location and security information should be transmitted using the Inland AIS. The provisions concerning the data contained in the AIS messages may vary according to the regulations in force in the State concerned or in the region concerned. The data transmitted by Inland AIS devices can be classified into different categories.
The static data relating to the boat include the following data:

- MMSI (the maritime mobile radiotelephone service number), the name of the vessel, the call sign and the ENI number. Some boats also have an IMO number;
- The type of vessel, the dimensions (length and width) and the location of the GPS antenna on board are static data for all insulated vessels (ie not part of a convoy pushed or towed), whereas this is trip data when it is a convoy. The static data relating to the boat does not change, as long as its owner, nationality or other parameters are not modified. Static ship data is entered, configured, and password protected during the installation process. If one or more static vessel data fields contain incorrect data, this must be corrected by an approved specialized company.

The dynamic data relating to the boat is all the data concerning the movements of the boat, for example its position, speed, heading and navigational status. The dynamic data for the boat is automatically derived from the sensor signals installed on board.
Travel data is the data that relates to the actual trip of the boat. Among them are the port of destination, the current depression and the nature of the goods transported (The dangerousness of the goods is determined by a number of blue cones). All the data mentioned under "travel data" are not mandatory in all countries.
Traffic management information is intended for the specific use of inland navigation. This information is transmitted when necessary or by request by / to inland navigation vessels only.

1.1.4.2.3 France

● *Article R4241-50 of the Transport Code*
● *Article A4241-50-2 of the Transport Code*
● *Order of 2 February 2011 on the approval of equipment and companies installing signal lights, radar equipment, rate-of-turn indicators and Inland AIS equipment.*

Article R4241-50 of the Transport Code provides that special police regulations may also require the use of an automatic identification system on certain vessels.
The type of equipment, the installation methods and the methods of use of the radar device and the automatic identification system are defined by order of the Minister of Transport.
When the special police regulations, in application of Article R. 4241-50, require the use of an automatic identification system (AIS), this system must be installed and used in accordance with the

provisions of the provisions of the Article A4241-50-2 of the Transport Code. Only AIS for inland navigation approved and installed in accordance with the provisions of the decree of 2 February 2011 on the approval of equipment and companies installing signal lights, radar equipment, speedometer indicators, are authorized. The Inland AIS unit must be in good working order, it must operate continuously and the data entered must correspond at all times to the actual data of the vessel or convoy. The Inland AIS device must transmit at maximum power.

The obligation to operate permanently does not apply to stationary vessels unless they are parked in the channel or in other situations defined by the specific police regulations; nor to law enforcement and customs ships if the transmission of AIS data is likely to compromise the performance of police or customs operations. Vessels belonging to a convoy, with the exception of the main propulsion vessel, shall switch off the AIS devices on board as long as these vessels remain in the convoy.

The following data must be issued in accordance with the Inland AIS standard referred to Article 4241-50-2 §5 of the Transport Code:

- Transpondeur identifier (Maritime Mobile Service Identity, MMSI);
- Name of the boat;
- Type of boat or convoy;
- Unique European Vessel Identification Number (ENI) or, for seagoing vessels not assigned an ENI, the IMO number;
- Overall length of the vessel or convoy with an accuracy of 0.1 meters;
- Overall width of the boat or convoy with an accuracy of 0.1 meters;
- Position (WGS 84);
- Speed on the road;
- Road;
- Time of the electronic device of location;
- Navigation status;
- Point of acquisition of the information relating to the position on board the boat.

1.1.2.9.2.4 Germany

All commercial vessels over 300 GT on international voyages since January 1st, 2004 and commercial vessels over 500 GT on domestic voyages from first of July 2008, are required to run the AIS system. Vessels longer than 20 meters or carrying more than 50 passengers must also be equipped with AIS devices. The equipment requirements were introduced on the first of July 2002, for both new ships and for ships existing since 2004. The International Maritime Organization has set different transition periods for passenger ships, ferries, cargo ships and oil tankers.[9]

Each ship uses special means of transport to send very specific data such as destination port, location, route, speed or draft. With these position data, ships can be displayed on the electronic maps.[10]

[9] http://www.schiffundtechnik.com/lexikon/a/ais.html

[10] https://www.brueckenbote.de/das-ist-ais/

1.1.2.9.2.5 Belgium

• *Article 4.07 of the Royal Decree of April 4, 2014 laying down the General Police Regulations for Navigation on the Inland Waters of the Kingdom, which lays down the rules on AIS in Belgium.*

Under this text, vessels must be equipped with an Inland AIS device to be permanently operational. The data entered must correspond at all times to the actual data of the vessel or convoy.

• *In Flanders, according to Decree 17.11.2017*, all inland navigation vessels, regardless of their use (freight or passenger transport), are required to have an AIS device on board since 8 January 2018. The installation and operation of the river navigation system.

• *Since the 1st January 2012, the AIS system is mandatory in the port area of the Port of Antwerp.*

1.1.4.2.6 Netherlands

● *Law of 21 July 2007 amending the law on maritime traffic as part of the implementation of Directive 2005/44/EC*
● *Decree of 2 October 2007 setting the date of entry into force of the law of 21 July 2007 amending the law on maritime traffic September 2005; laying down rules on the receipt, storage and supply of transport data by organizations and persons not involved in the transport and application of river information services to Inland navigation*
● *Regulation of the Secretary of State for Transport, Public Works and Water Management designating the competent authority and providing data relating to navigation under the Merchant Shipping Data Decree 2007*

AIS has been mandatory since the 1st of December 2014 and on Dutch inland waterways since 1 January 2016. The introduction of AIS into Dutch inland navigation is the result of the European RIS rules.

1.1.4.2.7 United-kingdom

1.1.5 Cyber Security : protection of information system

1.1.5.1 International

•*The Convention on Cybercrime of the Council of Europe (Budapest Convention) – 23 November 2001*
The Convention on Cybercrime is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

1.1.5.2 European Union

• *The Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*

It proposes a wide-ranging set of measures to boost the level of security of network and information systems (cybersecurity*) to secure services vital to the EU economy and society.

1.1.5.3 France

•*The Law n°88-19 on computer fraud - 5 January 1988*

France has adopted an extensive legal framework on cybercrime and computer-related offences, starting with the Law no 88-19, 5 January 1988, on computer fraud ("Godfrain Law") and its amendments, as codified by Article 323-1 à 323-7 of the Penal Code.

1.1.5.4 Germany

The "Cybersecurity Strategy for Germany 2016" adopted by the Cabinet on November 9., 2016, is currently being evaluated and subsequently updated. It forms the cross-departmental strategic framework for the German government's cybersecurity activities. The new cybersecurity strategy, which will be introduced in the future, will contain strategic goals and measures to further improve the security of cyberspace.[11]

1.1.5.5 Belgium

•*Law on Computer crime – 28 November 2000*

1.1.5.6 Netherlands

• *Computer Crime Act III (Wet Computercriminaliteit III) - 21 September 2018*

The Act aims to improve the efficiency of tackling cybercrime, to which end various provisions in the Dutch Criminal Code (DCrC) and the Dutch Code of Criminal Procedure (DCCrP) will be amended.

[11] https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/it-und-cybersicherheit-node.html

1.1.5.7 United-Kingdom

•*Computer Misuse Act 1990*

It is an act to make provision for securing computer material against unauthorized access or modification; and for connected purposes.

•*The National Cyber Security Strategy 2016 to 2021*

The Programme provides a focal point for cyber activity across government and has already led to some notable innovation, such as the establishment of the National Cyber Security Centre (NCSC). The Programme has also reduced the UK's vulnerability to specific attacks.

1.2. Reporting formalities for ships in Inland waterway

1.2.1. Maritime Single window

1.2.1.1. European union

• *Directive 2010/65/EU 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*

The EU Directive 2010/65/EU requires Member States to provide a national 'Single Window' through which maritime reports can be made, including data covered by the International Maritime Organization's standard forms under the "IMO FAL Convention". Member States shall, in accordance with the applicable legal acts of the Union or national legislation, take the necessary measures to ensure the confidentiality of commercial and other confidential information exchanged in accordance with this Directive. Member States shall take particular care to protect commercial data collected under this Directive. In respect of personal data, Member States shall ensure that they comply with GRPR.

The forms provide advance data regarding the ship, its voyage, stores, crew, passengers, dangerous cargo, and security, waste / health information. The aim of the directive is to simplify and digitize the process of handling legally required pre-arrival/departure paperwork, where necessary, so that data can be submitted simply and quickly via one online portal, alongside existing portals, in an electronic format, and meeting the Directive's requirements.

The ship's Master, or a person authorized by him/her (i.e. a "ship's agent"), is responsible for making the report. A shipping agent usually lodges the report on the master's behalf. Original documents can be uploaded as an attachment to the form if necessary.

➢ <u>List of reporting formalities referred to in this directive</u>

- Reporting formalities resulting from legal acts of the Union
- This category of reporting formalities includes the information which shall be provided in accordance with the following provisions:
- Notification for ships arriving in and departing from ports of the Member States (Article 4 of 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 (OJ L 208, 5.8.2002, p. 10).
- Border checks on persons (Article 7 of Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 105, 13.4.2006, p. 1))
- Notification of dangerous or polluting goods carried on board (Article 13 of 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)
- Notification of waste and residues (Article 6 of Directive 2000/59/EC of the European Parliament and of the Council of 27 November 2000 on port reception facilities for ship-generated waste and cargo residues (OJ L 332, 28.12.2000, p. 81))
- Notification of security information (Article 6 of Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6))

Until the adoption of a harmonized form at international level, the form set out in the Appendix to this Annex shall be used for the transmission of information required under Article 6 of Regulation (EC) No 725/2004. The form can be transmitted electronically.

- Entry summary declaration (Article 36a of Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code (OJ L 302, 19.10.1992, p. 1) and Article 87 of Regulation (EC) No 450/2008 of the European Parliament and of the Council of 23 April 2008 laying down the Community Customs Code (Modernised Customs Code) (OJ L 145, 4.6.2008, p. 1))
-

➢ <u>FAL forms and formalities resulting from international legal instruments</u>

Member States shall accept FAL forms for the fulfilment of reporting formalities. This category of reporting formalities includes the information which shall be provided in accordance with the FAL Convention and other relevant international legal instruments.

- FAL form 1: General Declaration:

The FAL concerns arrival/departure particulars of the ship, its voyage, crew/passengers numbers, cargo description, and indicates which other FAL forms are to be completed as part of the final submitted package. The authorities receive relevant data at least 24 hours in advance of arrival at the port in the United Kingdom. If the voyage length is under 24 hours, the report must be completed at the time the ship leaves the previous port. If the port of call changes during the voyage, or is unknown at departure, the report must be submitted as soon as this information becomes available. The time of report will be taken from the receipt of the package. Ships are typically also required by port operators to provide information before or upon arrival, to ensure that the ship is serviced appropriately during its call.

- FAL form 2: Cargo Declaration

The FAL 2 form is a declaration of cargo carried.

- FAL form 3: Ship's Stores Declaration
-
- FAL form 4: Crew's Effects Declaration

The FAL 4 form is used to declare certain personal effects of individual crew members. Each member of the crew is only required to complete this form in respect of any personal effects that are in excess of their travellers allowance or subject to prohibitions or restrictions. The FAL 4 form is to be made available for inspection when requested by Border authorities.

- FAL form 5: Crew List / FAL form 6: Passenger List

The FAL5 and FAL6 combined form must always be reported for all applicable voyages/vessels. The crew and passenger manifests are required for security / immigration and customs purposes. It is therefore imperative that the FAL5/6 form is completed accurately. The completed FAL5/6 data will be submitted to Border Force.

- FAL form 7: Dangerous Goods

Ships carrying dangerous goods as cargo (defined in guidance and legislation) must submit a declaration of the dangerous goods in the manifest. The FAL 7 form constitutes the minimum information required, which in many cases may have been superseded by more modern methods of cargo data transfer (as is also the case with the FAL 2 cargo declaration) including Vessel Traffic Monitoring information.

The ISPS code requires ships engaged on international voyages to provide prearrival notification. It applies to all passenger vessels and cargo vessels over 500GT, unless a specific exception is in place (further guidance is available on applying for an exception from the Department for Transport). The ISPS declaration (also known as the Pre-Arrival Notification or PAN) is currently submitted in advance directly to the Port's Port Facility Security Officer (PFSO).
The Directive 2010/65/EU will be repealed from 15 August 2025 and Regulation (EU) 2019/1239 will apply from that date.

• *Regulation (EU) 2019/1239 of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU*

Despite the contributions of Directive 2010/65 / EU on the reporting formalities applicable to ships, the fluidity of traffic in European ports remains weighed down by formalities. The Regulation (EU) No 2019/1239 repeals this directive and sets up a single European maritime window system (" EMSWe ").

The European Commission has indeed noted a lack of harmonization between the various National Single Window (NSW). Interface, data formats and declarative procedures differ as Directive 2010/65/EU has no binding specifications. Only a certain number of reporting obligations pass through the NSW, while many others, including customs, pass through other channels. In addition, in most Member States, data sharing between administrations is not satisfactory, forcing maritime operators to provide the same information several times within the same call, contrary to the principle of Reporting only once.

Hence the adoption of Regulation (EU) No 2019/1239 whose main objective is to establish harmonized rules for the provision of the information required in the context of stopovers, in particular by ensuring that the same data sets can be communicated in the same way to each NSW. It is also intended to facilitate the transmission of information between registrants, competent authorities and port service providers in the port of call and the Member States.

All Member States will therefore have to implement simplified, digitized and harmonized declarative procedures that will feed into one European Maritime Single Window (EMSWe) constituted by all NSWs. The idea of purely and simply replacing the national single windows in each Member State with a single, fully centralized and Europe-managed European window has not been retained, as Member States want to retain control of their national single window. However, several Member States may jointly set up a shared single window.

In each Member State operators will have a single point of entry for declarative information. The recipients of this information will be the administrations concerned (ports, customs, other national one-stop shops via the SafeSeaNet System). Each NSW will have to allow the declarant to share certain information with other predefined providers at national level (pilots, tugs, terminal operators, mooring boats, bunkers, passenger services, waste collectors).
For ports that are equipped with a Port Community System (PCS), such as for example the S) ONE platform at the ports of Le Havre and Rouen, the Regulation provides for the possibility of declarative obligations via this port, provided that that this approach remains voluntary and not imposed.
With regard to the information that must be transmitted for safety and security purposes by the shipping carrier to the customs authorities in the context of the electronic entry summary declaration (ENS), Regulation (EU) No 952/2013), they will continue to use a particular channel in view of their sensitive nature. However, and to the extent that this information will be required for other reporting requirements, EMSWe and NSWs will need to be able to access it.
Information, other than customs, provided by the ship when departing from an EU port shall not be required again on arrival at another port of the Union, except where the ship has stopped in the port of a third State during the voyage.

For all NSWs, harmonization will be carried out at Union level: harmonization of interfaces, harmonization of data formats, and harmonization of information to be inserted in application of international, European and national regulations.

In order to improve interoperability, multimodality and the proper integration of maritime transport into the freight and passenger transport supply chain, NSWs should provide for the possibility of exchanging useful information (such as ETAs and ETDs). ships) with similar structures put in place for other modes of transport.

The Commission will also create a number of common databases:

- a ship database (EMSWe Ship Database) which should include a reference list presenting the characteristics of the vessels and their declaration exemptions, as communicated to the different national one-stop-shops;
- To facilitate the provision of information by registrants, a Common Location Database will include a reference list of location codes, including the United Nations Code for Places Used for Trade and Transport. (UN / LOCODE), the specific SafeSeaNet codes and port facility codes listed in the International Maritime Organization's (IMO) Global Integrated Marine Information System (GISIS);
- a Hazmat (Common Hazmat Database) common database will include a list of dangerous and polluting goods to be notified to the NSW in accordance with Directive 2002/59 / EC and IMO FAL No. 7, taking into account relevant data from IMO conventions and codes;
- A common database on the hygiene and safety of vessels, which will be able to receive and store data on maritime health declarations under Article 37 of the International Health Regulations (IHR) 2005.

1.2.1.2. France

● *Ordinance No. 2013-139 of 13 February 2013 on declaratory formalities applicable to ships entering and leaving seaports*
● *Article L5334-6-2 of the Transport Code*

In application of the directive, France has set up the “guichet unique maritime et portuaire”, maritime and port single window (GUMP). It is an information system for the capture and transmission of dematerialized data provided by registrants in port information systems to the information systems of French and European administrations.

The GUMP thus ensures the transmission of data electronically, in a structured format, usable for computer processing. The transmission of the declarative formalities in electronic form in the port information systems must be ensured by the declarant (article L.5334-6-2 of the transport code).
From an operational point of view, the transmission in electronic format of the declarative formalities must be able to be done in two ways:

- Data entry via input screens dedicated to the different forms in the port information systems. When declaratory formalities are required from reporters, entry screens are proposed in all port information systems. It is possible for port information systems to provide entry screens for declarative formalities that are not required by the Ministry in the GUMP. In this case, the registrants are free to use all or part of the screens available in the port's IS, subject to compliance with reporting requirements. The corresponding file formats as well as the operation mode can be downloaded via the links below.
- The import of files manually filled by the declarants or generated and automatically transmitted by the shipowners' information systems to the port information systems.

1.2.1.3. Germany

● *Gesetzes über das Verfahren für die elektronische Abgabe von Meldungen für Schiffe im Seeverkehr über das Zentrale Meldeportal des Bundes, zur Änderung des IGV-Durchführungsgesetzes und des Seeaufgabengesetzes vom 30. Juni 2017*

The "National Single Window"passes this data to the competent authorities for the respective port visit or for the transit of a vessel through the Kiel Canal[12] .

Required notifications according to respective federal or federal state laws or regulations could be delivered directly and legally binding to the respective responsible authorities either via the web-based reporting client of the "National Single Window" or via reporting interfaces (port community information systems) of the "National Single Window", announced in the "Verkehrsblatt" (transport gazette) of the federal government.

1.2.1.4. Belgium [13]

● *Royal Decree on Maritime Security - April 21, 2007*

1.2.1.5. Netherlands

● *Decree of 4 May 2012, laying down rules for shipping on reporting formalities and on the processing of data received by organizations and persons not participating in shipping (Decree on reporting formalities and data processing for shipping) (Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart)*

1.2.1.6. United Kingdom

● *The Merchant Shipping (Port State Control) Regulations 2011*

● *The Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements)(Amendment) Regulations 2011*

● *Gibraltar Merchant Shipping (Reporting Formalities for Ships) Regulations 2012*

● *Merchant Shipping Notice - Vessel Traffic Monitoring Notification and Reporting Requirements for Ships and Ports*

The UK's National Maritime Single Window (NMSW) implements EU Directive 2010/65/EU. The aim of the NMSW is to simplify and digitise the process of handling legally required pre-arrival/departure paperwork, where necessary, so that data can be submitted simply and quickly via one online portal, alongside existing portals, in an electronic format, and meeting the Directive's requirements.

[12] https://www.national-single-window.de/info/doc/broschuere_b2mos_2015_en.pdf

[13] http://mswbelgium.be/wp-content/uploads/2015/05/technische-brochure.pdf

1.2.2. Customs

1.2.2.1. European Union

● *Regulation (EU) n°952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code*

● *Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code*

● *Commission Delegated Regulation (EU) 2016/341 of 17 December 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards transitional rules for certain provisions of the Union Customs Code where the relevant electronic systems are not yet operational and amending Delegated Regulation (EU) 2015/2446*

● *Commission Implementing Regulation (EU) 2018/1602 of 11 October 2018 amending Annex I to Council Regulation (EEC) No 2658/87 on the tariff and statistical nomenclature and on the Common Customs Tariff*

● *Regulation (EU) 2019/632 of the European Parliament and of the Council of 17 April 2019 amending Regulation (EU) No 952/2013 to prolong the transitional use of means other than the electronic data-processing techniques provided for in the Union Customs Code*

The UCC legal package entered into force on 1 May 2016, repealing and replacing the previous framework for customs legislation, contained in the Community Customs Code (Council Regulation (EEC) No 2913/92) and the Code's implementing provisions (Commission Regulation (EEC) No 2454/93) and recasting the Modernised Customs Code (Regulation (EC) No 450/2008) so as to align EU customs legislation with the requirements of the Lisbon Treaty.
Its aim is to:

- Offer greater legal certainty and uniformity to businesses and increase clarity for customs officials throughout the EU
- Complete the shift to a paperless and fully electronic customs environment
- Reinforce swifter customs procedures for compliant and trustworthy economic operators (AEO)
- Enhance the competitiveness of European businesses and thereby advance the main goals of the EU strategy for growth and jobs.
- Protect the flow of goods transiting or moving in and out of the EU
- Safeguard the financial and economic interests of the EU and of the Member States, as well as the safety and security of EU citizens.
- While the substantive provisions of the UCC entered into force on 1 May 2016 a transition period is necessary before full implementation can be achieved. This is primarily due to the fact that there is a need to develop new IT systems or upgrade existing ones in order to fully implement the legal requirements.

The transition period was initially until 31 December 2020 at the latest, but it has be extended to 2025 for a small number of customs formalities managed by electronic systems that may not be fully completed until 2025[14] .

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

The purpose of Regulation N° 1100 / 2008 is to make traffic flow within the Union. States may carry out checks on the technical characteristics, authorizations and documents to which vehicles and vessels must comply. These controls cannot, however, be used as border checks but only as normal controls applied in a non-discriminatory manner throughout the territory of a Member State.

1.2.2.2. France

● *National Customs Code*

● *Tax Code*

In customs matters, there are two codes, the National Customs Code and the European Customs Code. However, the National Customs Code has been emptied of its substance, it is now a special code of civil and criminal procedure and a penal code, since the provisions relating to customs formalities, customs clearance are governed by the EU . The bulk of customs law is now regulated at European level.
Tax Code concerns the regulation of import VAT, taxes and goods exchange declarations for intra-Community trade.

1.2.2.3. Germany

● *The Law on the Customs Administration (ZollVerwaltungsGesetz, [BGBl I S. 2125, 1993 I S. 2493] of 21 December 1992), as amended by Article 10 of the Law of 23 June 2017 (BGBl I S. 1822[15])*
● *The Customs decree (ZollVerodnung) of 23 December 1993 adopted for its application*
● *The tax code (der Abgabenordnung enthalten).*

These rules apply only to the extent that the Union Customs Code or its implementing rules do not contain any provisions and / or refer to national legislation.

1.2.2.4. Belgium

● *General Law on Customs and Excise, July 18, 1977;*
● *An Act to amend the General Customs and Excise Act and to make various provisions, May 12, 2014.*

General Law on Customs and Excise of July 18, 1977 regulates customs debt, determination of rate or amount applicable, prohibited goods, penalties.

[14] Regulation (EU) 2019/632 of the European Parliament and of the Council of 17 April 2019 amending Regulation (EU) No 952/2013 to prolong the transitional use of means other than the electronic data-processing techniques provided for in the Union Customs Code
[15] https://www.gesetze-im-internet.de/zollvg/BJNR121250992.html

1.2.2.5. Netherlands

● *General Customs Act (« De Algemene douanewet ») ;*
● *General Customs Decree and the General Customs Regulations («Het Algemeen douanebesluit » et « Algemene douaneregeling »)*

The Adw contains provisions in the areas of customs formalities, administrative activities, supervisory powers, the manner of collection (invitation to tender), administrative fines and criminal law, as well as oppositions and appeals. The General Customs Decree and the General Customs Regulations are based on the Adw and contain additional provisions.

1.2.2.6. United Kingdom

● *Customs and Excise Management Act 1979* [16]
● *The Ship's Report, Importation and Exportation by Sea Regulations 1981* [17]
● *The Customs and Excise Duties (Personal Reliefs for Goods Permanently Imported) Order 1983.*[18]
● *The Customs and Excise Duties (Personal Reliefs for Goods Temporarily Imported) Order 1983*[19].
● *The Customs Duty (Personal Reliefs) (No. 1) Order 1975* [20]

[16] https://www.legislation.gov.uk/ukpga/1979/2/contents
[17] https://www.legislation.gov.uk/uksi/1981/1260/contents/made
[18] [18] Available only in its original format, we have not the modified version.
http://www.legislation.gov.uk/uksi/1992/3193/made
[19] https://www.legislation.gov.uk/uksi/1983/1829/made
[20] https://www.legislation.gov.uk/uksi/1975/1132/made

1.3. Carriage by Inland Waterway

1.1.1. International Level

• *The Budapest Convention on the Contract for the Carriage of Goods by Inland Waterway (CMNI) - Ratified by France, Germany, Belgium and the Netherlands*

The CMNI lays down the regime of the contract for the international carriage of goods by inland waterway. This convention entered into force on April 1, 2005. It is applied by all states covered by the ST4W project, except for the United Kingdom, which has no connected waterways with these other states. Apart from certain provisions relating to Carrier's liability which can't be set aside, parties may arrange differently their contractual relationship. Each State may decide to apply the CMNI to national contracts of inland waterway carriage (CMNI, art. 31). Only Dutch legislation allows the parties of a national transport contract to agree to apply the provisions of the CMNI to this contract.

1.3.2. European level

• *The Regulation (EC) n°1356/96 of 8 July 1996 on common rules applicable to the transport of goods or passengers by inland waterway between Member States with a view to establishing freedom to provide such transport services*

Under Regulation (EC) No 1356/96, any carrier of goods or persons by inland waterway is allowed to carry out transport operations without discrimination provided that he is established in a Member State to carry out international inland water transport, for which it uses inland navigation vessels registered in a Member State, or in the absence of registration, having a certificate of membership in the fleet of a Member State member.

• *The Directive 2008/68 / EC of the European Parliament and of the Council*

The transport of dangerous goods by inland navigation vessels presents a considerable risk of accident. Measures must therefore be taken to ensure that this transport takes place in the best safety conditions.
To this end, the Commission recommended in 1999 that ADN (the European Agreement on the Transport of Dangerous Goods by Inland Waterway) be reconciled on the basis of the ADNR applicable on the Rhine. Taking advantage of the merging of the specific directives "Dangerous substances for road transport and rail transport" and the introduction of safety advisers, the EU has introduced in the same text the provisions on the transport of dangerous goods. So today we have a single text with uniform rules for the transport of dangerous goods regardless of the ground mode used (road, rail or waterway).

• *Regulation (EU) 2018/974 of the European Parliament and of the Council of 4 July 2018 on statistics of goods transport by inland waterways*

1.3.3. France

● *Commercial Code: art. L.133-1 to L.133-9 : carrier liability regime*

The content of a transport contract is largely left to the initiative of the co-contracting parties. The Commercial Code lays down some basic principles applying to carriers, concerning

liability for loss and damage of goods (Article L 133-1), time limits for bringing actions in case of damage (Articles L 133-3 and L 133-6), the direct action for payment (Article L 132-8) and the consignment note (L 132-9). Other obligations to which the parties are subject are outside the law and may be set out in a written contract. In fact, and particularly in the field of road freight transport, the parties may not sign a written contract or the carrier may not draw up the general conditions of sale mentioned in Article L 441-6 of the Commercial Code.

● *"Contrats-types"*

In order to establish and secure the relationship between the carrier and his customer, Articles L.1432-4 and L.1432-12 of the Transport Code provide that the clauses of the "Contrat-type" (standard contract) governing carriage apply in the absence of any provisions contractual. The case law has specified that they also apply to substitute for an illegal clause.
There are 4 Contrats-types for Inland waterway transport: Voyage contract (single or multiple trips); volume contract; Time contract; Subcontracting. For pallets or containers carriage the two most used Contrats-types are the "Voyage contract" Contrat-type (code des transports, Annexe to art. D. 4451-4) and "Time contract" Contrat-type (code des transports, Annexe to art. D. 4451-2). The Contrats-types list the data that must be transferred between contracting parties. This data is slightly different depending on the type of Standard Contract.

● *Article R. 4461-2 of the Transport*

The article R. 4461-2 of the Transport Code authorizes the dematerialization of the Consignment note and the Declaration of loading (specifically French control document and intended for VNF) are authorized by the national legislation only if these documents can be presented at the request of the control Authorities.

• *Decree of 29 May 2009*[21]

France incorporated into its national law the Directive 2008/68 / EC by Decree of 29 May 2009, known as the "TMD Order" .

• *Regulation (EU) 2018/974 of the European Parliament and of the Council of 4 July 2018 on statistics of goods transport by inland waterways*

The Loading Declaration is a paper or electronic declaration which is intended to the establishment of river transport statistics in application of Regulation (EU) N° 2018/974 of 4 July 2018 on statistics of goods transport by inland waterways.

1.3.4. Germany

• *Gesetz betreffend die privatrechtlichen Verhältnisse der Binnenschiffahrt (« Binnenschiffahrtsgesetz » - BinSchG).*

This Law is concerning the Private Law Conditions of Inland Navigation ("Inland Waterways Act" - BinSchG). It has been amended in 1998 and reefers now to Handelsgesetzbuch.

● *Handelsgesetzbuch – HGB: Sec. 408 Subsection 3 of the German Commercial Code*

[21] Arr. May 29, 2009, NOR: DEVP0911622A: OJ, June 27

● *Verordnung über die innerstaatliche und grenzüberschreitende Beförderung gefährlicher Güter auf der Straße, mit Eisenbahnen und auf Binnengewässern (Gefahrgutverordnung Straße, Eisenbahn und Binnenschifffahrt - GGVSEB)*
The text transposes the ADN Agreement to national transport law.

● *Richtlinien zur Durchführung der Gefahrgutverordnung Strasse, Eisenbahn und Binnenschiffahrt (RSES)*

This is a Guideline for the application of the Ordinance on the Transport of Dangerous Goods by Road, Rail and Inland Waterway.

1.3.5. Belgium

● *Law of May 5, 1936 on river chartering*

The Law of May 5, 1936 on river chartering is rather adapted to charter rather than transport contract. It isn't adapted to container's carriage but rather to bulk transport. It is currently subject to a broad reform of maritime and inland waterways navigation law (Transport Code project). Except articles 5 and 33, Law of May 5, 1936 is suppletive. So, Belgian operators may and do submit their transport contract (in their General Conditions of Transport) to other provisions like the CMNI or Professional Conditions of Carriage.
Wallonia has incorporated the Directive 2008/68 by Order of the Walloon Government of 2 February 2012 on the inland transport of dangerous goods by inland waterway.

1.3.6. Netherlands

● *Dutch Civil Code (Burgerlijk Wetboek)* [22]

Inland waterway transport, the stakeholders can choose to applied CMNI [23]. It's authorized by the Dutch Civil Code (art. 8.889).

● *Regeling vervoer over de binnenwateren van gevaarlijke stiffen*

Regeling vervoer over de binnenwateren van gevaarlijke stoffen transposed the Directive 2008/68.

1.3.7. United-Kingdom

[22] http://www.dutchcivillaw.com/legislation/dcctitle881313.htm

[23] Dutch Civil Code, art. 8.889: "Free choice for the application of the Budapest Convention (CMNI)): "*Parties may agree that, in derogation from Sections 8.10.1 and 8.10.2 as well as in derogation from Section 8.20.1, the provisions of the Budapest Convention on the Contract for the Carriage of Goods by Inland Waterway (CMNI) shall apply to the carriage*.

1.4. Carriage by road

1.4.1. International level

• *The Convention on the Contract for the International Carriage of Goods by Road (CMR) 19 May 1956*
• *Additional Protocol to the Convention on the Contract for the International Carriage of Goods by Road (CMR, Geneva 19 May 1956) concerning the E-Consignment note, Geneva 27 May 2008 (E-CMR Protocol)*

The CMR regulates the conditions of carriage and the responsibility of the different parties to the contract of carriage (Client, Loader, Carrier, and Consignee). This convention entered into force on July 2, 1961.The CMR Convention can certainly apply to a road and inland waterway transport, but on the condition that road transport is international.

1.4.2. European level

• *Dir 2010/40 / EU of the European Parliament and of the Council 7 July 2010: OJ No L 207, August 6*

In some Member States, national applications combining telecommunications, electronics and information technology have been developed in order to limit the increasing congestion of road infrastructures and the increase in energy consumption. Noting that these applications have multiplied without any coordination, the Union wished to define a uniform framework for Intelligent Transport Systems (ITS). This is the aim of the directive of 7 July 2010, which aims to ensure a coordinated and coherent deployment of ITS in the road sector (Dir 2010/40 / EU of the European Parliament and of the Council 7 July 2010: OJ No L 207, August 6). The objectives of this directive are to ensure the interoperability of the systems, which must be based on open and public standards and accessible to both suppliers and users, the provision of uninterrupted access, continuity of services and the provision of services in place of an effective cooperation mechanism.
Four Commission Delegated Regulations set out the technical implementation arrangements and specifications required to ensure interoperability and continuity of systems:

- the first concerns the European emergency call (e-Call) system (Commission Regulation (EU) No 305/2013 of 26 Nov. 2012: OJ No. L 91, 3 Apr. 2013);
- the second concerns traffic safety and lists the events justifying minimal information, such as slippery road, animal or obstacle on the roadway, work area, etc. (Commission Regulation (EU) No 886/2013 of 15 May 2013: OJ L 247, 18 Sep);
- the third applies to information concerning safe parking areas for heavy goods vehicles (Commission Regulation (EU) No 885/2013 of 15 May 2013: OJ L 247, 18 Sep.);
- the fourth sets out the specifications necessary for the accessibility, exchange, reuse and updating of traffic data for real-time information services (Regulation No. (EU) 2015 / 962 of the Commission 18 Dec. 2014: OJ No. L 157, 23 June).

1.4.3. France

France ratified the CMR on May 20th, 1959 and the E-CMR Protocol (in force since October 5, 2016).

• *Décret n° 2017-461 du 31 mars 2017*

In order to establish and secure the relationship between the carrier and his customer, Articles L.1432-4 and L.1432-12 of the Transport Code provide that the clauses of the "Contrat-type" (standard contract) governing carriage apply in the absence of any provisions contractual. The case law has specified that they also apply to substitute for an illegal clause.
There are 10 "Contrats-types" for road carriage adapted to a category of goods or a type of transport operation. The carriage of containers or pallets is generally governed by the "General" Contrat-type"[24].

• *Décret no 2015-474 du 27 avril 2015*

French law has been brought into line with the various texts concerning intelligent transport systems by a decree of 27 April 2015 and two decrees of the same day [25].

1.4.4. Germany

Germany has incorporated into its national law the Directive 2010/40 by the Law on Intelligent Transport Systems in Road Traffic and their Interfaces to other modes of transport (20/06/2013).
The State has joined in 2018 the Czech Republic, Greece, Romania and Serbia to test e-CMR in cross-border transport as part of a project funded by the European Commission. The pilot program is planned to finish in August 2019. However, only one German company is involved in this project[26] .

1.4.5. Belgium

● *Law of July 15, 2013 on the carriage of goods by road*

In accordance with the Law of July 15, 2013 on the carriage of goods by road (Article 29 § 1), Belgium applies the provisions of the CMR to its domestic transport.

● *Royal Decree of 10 April 2016 on the electronic consignment note*

Although Belgium is not a Party to E-CMR Protocol, the Royal Decree of 10 April 2016 on the electronic consignment note authorizes the use of the electronic consignment note on an experimental basis.

● *Ordinance of 28 March 2013 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and interfaces with other modes of transport.*

Belgium has incorporated into its national law the Directive 2010/40 by Ordinance of 28 March 2013 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and interfaces with other modes of transport.

● *Ministerial Decree of 23 May 2014 implementing the Royal Decree of 22 May 2014 on the carriage of goods by road (Mon. 15 July 2014)*

---

[24] Décret n° 2017-461 du 31 mars 2017 relatif à l'annexe II à la partie 3 réglementaire du code des transports concernant le contrat type applicable aux transports publics routiers de marchandises pour lesquels il n'existe pas de contrat type spécifique https://www.idit.fr/legislation/documents/Contrat_type_general_2017.pdf

[25] *D. n° 2015-474, 27 avr. 2015 : JO, 29 avr.* u *Arr. 27 avr. 2015, NOR : DEVT1506849A : JO, 29 avr.* u *Arr. 27 avr. 2015, NOR : DEVT1506850A : JO, 29 avr*

[26] https://trans.info/en/germany-is-not-likely-to-introduce-e-cmr-anytime-soon-102009

● *Royal Decree of 22 May 2014 relating to the carriage of goods by road (Mon. 15 July 2014)*
2.1.3.6. Netherlands

• *Dutch Supreme Court 5 January 2001, NJ 2001, 391*

It is allowed for parties to choose for the application of the CMR on contracts of carriage of goods by road without any international aspect, for instance between a Dutch consignor (sender) and a Dutch carrier in relation to the transport of goods between two places within the Netherlands. By making such choice, parties are able to set aside the Dutch Civil Code entirely, including all its mandatory and semi-mandatory provisions, like those to be found in Title 8.13.2. This can be done also by means of a general agreement regulating al possible future contracts of carriage of goods by road between the same parties, provided that that agreement meets the requirements of Article 8:1102, paragraph 1.

• *Wet van 21 mei 2012 tot wijziging van de Wegenverkeerswet 1994 in verband met de implementatie van richtlijn nr. 2010/40/EU van het Europees Parlement en de Raad van de Europese Unie van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen*

The Law of 21 May 2012 is amending the Road Traffic Act 1994 with regard to the implementation of Directive 2010/40 / EU of the European Parliament and the Council of the European Union of 7 July 2010 on the framework for the introduction of intelligent transport systems on in the field of road transport and for interfaces with other transport modes

1.4.7. United-Kingdom

United Kingdom intends to ratify the E-CMR Protocol. In July 2019, the secretary of state for foreign and commonwealth affairs presented parliament with its intention to accede to the e-CMR protocol[27].

National road carriage is governed by Professional Conditions of Carriage:Freight Transport Association (FTA) Model Conditions for the Carriage of Goods by Road in the United Kingdom[28] .

● *Intelligent Transport Systems Regulations 2012 of 19/07/2012*

[27] https://www.gov.uk/government/publications/additional-protocol-to-the-convention-on-the-contract-for-the-international-carriage-of-goods-by-road-cmr-concerning-the-electronic-consignment-note
[28] http://www.bridgetimegroup.com/conditions_of_carriage.pdf

PoA 2: Identify the various relationships between stakeholders and the data that are collected and exchanged between them

On the one hand, from the regulation identified in the Legal Framework section and, on the other hand, from the information contained in the reports of interviews, IDIT will identify the information that are exchanged between the different stakeholders (shipper, freight forwarder, carrier, terminal operator, consignee, authorities) who are involved in inland waterways operation, possibly completed by one or several road phases.

2.1 Identification of the possible transport scenarios that must be explored (current practices or what is contemplated in ST4W)

The aim is to define the scope of the analysis by specifying the "logistic" scenarios that will be considered by the project during the implementation of pilots.
In fact, the information that are issued and transferred during a transport, the way in which they are issued-transferred-used, as well as the issuers and consignees, depend on the way in which the transport is organized and the stakeholders who are involved in the organization of such transport.

For e.g.:

- Shipper (seller) → Inland Freight forwarder → Freight broker → Waterway carrier → Consignee

- Shipper (seller) → Consolidator → Maritime Freight forwarder (sea carrier organizing a door-to-door transport) → Inland Freight forwarder → Waterway Carrier → Road carrier → Consignee

Indeed, several questions arise: Who organizes the door-to-door transport? Who contracts with whom? Who subcontracts and to whom?

The information should be provided to IDIT throughout the project so that it can properly carry out its analysis and work on realistic and compliant scenarios with regard to current practices or envisaged by the ST4W project.
The information will mainly result from the reports of interviews conducted by our partners and the discussions we will have with them.

2.2 Identification of data collected and exchanged

The objective is to identify data that are collected, inserted in the various commercial / transport / customs documents or databases, or exchanged between operators (shipper, freight forwarder, carrier, terminal operator, consignee, authorities) according to the various regulations identified in PoA 1 (*creation of the Legal Framework of ST4W*), or in practice (information contained in the interviews).

NB: To complete this work, some relevant information has been collected during the interviews such as: what scenarios currently apply? How are transports organized? What are the relations between stakeholders? What information are collected and transmitted? Whose? What documents are issued?

This report gathers the data that are exchanged between operators (consignor, freight forwarder, carrier, terminal operator, consignee, authorities) and inserted in the various commercial

/ transport / customs documents or databases, according to the various regulations identified in PoA 1 (*creation of the Legal Framework of ST4W*).

2.3 Goods data in inland waterway transport (IWT)

2.3.1. Contract of carriage by inland waterways (private law)

- **Data required by transport law and professional conditions**

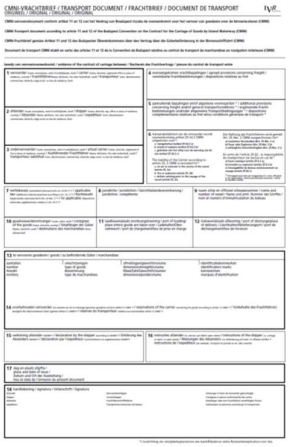
Are presented below:
- The Name and Form (paper / electronic) of the Document of carriage
- The Information / Data that must be provided by the Principal to the Carrier according to International and National Regulations, Professional General Conditions drafted by Carriers associations.

2.1.1.1 International carriage (CMNI)

International carriage contract by inland waterway carriage is ruled by the Budapest Convention on the Contract for the Carriage of Goods by Inland Waterway (CMNI). This convention entered into force on April 1, 2005. It is applied by all states covered by the ST4W project, except for the United Kingdom, which has no connected waterways with these other states.
Apart from certain provisions relating to Carrier's liability which can't be set aside, parties may arrange differently their contractual relationship.
Each State may decide to apply the CMNI to national contracts of inland waterway carriage (CMNI, art. 31).
Only Dutch legislation allows the parties of a national transport contract to agree to apply the provisions of the CMNI to this contract.

- **Contract of carriage (name and form)**

Name:
- Consignment note



- And/or Bill of Lading (only on the consignor request) (art. 11-1). The BL is usually a paper-based document. It is composed of several originals and copies. The original copy of the BL is negotiable (≠ Consignment note) and the consignee must present it to the carrier in order to get the goods (art. 13) or to modify the transport ("right of disposal", art. 14 & 15). So the BL

is usually in a paper form. In practice, the BL is used for an entire shipment of bulk cargo[29], not for containers.

Form : Paper or electronic document :
CMNI, art. 1.8 : "In writing" includes, unless otherwise agreed between the parties concerned, the transmission of information by electronic, optical or similar means of communication, including, but not limited to, telegram, facsimile, telex, electronic mail or electronic data interchange (EDI), provided the information is accessible so as to be usable for subsequent reference."
CMNI, art. 11 : "The original of the transport document must be signed by the carrier, the master of the vessel or a person authorized by the carrier. The carrier may require the shipper to countersign the original or a copy. The signature may be in handwriting, printed in facsimile, perforated, stamped, in symbols or made by any other mechanical or electronic means, if this is not prohibited by the law of the State where the transport document was issued."

- **Data to be furnished by the Principal before handing over the goods**

  - Dimensions, number or weight and stowage factor ("coefficient d'arrimage") of the goods (art. 6-2-a)
  - Identification marks of the goods (art. 6-2-b) that is: Number of the container, number / marks of the packages or other units in it. Insufficiency or inadequacy of marks identifying the goods is a ground for exempting the carrier from liability (art. 18-1-f). Furthermore, it is important to mention the number of units put in the container in order to get a higher compensation in the event of losses or damage of goods (art. 20-2)
  - Instructions concerning the Customs or administrative regulations applying to the goods (art. 6-2-d)
  - Nature, characteristics and properties of the goods (art. 6-2-c)
  - Other necessary particulars which must be mentioned in the Transport document (art. 6-2-e)

- **Data to be incorporated in the Transport document**

  - Name, domicile, registered office or place of residence of the carrier and of the consignor (art. 11-5-a)
  - Consignee of the goods (art. 11-5-b)
  - Name or number of the vessel, where the goods have been taken on board, or particulars in the transport document stating that the goods have been taken over by the carrier but not yet loaded on the vessel (art. 11-5-c)
  - Port of loading or the place where the goods were taken over (art. 11-5-d)
  - Port of discharge or the place of delivery (art. 11-5-d)
  - Usual name of the type of goods and their method of packaging (art. 11-5-e)
  - For dangerous or polluting goods : their name according to the requirements in force or, if there is no such name, their general name (art. 11-5-e)
  - Dimensions, number, weigh of goods (art. 11-5-f)
  - Identification marks of goods (art. 11-5-f)
  - If goods shall or may be carried on deck or on board (art. 11-5-g)
  - Agreed provisions concerning freight (art. 11-5-h) : freight prepaid, freight to collect on delivery

[29] See for ex. CG SOMEX S.A., art. 4.20, al. 3 : « *Sauf convention contraire, l'établissement d'un connaissement ne vaut que pour un lieu de chargement et un lieu de déchargement avec le transport du tout.* »

- In the case of a consignment note : the specification as to whether it is an original or a copy (art. 11-5-i)
- In the case of a Bill of Lading : the number of originals (art. 11-5-i)
- The place and date of issue (art. 11-5-j)
- Declaration of value (art. 20-4)
- Delivery time (art. 5)

- **Data to be added in the Transport document (or transmitted by other electronic means) at taking over or delivery**

- Carrier's reservations (art. 12-1) concerning :
    - Dimensions, number or weight of the goods
    - Identification marks
    - The apparent condition of the goods
- Consignee reservation in case of apparent (at the time of delivery) or non-apparent (within 7 consecutive days following delivery of goods) loss or damage (art. 23-3 & 23-4)

***General Remarks*:**
According to the interview reports, pallets are sometimes identified with a tracking number (EAN13 bar code[30])

[30] Roosens Beton interview report_2018_09_05

2.1.1.2 Inland Carriage

2.1.1.2.1 France

National carriage by inland waterways is governed by :

- Transport Code
- Commerce Code: art. L.133-1 to L.133-9
- Contrats-types: Article L.133-1 of the Commerce Code rules the provisions of the contract of carriage are, in absence of any provisions between the parties, ruled by the *Contrats-types*. These are contractual provisions set out by decree and applying to contract of carriage without any stipulations of the parties. Contrats-types are suppletive law (i.e. their provisions are compulsory unless parties have agreed otherwise). There are 4 Contrats-types for IWT :

    - Voyage contract (single or multiple trips)
    - Volume contract
    - Time contract
    - Subcontracting

For pallets or containers carriage the two most used Contrats-types are the "Voyage contract" Contrat-type (code des transports, Annexe to art. D. 4451-4) and "Time contract" Contrat-type (code des transports, Annexe to art. D. 4451-2).
The Contrats-types list the data that must be transferred between contracting parties. This data is slightly different depending on the type of Standard Contract.
We must caution that French Contrats-types for IWT are quite outdated because they were based on previous Chartering Contracts, which are quite different in fact form Carriage Contracts. Some of this data transfer obligation is consequently not ever understandable.

- CMNI[31] if parties agree[32]
- General Conditions for Transport

➢ **Confirmation of the Transport Contract**

In the case of a Voyage Contract, the contract of carriage concluded between the parties is subject to an approved confirmation from the Carrier and the Principal (C. transp., art. L.4451-7).
The Principal shall, prior to the presentation of Vessel to the load, transmit to the latter, in writing or by any other electronic means of transmission and conservation of data, the necessary information for the performance of the contract.
The confirmation of the transport contract must be on board the river unit as well as in the company of the other party and be immediately presented to the inspection agents mentioned in article L. 4461-1, in writing or by any other electronic transmission and data retention means.

➢ **Contract of carriage (name and form)**

Name : Consignment note or Bill of Lading (*Lettre de voiture* ou *Connaissement*).

[31] Budapest Convention on the Contract for the Carriage of Goods by Inland Waterway (*see 1.1.1.1.*)
[32] See for example the « *Conditions d'expéditions d'expédition et de transport de CFNR TRANSPORT SAS* » (Groupe Rhenus Logistics) http://www.cfnr.com/wp-content/uploads/2018/01/conditions-generales-eng.pdf

Form : French regulations require the presence of Consignment Note or Bill of Lading on board the vessel (C. transp., art. A.4241-33-11°). They may be requested by the Authorities to check their conformity with the information on the declaration of loading[33] (C. transp., art. R.4461-2).
French Contrats-types) also require that the Consignment note or the Bill of lading accompanies the goods.

Computerized data recording systems are permitted only if the presentation of the consignment or the Bill of lading is possible at the very moment of the agents' request (C. transp., art.R4461-2)[34].
The Bill of Lading is a document worthy of title, "to order" or "to bearer". In that case, only the bearer of the original prints of the Bill of Lading will be authorized to withdraw the goods. This is the reason why the Bill of Lading is in a paper form. But we don't think BL are usually used in Containers/Pallets IWT.

- **Data to be transferred by the Principal to the Carrier**

- Name / address of the Consignor / Consignee
- Loading and unloading points or zones, including possible stopping places
- Loading and unloading installation's characteristics
- ETA date
- Expected date of arrival at destination, taking into account the laydays granted for loading ("délai de planche") and the regulatory journey time ("temps conventionel de parcours")
- Type of goods
- Weight (but the carrier will only be liable of the tonnage contradictory measured with the barge's deadweight scale, art. 3-2)
- Volume and/or dimensions
- Number of packages or load unit (ex: pallets, containers) but the carrier will only be liable of the number contradictory counted, art. 3-2
- Dangerous character of the goods and precautions to take for transport
- Waste ("freinte")
- Freight cost and freight debtor
- Declaration of value
- Declaration of interest in delivery

- **Data to be incorporated in the Transport Document**

The Transport Document contains the main Data above-mentioned, and :
- Dates and hours of boat's arrival at destination
- Dates and hours of beginning and end of loading operations
- Dates and hours of beginning and end of the unloading operations
- Principal and Carrier's reservation at loading
- Consignee's discharge and reservation at unloading

[33] See 1.3.1.
[34] It should be noted that, more generally, according to article 1366 of the French Civil Code, an electronic document could not be refused by a court only because it is in electronic form. However, the law further specifies, the probative value of the document could be questioned if the identification of the persons referred in the document and / or the integrity of the documents could not be guaranteed.

2.3.1.2.1 Belgium

National carriage by inland waterways is governed by:

- Law of May 5, 1936 on river chartering. This law is deemed quite obsolete. It does not even deal with the consignment note. It is rather adapted to afreightment rather than transport contract. It isn't adapted to container's carriage but rather to bulk transport. It is currently subject to a broad reform of maritime and inland waterways navigation law (Transport Code project).

Except articles 5 and 33, Law of May 5, 1936 is suppletive. So, Belgian operators may and do submit their transport contract (in their General Conditions of Transport) to other provisions like:

- CMNI[35]
- Professional Conditions of Carriage :
  - Ex: Centraal Bureau voor de Rijn- en Binnenvaart (CBRB) Conditions of Carriage[36]. These conditions have been developed by the Centraal Bureau voor de Rijn- en Binnenvaart (Netherlands). Belgian and Duch Carriers are referring to CBRB Conditions of Carriage in their General Conditions[37]

➢ **Contract of carriage (name and form)**

Name : Consignment note and/or Bill of lading (on Consignor's request)
Form : Paper (if Bill of Lading) or electronic document.
According to 1936 Law (art. 9), if a Bill of Lading (BL) is issued, it is completed by the Principal and signed by the Carrier. It is established in several original copies signed by the carrier and mentions the number of original copies. If a Bill of Lading is requested by the Consignor, it will be in a paper form. The Carrier shall receive one original copy.
In practice, the BL can be also issued by the Carrier on request of the Principal[38]. Some Carriers'GC (General Conditions) provide it will be issued according to CMNI provisions (CMNI, art. 11 and 13)[39].
The CBRB Conditions of Carriage are not quite clear concerning the form (paper or electronic) of the Document of carriage. They define the term "In writing" by "*In writing: in each manner in which data can be provided whereby the data is stored, can be verified and can serve as evidence*." (art. 2.9.) and they state that "*The document of carriage can be issued in every format*." (art. 4.1.). "*The carrier can demand that the consignor signs the original or a copy of the document of carriage*" (4.2.).
In our view, these provisions of the CBRB just require that the data is put in a secured format (paper or electronic format) that enables to reuse or produce the data (storage, proof). If an electronic Document of Carriage is used, the signature that can require the Carrier shall be in an electronic form.
What is the Belgian Carrier current practice? Paper or Electronic document of carriage?

➢ **Data to be transferred by the Principal to the Carrier**

CMNI ☞ *See 1.2.1.1.2.*

CBRB Conditions of Carriage :

- Address, telephone number and/or place for notification (CBRB, 3.6)

[35] Budapest Convention on the Contract for the Carriage of Goods by Inland Waterway. Ex : SOMEF S.A. http://www.somef.be/wp-content/uploads/2016/12/CONDITIONS-GENERALES-DE-VENTE-SOMEF.pdf
[36] https://www.cbrb.nl/index.php?option=com_content&view=article&id=360:documentaire-over-4-jaar-voortvarend-besparen-een-brandstofbesparend-initiatief-in-de-binnenvaart&catid=2:nieuws&Itemid=2
[37] Ex : VANUDEN Shipping Terms & Conditions, art. 2.2. d http://www.vanudenshipping.com/termsandconditions ; ANTWERP PORT SHUTTLE General Terms, http://www.apsantwerp.be/en/static_pages/terms_and_conditions ; HUTCHISON Ports Belgium, art. 2.3. http://www.europeangatewayservices.com/uploads/ENG_Purchase_conditions_TCT_Belgium.pdf
[38] See for ex. CG SOMEX S.A., art. 4.20
[39] See for ex. CG SOMEX S.A., art. 4.20

- Consignee's/Receiver name and exact place of delivery (SOMEF, 9.1; CBRB, 3.6), a safe loading and
- discharging place (CBRB, 9.1)
- Quality and weight of the loaded goods (CBRB, 3.12)
- Nature of the Goods, dimensions, number, weight, content, quality, value, identification marks and numbers, incompatibilities of the goods (SOMEF, 4.2 ; DE GRAVE – ANTVERPIA N.V. S.A.). Some Carriers require the seal number (HUTCHISON Ports Belgium, art. 6.3.)
- Required treatment of the goods, the danger that they might cause, the possibility that the goods could pollute or damage for instance, all relevant information with respect to a safe carriage (CBRB, 3.5.)
- In case the cargo in the container requires special care such as food, goods that demand special temperature, are dangerous or otherwise require a special treatment, the data with respect thereto must be notified to the carrier in writing at least 24 hours prior to loading (CBRB, 3.12.)
- Containers : Deviating dimensions in height, breadth, weight, model, form or otherwise and/or contain cargo which extends beyond the container(s) (CBRB, 3.11.)
- All information and instructions concerning the Customs or administrative regulations applying to the goods (CBRB, 3.5.)
- Request of the Principal for the issuance of a BL (GC)

➢ **Data to be incorporated in the Transport Document**

- 1936 Law, art. 9

- Name / address of the Consignor / Consignee
- Name of the Carrier
- Name of the Boat
- Loading and unloading points
- Freight to be paid by the Consignee
- Type and quantity of Goods
- Marks and numbers of packages
- Date of the bill of lading

- CMNI ☞ *See* 1.2.1.1.3.

2.3.1.2.3 NETHERLANDS

National carriage by inland waterways is governed by :

- Dutch Civil Code (Burgerlijk Wetboek)
- The CMNI if agreed by Parties ☞ (Dutch Civil Code, art. 8.889: "Free choice for the application of the Budapest Convention (CMNI)): "*Parties may agree that, in derogation from Sections 8.10.1 and 8.10.2 as well as in derogation from Section 8.20.1, the provisions of the Budapest Convention on the Contract for the Carriage of Goods by Inland Waterway (CMNI) shall apply to the carriage*."[40]
- Professional Conditions of Carriage

Ex :

[40] http://www.dutchcivillaw.com/civilcodebook088.htm

- **Centraal Bureau voor de Rijn- en Binnenvaart (CBRB)** Conditions of Carriage[41]
- **Affreightment Conditions 1991**[42]. These conditions law are deemed quite obsolete. The BV 2016 are intended to replace them.
- **IVTB / ICLT / CICT 2010**[43]
- Algemene voorwaarden inzake het met één reis vervoeren van goederen over binnenwateren ("**BV 2016**")[44] Stichting Vervoeradres (SVA)

- General Conditions of Transport[45]. Certain GC provide for the application of the CMNI[46] but other don't[47].

➢ **Contract of carriage (name and form)**

Name: Waybill or Consignment note and/or Bill of lading (on Consignor's request)
Form:

- Paper if Bill of lading[48]
- Electronic document, if :
  - CMNI is applicable in accordance with Parties agreement (Art. 8:889 of the Dutch Civil Code)
  - IVTB / ICLT / CICT 2010: "In writing" shall include, unless otherwise agreed upon by the parties concerned, the case that the information is contained in electronic, optical or similar media of communication, including, but not limited to telegram, telecopy, telex, electronic mail or electronic data interchange (EDI), provided that the information is available in a manner that it can be used for later reference (§1.8.)
  - "BV 2016" provide for the application of the CMNI to the Contract of Carriage between Dutch ports, but also in case of national transport within other states (whether or not party to the CMNI (BV 2016 art. 2.2 ; Toelichting op de Reisbevrachtingsvoorwaarden 2013, art. 2[49])

Currently, the CMNI consignment note is either in paper form or digitalized in PDF format, etc. There is no digital format yet like e-CMR[50]. Dutch Police requires, based on Regulation 11 (1960) that ships have paper documentation on board indicating what cargo is on board the ship[51] (manifest?)

➢ **Data to be transferred by the Principal to the Carrier**

[41] https://www.cbrb.nl/index.php?option=com_content&view=article&id=360:documentaire-over-4-jaar-voortvarend-besparen-een-brandstofbesparend-initiatief-in-de-binnenvaart&catid=2:nieuws&Itemid=2
[42] Affreightment Conditions 1991 filed with the registrars of the courts of Amsterdam and Rotterdam
[43] *Internationale Verlade- und Transportbedingungen* (IVTB) – *Internationale vervoervoorwaarden 2010- International Conditions of Loading and Transportation* (ICLT) - *Conditions internationales de chargement et de transport* (CICT). These professional conditions of carriage are drawn up by **VBW (Verein für europäische Binnenschifffahrt und Wasserstraßen, Duisburg, Germany) and IVR (Rotterdam, Netherlands)**. Ex : VAN UDEN Terms and conditions, art. 2.2.d.
[44] Conditions générales relatives au transport de marchandises par voies d'eau intérieures en un voyage « BV 2016 » [conditions d'affrètement 2016]
[45] Ex : CTU Intermodal Barge Conditions, M.J. VAN RIEL B.V. General Terms and Conditions, VITO (Vereniging van Nederlandse Inland Terminal Operators) - Intermodal barge conditions, General conditions of Neo Logistic Services B.V., VAN UDEN Terms and conditions
[46] CTU Intermodal Barge Conditions, art. 2, VITO-Intermodal barge conditions, art. 2
[47] M.J. VAN RIEL B.V. General Terms and Conditions, art. 5.4. : "*For transport on inland waterways: Title 10 of Book 8 of the Civil Code, supplemented by the Affreightment Conditions 1991*" ; General conditions of Neo Logistic Services B.V., art. 1.2. : "*to barging : the CBRB conditions of carriage, deposited by the CBRB (Centraal Bureau voor de Rijn- en Binnenvaart)*" ; VAN UDEN Terms and conditions, art. 2.2.d. : "*In case of national carriage by inland waterways, in addition to the mandatory provisions of Section 8.10.2 of the Dutch Civil Code, the International Conditions of Loading and Transportation (ICLT) 2010*"
[48] Dutch Civil Code, Article 8:920 Number of original prints of the bill of lading : *The negotiable original prints of the bill of lading, in which is stated how many of such original prints have been issued on the whole, apply all for one and one for all.*
[49] https://www.sva.nl/sites/bva_sva/files/downloads/2017-12/Engels%20BV%202016%20Toelichting%20final.pdf
[50] ECOSYRIS, *State of play and barriers to the use of electronic transport documents for freight transport - Options for EU level policy interventions : annexes*, 2018, p. 402
[51] Ibid, p. 402

- IVTB / ICLT / CICT 2010 :
    - Indications necessary for the transport
    - Designation of the goods, marks, number, quantity, weight and/or volume
    - Hazardous Goods : Danger class, nature of the risk and precautionary measures to be taken, written instructions according to the Decree ADNR
    - All characteristics of the freight relevant for the proper execution of the transport

Data to be incorporated in the Transport Document

- Dutch Civil Code (Article 8:915, §2):
    - the goods received for carriage
    - the place where the carrier has received the goods for carriage
    - the place to which the carrier shall transport the goods pursuant to his obligation to do so
    - the consignee
    - the freightage (transport fee)
    - all other information that the consignor and carrier jointly deem fit

- CMNI ☞ *See 1.2.1.1.3.*
- "BV 2016":
    - Address, contact and financial particulars of the Consignor / Carrier
    - Description of the Goods,
    - Associated NSTR goods number
    - Transport unit ('bulk', stating the bulk density, 'container', 'pallet', etc.)
    - Dangerous Goods : UN number, shipping name, classification code and packaging group
    - Special precautions with respect to the environment, the working conditions or the Ship if these are not included in government regulations
    - Agreed loading capacity to be provided by the Carrier
    - Name and ENI number of the Ship (if the Parties have agreed on the charter of a specific ship)
    - Agreed Loading and Discharging Place, Contact particulars
    - If a time has been agreed at which the Ship must be ready for loading at the Loading Site
    - If a time has been agreed at which the Ship must be ready for discharging at the Discharging Site

- IVTB / ICLT / CICT 2010 :
    - Dimension, number or weight of the goods. Reservation of the Carrier shall be include in the waybill (Consignement note or Bill of Lading)
    - Identification marks. Reservation of the Carrier shall be include in the waybill (Consignement note or Bill of Lading)

2.3.1.2.4 Germany

National carriage by inland waterways is governed by:

- Gesetz betreffend die privatrechtlichen Verhältnisse der Binnenschiffahrt[52] (« Binnenschiffahrtsgesetz » - BinSchG) : This law has been amended in 1998 and reefers now to Handelsgesetzbuch (4th book, §407 et seq.)
- Handelsgesetzbuch – HGB : Sec. 408 Subsection 3 of the German Commercial Code
- Professional Conditions of Carriage :
  - Ex : **IVTB / ICLT 2010**[53]

➢ **Contract of carriage (name and form)**

Name:
Consignement note (*Frachtbrief*) or Bill of Lading

Form:
- Paper if Bill of lading
- Electronic document if Consignment note :

- Handelsgesetzbuch, § 408 *Frachtbrief. Verordnungsermächtigung :*

The consignment note shall be drawn up in three original copies signed by the consignor. The sender may require the carrier to also sign the waybill. One copy is destined for the sender, one accompanies the goods, the consignor keeps the third.
The consignment note may be in electronic format if its authenticity and integrity are guaranted (§408 (3)[54]).

- IVTB / ICLT 2010 : "In writing" shall include, unless otherwise agreed upon by the parties concerned, the case that the information is contained in electronic, optical or similar media of communication, including, but not limited to telegram, telecopy, telex, electronic mail or electronic data interchange (EDI), provided that the information is available in a manner that it can be used for later reference (§1.8.)

➢ **Data to be transferred by the Principal to the Carrier**

- Handelsgesetzbuch, § 410 (§ 410 *Gefährliches Gut*)
  - The Sender has to inform the Carrier in time in writing form of the exact kind of the danger and, so far necessary, precautionary measures.

- IVTB / ICLT / CICT 2010 :
  - Dimension, number or weight of the goods. Reservation of the Carrier shall be include in the waybill (Consignement note or Bill of Lading)
  - Identification marks. Reservation of the Carrier shall be include in the waybill (Consignement note or Bill of Lading)

➢ **Data to be incorporated in the Transport Document**

[52] http://www.gesetze-im-internet.de/binschprg/BJNR003010895.html#BJNR003010895BJNG000401377
[53] See note 12. Ex : Haeger & Schmidt Logistics GC, Sect. 9 (1) ; VÄTH GC
[54] Dem Frachtbrief gleichgestellt ist eine elektronische Aufzeichnung, die dieselben Funktionen erfüllt wie der Frachtbrief, sofern sichergestellt ist, dass die Authentizität und die Integrität der Aufzeichnung gewahrt bleiben (elektronischer Frachtbrief).

- Handelsgesetzbuch, § 408 *Frachtbrief. Verordnungsermächtigung*

  - Name / address of the Principal
  - Name / address of the Consignor
  - Place and date of Loading / Place of Unloading
  - Name / address of the Consignee
  - Description of the Goods and the load unit, identification marks and numbers
  - weight, content
  - Dangerous Goods : UN number, special precautions
  - Instructions concerning the Customs or administrative regulations applying to the goods
  -

- GC :
  - Goods to be transported at specific temperatures: actual and set temperatures when taking over the load and when the load is transferred out of the sphere of responsibility of the Carrier (CONTARGO GC, art. 8.4.).
  - Seal number of the Container must be specified on the consignment note (Haeger & Schmidt Logistics GC, Sect. 4 (1)

2.3.1.2.5 United Kingdom

National carriage by inland waterways is governed by :

- Transport Act 1962, Sect. 43 ☞ *No relevant provision*
- Carriage of Freight Vessel Conditions 2003 published by British Waterways. Despite their name these conditions do not govern the terms of the contract between the Principal and the Carrier but instead set out the terms upon which any freight operator (Carrier) is permitted to use British Waterway's navigations for the carriage of goods.

Nota : There does not appear to be any regulation on the transport document in inland waterway[55].

- **Contract of carriage (name and form)**

We know from the interviews and also from the discussions in the workshop that in the UK that most transport documents are in paper form.

- **Data to be transferred by the Principal to the Carrier**

No Results Found

- **Data to be incorporated in the Transport Document**

No Results Found

2.3.2 Data Required By Carriers

In practice, for the Booking process, Carriers require Principal to provide much more information than required by Transport Law. This information can be found in the Carrier's Standard Operating Procedure ("SOP") and is suited to the type of operation (Import Booking, Export Booking, Port Transfer, Empty Repositioning …).

[55] Cf. ECOSYRIS, *State of play and barriers to the use of electronic transport documents for freight transport - Options for EU level policy interventions : annexes*, 2018

2.3.3 RIS DATA

Texts :

- *Directive 2005/44/EC of the European Parliament and of the Council of 7 September 2005 on harmonised river information services (RIS) on inland waterways in the Community*[56]

- *Commission Regulation (EU) No 164/2010 of 25 January 2010 on the technical specifications for electronic ship reporting in inland navigation referred to in Article 5 of Directive 2005/44/EC of the European Parliament and of the Council on harmonised river information services (RIS) on inland waterways in the Community*[57]

- *Commission Regulation (EC) No 415/2007 of 13 March 2007 concerning the technical specifications for vessel tracking and tracing systems referred to in Article 5 of Directive 2005/44/EC of the European Parliament and of the Council on harmonised river information services (RIS) on inland waterways in the Community*[58]

The European Commission launched, in 2015, the **Digital Inland Waterways Activity (DINA)** initiative with the objective to digitalise information flows on infrastructure, people, operations, fleet and cargo in the inland waterway transport sector and to allow seamless integration of IWT in multimodal transport chains by connecting this information with other transport modes. Currently several digital tools exist or are being developed to support these information flows, for information on inland waterways vessels and on personnel.

RIS (River Information Services) is used to electronically share the information on dangerous goods with authorities and parties involved in the chain. RIS regulation[59] requires the transfer to Authorities of certain information relating to Dangerous Goods (2.3.2.3. Voyage related ship information):

- Category of dangerous cargo
- Hazardous cargo classification

This information is broadcasted autonomously from ship or on request.

See here http://www.ris.eu/docs/File/340/commission_regulation_164_2010_en.pdf
http://www.ris.eu/expert_groups/eri
http://www.ris.eu/docs/File/429/leaferi2015_e.pdf

[56] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02005L0044-20090420&qid=1564733197676&from=FR
[57] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010R0164&qid=1564733319882&from=FR
[58] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02007R0415-20120817&qid=1564733373480&from=FR
[59] Commission Regulation (EC) No 415/2007 of 13 March 2007 concerning the technical specifications for vessel tracking and tracing systems referred to in Article 5 of Directive 2005/44/EC of the European Parliament and of the Council on harmonised river information services (RIS) on inland waterways in the Community

2.3.4 DANGEROUS GOODS (DG)

2.3.4.1 INTRA-COMMUNITY TRANSPORT

Intra-Community transport of dangerous goods by inland waterway is governed by **Directive 2008/68/EC on the inland transport of dangerous goods**. More generally, this Directive governs the transport of dangerous goods by road, rail and inland waterway between several Member States.
Directive 2008/68 / EC requires compliance with the Regulations annexed to the ADN, as applicable from 1 January 2019. This is the **European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (" ADN 2019 ")**[60] adopted under the auspices of the United Nations Economic Commission for Europe (UNECE) and the Central Commission for the Navigation of the Rhine (CCNR).
Only the United Kingdom is not party to the ADN 2019, which is logical since there is no river transport between this state and the other European states.
As regards the transport of dangerous goods on the Rhine, since 2011 ADN has replaced ADNR.

2.3.4.1.1 Dangerous Goods Transport Document[61] (ADN, art. 5.4.1 and 8.1.2)

A Transport Document for carriage of Dangerous Goods is required on board.
All the information which must appear on this document can be incorporated in the document which formalizes the waterway contract of carriage (Consignment note or Bill of Lading).
All documents shall be on board in a language the master is able to read and understand.
The use of electronic data processing (EDP) or electronic data interchange (EDI) techniques as an aid to or instead of paper documentation is permitted, provided that the procedures used for the capture, storage and processing of electronics data meet the legal requirements as regards the evidential value and availability of data during carriage in a manner at least equivalent to that of paper documentation (ADN, art. 5.4.0.2).
When the dangerous goods transport information is given to the carrier by EDP or EDI techniques, the consignor shall be able to give the information to the carrier as a paper document (ADN, art. 5.4.0.3).
This provision, which requires the shipper to be able to provide the carrier with the information in paper format, is likely to encourage shippers to do so from the outset.

- **Data to be incorporated in the Transport Document by the Principal**

For carriage in bulk or in packages (ADN, art 5.4.1.1.1.):
- UN number, preceded by the letters "UN" or substance identification number
- Proper shipping name
- Label model numbers

Ex: "UN 1098 ALLYL ALCOHOL, 6.1 (3), I" or "UN 1098, ALLYL ALCOHOL, 6.1, (3), GE I".
- If applicable, the packing group assigned to the material
- Number and description of packages
- Name and address of the consignor
- Name and address of the consignee(s)
- Statement regarding actions, if any, that is required to be taken by the carrier (ADN, article 5.4.1.2.5.2.):

o Supplementary requirements for loading, stowage, carriage, handling and unloading of the package, overpack or container;

[60] https://www.unece.org/trans/danger/publi/adn/adn2017/19files_e.html
[61] Also called « Dangerous Goods Certificate » (DGC)

o Restrictions on the mode of carriage or vehicle or wagon and any necessary routing instructions;
o Emergency arrangements appropriate to the consignment.
The statement shall be in the languages deemed necessary by the carrier or the authorities concerned.

Additional information or additional mentions is required depending on the types of dangerous goods and their class.
Eg: if the transport is part of a transport chain comprising a maritime, road, rail or air route, the mention "Transport according to 1.1.4.2.1." must appear.

- **Other Documents**

Container Packing Certificate (ADN, art. 5.4.2)
If the carriage of dangerous goods in a *container* precedes a voyage by sea, a container packing certificate conforming to section 5.4.2 of the IMDG Code shall be provided with the transport document.
The functions of the transport document required under 5.4.1 and of the container packing certificate may be incorporated into a single document.

2.3.4.2 INLAND TRANSPORT

➢ Application of Directive 2008/68 / EC and ADN
Inland transport of dangerous goods in EU states is also regulated by **Directive 2008/68/EC** on the inland transport of dangerous goods. This directive provides for the application to inland waterways of the provisions of the Regulations annexed to the ADN. Therefore, the laws of the EU Member States provide for the application of the ADN.
Pursuant to article 5.4.0.2.of ADN, the use of electronic data processing (TEI) or electronic data interchange (EDI) techniques must be accepted for inland transport. But, according to AND, when the dangerous goods transport information is given to the carrier by EDP or EDI techniques, the consignor must be able to give the information to the carrier as a paper document (AND, art. 5.4.0.3).
National texts supplement the provisions of ADN.

2.3.4.2.1 France

The application of the ADN Agreement to national transport is provided by:

- *Decree of May 29, 2009 "concerning the transport of dangerous goods by land routes" (called "Arrêté TMD")*[62]*,*

The decree of May 29, 2009, and in particular its Annex III, completes the provisions of ADN.
It applies to national or international transport of dangerous goods by road, rail and inland waterways carried out in France.
In particular, it provides that it is the responsibility of the remitter of the goods to ensure that the Dangerous Goods Transport Document appears in the ship's documents (Decree of May 29, 2009, Appendix III, 2.1.1). Whereas the Dangerous Goods Transport Document is not included in the list of documents to be on board (C. transp., Article A4241-33).

[62] Arrêté du 29 mai 2009 relatif aux transports de marchandises dangereuses par voies terrestres (dit « arrêté TMD »)
https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=776A3F64F8758283D6911F3AD1B7AD26.tplgfr31s_2?cidTexte=JORFTEXT000020796240&dateTexte=20190403

In accordance with Article 5.4.0.2 of the ADN, the transport document may be in digital form provided it is accessible to the control authorities.
Recall an ADN provision already reported (see 1.3.1): When the dangerous goods information is provided to the carrier using TEI or EDI techniques, the shipper must be able to provide this information to the carrier as a paper document (ADN 5.4.0.3.). This ADN provision is likely to encourage shippers to provide the data in paper format.

It must be concluded from these provisions that international and national regulations lack clarity and legal certainty as to the possibility of using EDI in the transport of Dangerous Goods by inland waterways.

2.3.4.2.2 Belgium

Some regional legislation specifies the provisions of the national legislation:

- *Wallonia : Order of the Walloon Government of 2 February 2012 on the inland transport of dangerous goods by inland waterway* [63]

This order requires the driver of a dry cargo vessel or of a tanker carrying dangerous goods to **notify the Authorities the following information** before the start of any journey when it begins in the Region Walloon:

A. General information
(a) Identification of the Vessel:
- name;
- official identification number;
- deadweight.
(b) Place of destination.
(c) Intended route - probable time of arrival at the place of destination and probable time of departure.
(d) Total number of people on board.
B. Cargo information
(a) The exact technical designation of the dangerous goods (according to the transport document):
- UN number assigned, preceded by the letters UN, or the identification number of the material,
- proper shipping name (column (2) of Table C of Chapter 3.2 of the Regulation),
- data in column (5) of Table C of Chapter 3.2 of the Regulation,
- if applicable, the packing group assigned to the material that may be preceded by the letters GE.
(b) Quantities of such goods and their location on board and, if carried in cargo transport units other than tanks, identification numbers thereof.
(c) Confirmation of the presence on board of an appropriate list, manifest or loading plan detailing the dangerous goods loaded on board the vessel and their location.
(d) Address at which detailed cargo information can be obtained.
The information may be given orally, by radiotelephone or by an automatic radiotelegraphy message service where appropriate, or in writing.

2.3.4.2.3 Netherlands

Regulation : *Regeling vervoer over de binnenwateren van gevaarlijke stiffen*[64]

According to ECORYS study (answers given by Stakeholders, p. 348), electronic versions of dangerous goods certificates are accepted by Dutch authorities. However, they are not often used.

[63] http://www.ejustice.just.fgov.be/cgi/article.pl
[64] https://wetten.overheid.nl/BWBR0010115/2019-07-01#Artikel5

According to these same answers, when tankers (transport de vracs liquides) carry goods, electronic documents are used. In container transport, paper documents are still used.

2.3.4.2.4 Germany

The application of the ADN Agreement to national transport is provided by:

- Verordnung über die innerstaatliche und grenzüberschreitende Beförderung gefährlicher Güter auf der Straße, mit Eisenbahnen und auf Binnengewässern (Gefahrgutverordnung Straße, Eisenbahn und Binnenschifffahrt - GGVSEB) [65]
- Richtlinien zur Durchführung der Gefahrgutverordnung Strasse, Eisenbahn und Binnenschiffahrt (RSES) (*Guidelines for the application of the Ordinance on the Transport of Dangerous Goods by Road, Rail and Inland Waterway*)

2.3.4.2.5 United Kingdom

The application of the ADN Agreement to national transport is provided by The Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009[66]

[65] http://www.gesetze-im-internet.de/ggvseb/
[66] http://www.legislation.gov.uk/uksi/2009/1348/made

2.3.5. Loading Declaration (REGULATION (EC) N° 1365/2006)

Regulation (EU) N° 2018/974 of the European Parliament and of the Council of 4 July 2018 on statistics of goods transport by inland waterways

Previous text: **Regulation (EC) n° 1365/2006** of the European Parliament and of the Council of 6 September 2006 on statistics of goods transport by inland waterways and repealing Council Directive 80/1119/EEC

According to this Regulation, the Member States must transmit to the Commission (Eurostat) data relating to inland waterway transport on their national territory. These data concern in particular the nature of the goods transported (see Appendix VI)

2.3.5.1 France

The Loading Declaration is a paper or electronic declaration which is intended to the establishment of river transport statistics in application of Regulation (EU) N° 2018/974. It is also used for the establishment of invoicing of Voies Navigables de France (VNF) tolls.
For each transport, the Carrier must establish and transmit a Loading Declaration to VNF (C. transp., art. L.4461-1, R.4461-1). It applies to all IWT of goods using the inland waterways managed by VNF.
A decree of 24 July 2018 specifies the provisions of the transport code relating to the declaration of loading that must be prepared and transmitted by any river carrier of goods to VNF (C. transp., art. R.4461-1).

It allows knowing the type and number of units of charge but not the nature of the goods (information not required except for bulk).
Contents of Declaration of Loading (Arr. 24 juillet 2018[67]) :

- surname and given name of the carrier natural person or the legal name of the carrier legal person;
- carrier's contact details: email and postal addresses, and telephone number;
- surname and first name of the declarant natural person or the legal name of the declarant legal person;
- declarant's contact details: e-mail and postal addresses, and telephone number;
- where applicable, the declarant's declaration that he is authorized by the carrier;
- declaration number provided by VNF;
- European Identification Number (ENI) or the registration number of the vessel;
- Name of the vessel, its flag and its deadweight;
- the signature of the declarant (or electronic certificate in the case of a dematerialized declaration) attesting the filing of the declaration and its contents;
- the date of departure from the loading dock or point of entry on the French network or territory;
- the end date of unloading or exit from the French network or territory;
- the order number of the transport;
- the description of the goods or the type of cargo unit transported (including rimmed or filmed pallets);
- the tonnage transported and / or the number of units of load;
- the loading dock or point of entry on the French network or territory;

[67] Order of 24 July 2018 relating to the declaration of loading on the inland waterways managed by Voies Navigables de France, adopted pursuant to Article R. 4461-1 of the Transport Code
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037270483&fastPos=1&fastReqId=1394568175&categorieLien=id&oldAction=rechTexte

- the unloading platform or exit point of the French network or territory;
- the name of the recipient (s) of the transport service (shipper (s));
- the route taken during the trip, specifying the locks crossed

The Declaration of Loading is updated when the load originally declared is changed during the trip.
It must be established prior to the trip, either by dematerialized way or by means of a paper form which will have to be endorsed at the passage of the first and last lock control.
On an experimental basis, from 1 January 2019 to 31 December 2020, the Declaration of Loading must be established in a dematerialized form for journeys made wholly or partly on part of the French waterways (Seine and Escaut routes). Throughout the duration of this experiment, a Declaration of Loading which is not made by dematerialized way will be assimilated to a lack of transmission.
The dematerialized declaration is made on the internet (via computer or smartphone) in the VELI tool launched by VNF in 2013. 55 to 60% of carriers are currently carrying out their online loading declaration. The dematerialization of the Loading Declaration of loading will soon become mandatory[68].

2.3.5.2 Belgium

Unlike French authorities, Belgian authorities do not use a specific declaration but use RIS data : The STA-messages, which are based on the xml-messages from the River Information Services (RIS) and completed with some specific statistical information[69].

[68] Projet de loi d'orientation des mobilités
[69] ERIVOY https://www.bics.nl/?q=fr/node/100000058

2.4 GOODS DATA IN ROAD TRANSPORT

2.4.1. CONTRACT OF CARRIAGE BY ROAD (PRIVATE LAW)

2.4.1.1 DATA REQUIRED BY TRANSPORT LAW AND PROFESSIONAL CONDITIONS

Are presented below:

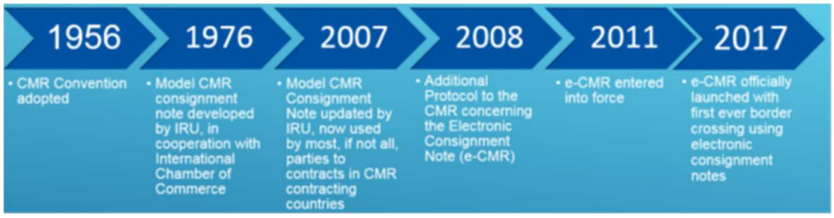
- The Name and Form (paper / electronic) of the Document of carriage
- The Information / Data that must be provided by the Principal to the Carrier according to International and National Regulations, Professional General Conditions drafted by Carriers associations.

2.4.1.2 INTERNATIONAL CARRIAGE (CMRI)

➢ International road carriage contract by road is ruled by the Convention on the Contract for the International Carriage of Goods by Road (CMR Convention, Geneva, 19 May 1956). This convention entered into force on July 2, 1961. It is applied by 55 states, especially by all states covered by the ST4W Project.

➢ The additional protocol to the CMR convention "concerning the electronic consignment note" ("E-CMR Protocol", February 20, 2008, in force since June 5, 2011) recognizes the legal value of the electronic consignment note :

""*Electronic consignment note" means a consignment note issued by electronic communication by the carrier, the sender or any other party interested in the performance of a contract of carriage to which the Convention applies, including particulars logically associated with the electronic communication by attachments or otherwise linked to the electronic communication contemporaneously with or subsequent to its issue, so as to become part of the electronic consignment note*" (E-CMR Protocol, art. 1).



An electronic consignment note that complies with the provisions of the E-CMR Protocol shall be considered to be equivalent to the consignment note referred to in the CMR Convention and shall therefore have the same evidentiary value and produce the same effects as that consignment note (E-CMR Protocol, art. 2.2).

E-CMR Protocol has been ratified by 20 States[70]. France (in force since October 5, 2016) and Netherlands (in force since January 7, 2009) are Parties to E-CMR Protocol. Belgium, Germany and the United Kingdom are not parties to the E-CMR Protocol.
The use of an E-Consignment note in an international transport crossing a State which is not Party to the E-CMR Protocol shall not affect the existence or the validity of the contract of carriage which shall remain subject to the provisions of the CMR Convention (CMR Convention, art. 4). But the E-Consignment won't be accepted by the supervisory authorities of the no Party State.

[70] Biélorussie, Bulgarie, Danemark, Espagne, Estonie, Finlande, France, Iran, Lettonie, Lituanie, Luxembourg, Moldavie, Pays-Bas, Pologne, République tchèque, Roumanie, Russie, Slovaquie, Slovénie, Suisse, Tadjikistan, Turquie.

Note that the use of an Electronic Consignment note has been authorized on an experimental basis during 3 years (2016-2019) for inland transport in Belgium, provided that it complies with the provisions of the E-CMR Protocol and provided that the supplier of the electronic consignment note has been approved by the Belgian Ministry of Transport (Royal Decree of 10 April 2016 on the electronic consignment note).
Since 2017, the Belgian experiment has been extended to the intra-BENELUX freight transport (Belgium, Netherlands, Luxembourg): an e-CMR provided by a certified IT provider in Luxembourg, the Netherlands or Belgium can be accepted by the authorities of each State. The experiment concerns both transport between the Benelux countries and national transport, including cabotage.
Therefore, the use of an electronic consignment note is possible for international and domestic transport in the BENELUX countries. However, this experiment is not valid in the case of an electronic consignment note issued in France and used in one of the BENELUX countries in the context of an international France-Belgium transport (for example) or within the framework of a cabotage transport in Belgium (for example).
Germany has joined in 2018 the Czech Republic, Greece, Romania and Serbia to test e-CMR in cross-border transport as part of a project funded by the European Commission. The pilot program is planned to finish in August 2019. However, only one German company is involved in this project[71].
United Kingdom intends to ratify the E-CMR Protocol. In July 2019, the secretary of state for foreign and commonwealth affairs presented parliament with its intention to accede to the e-CMR protocol[72].

- **Contract of carriage (name and form)**

Name: CMR Consignment note

Form : Paper or electronic document (in the case of an international transport between two States Parties to the E-CMR Protocol)

In case of paper consignment note, it shall be made out in three original copies signed by the sender and by the carrier. These signatures may be printed or replaced by the stamps of the sender and the carrier if the law of the country in which the consignment note has been made out so permits.
The first copy shall be handed to the sender.
The second copy shall accompany the goods.
The third copy shall be retained by the carrier (CMR Convention, art. 5).

In case of electronic consignment note, the electronic consignment note shall be authenticated by the parties to the contract of carriage by means of a reliable electronic signature that ensures its link with the electronic consignment note (E-CMR Protocol, art. 3.1).

[71] https://trans.info/en/germany-is-not-likely-to-introduce-e-cmr-anytime-soon-102009
[72] https://www.gov.uk/government/publications/additional-protocol-to-the-convention-on-the-contract-for-the-international-carriage-of-goods-by-road-cmr-concerning-the-electronic-consignment-note
https://www.lexology.com/library/detail.aspx?g=efb778f8-723d-4908-bade-98a4eb151bdc

The particulars contained in the electronic consignment must be accessible to any party entitled thereto (E-CMR Protocol, art. 3.3).
The procedure used to issue the electronic consignment note must ensure the integrity of the particulars contained therein from the time when it was first generated in its final form (E-CMR Protocol, art. 4.2).
The parties interested in the performance of the contract of carriage shall agree on the procedures and their implementation as regards:
(a) The method for the issuance and the delivery of the electronic consignment note to the entitled party;
(b) An assurance that the electronic consignment note retains its integrity;
(c) The manner in which the party entitled to the rights arising out of the electronic consignment note is able to demonstrate that entitlement (especially: right of disposal of the goods, CMR Convention, art. 12 and 13);
(d) The way in which confirmation is given that delivery to the consignee has been effected;
(e) The procedures for supplementing or amending the electronic consignment note; and
(f) The procedures for the possible replacement of the electronic consignment note by a consignment note issued by different means (E-CMR Protocol, art. 5.1).

- **Data to be furnished by the Principal before handing over the goods (CMR Conv., art. 7)**

- The name and address of the sender;
- The place and the date of taking over of the goods and the place designated for delivery;
- The name and address of the consignee;
- The description in common use of the nature of the goods and the method of packing, and, in the case of dangerous goods, their generally recognized description;
- The number of packages and their special marks and numbers;
- The gross weight of the goods or their quantity otherwise expressed;
- The requisite instructions for Customs and other formalities;
- A statement that trans-shipment is not allowed;
- The charges which the sender undertakes to pay;
- The amount of "cash on delivery" charges;
- A declaration of the value of the goods and the amount representing special interest in delivery;
- The sender's instructions to the carrier regarding insurance of the goods;
- The agreed time limit within which the carriage is to be carried out;
- A list of the documents handed to the carrier.

Other data :

- Mention providing that the Consignee shall have the right of disposal from the time when the consignment note is drawn up (CMR Conv., art.12, §3)

- **Data to be incorporated in the Transport document (CMR Conv., art. 6)**

- The date of the consignment note and the place at which it is made out;
- The name and address of the sender;
- The name and address of the carrier;
- The place and the date of taking over of the goods and the place designated for delivery;
- The name and address of the consignee;

- The description in common use of the nature of the goods and the method of packing, and, in the case of dangerous goods, their generally recognized description and if necessary, precautions to be taken (CMR Convention, art. 6 and 22);
- The number of packages and their special marks and numbers;
- The gross weight of the goods or their quantity otherwise expressed;
- Charges relating to the carriage (carriage charges, supplementary charges, customs duties and other charges incurred from the making of the contract to the time of delivery);
- The requisite instructions for Customs and other formalities;
- A statement that the carriage is subject, notwithstanding any clause to the contrary, to the provisions of this Convention.

Where applicable, the consignment note shall also contain the following particulars:

- A statement that trans-shipment is not allowed;
- The charges which the sender undertakes to pay;
- The amount of "cash on delivery" charges;
- A declaration of the value of the goods and the amount representing special interest in delivery CMR Convention, art. 6, 24 and 26);
- The sender's instructions to the carrier regarding insurance of the goods;
- The agreed time limit within which the carriage is to be carried out;
- A list of the documents handed to the carrier.

➢ **Data to be added in the Transport document**

- Carrier's reservations (CMR Conv., art. 8) concerning :
  - The accuracy of the statements in the consignment note as to the number of packages and their marks and numbers
  - The apparent condition of the goods and their packaging
  - The fact that the Carrier has no reasonable means of checking the accuracy of the statements in the consignment note as to the number of packages and their marks and numbers
  - Consignee reservation in case of apparent (at the time of delivery) or non-apparent (within 7 consecutive days following delivery of goods) loss or damage (CMR Conv., art. 30.1)

2.4.1.3 INLAND CARRIAGE

2.4.1.3.1 FRANCE

National road carriage is governed by:

- Transport Code
- Commerce Code : art. L.133-1 to L.133-9
- Contrats-types : Article L.133-1 of the Commerce Code rules the provisions of the contract of carriage are, in absence of any provisions between the parties, ruled by the *Contrats-types*. These are contractual provisions set out by decree and applying to contract of carriage without any stipulations of the parties. Contrats types are suppletive law (i.e. their provisions are compulsory unless parties have agreed otherwise). There are 10 Contrats-types for road carriage adapted to a category of goods or a type of transport operation. The carriage of containers or pallets is generally governed by the "Genera" Contrat-type"[73]

Standard Contracts list the data that must be transferred between contracting parties. This data is slightly different depending on the type of Standard Contract.

- CMR Convention if parties agree[74]
- Professional Conditions of Carriage :
  - FNTR

➢ **Contract of carriage (name and form)**

Text :

- *General contrat-type (art. 3.4)*
- *Arrêté of 9 November 1999 on transport or rental documents to be carried on board of goods road transport vehicles (art. 4).*

Name : Consignment note (*Lettre de voiture*).

Form :

- Either paper consignment note, at least one copy must be on board the vehicle;
- Either electronic consignment note, as long as it can be transmitted or communicated, each document being constituted solely by an electronic medium on board the vehicle, including smart phone, tablet or computer (Arr. 9 Nov. 1999). Article 3.4. of the General contrat-type provides that the transport document is drawn up, in writing or on any dematerialized medium.

During an inspection on the road or at a place of loading or unloading, the electronic consignment note and the summary statement must be able to be transmitted immediately to the control agent by any electronic means of transmission and preservation of the data.

➢ **Data to be transferred by the Principal to the Carrier**

Text : "General Contrat-type"

[73] Décret n° 2017-461 du 31 mars 2017 relatif à l'annexe II à la partie 3 réglementaire du code des transports concernant le contrat type applicable aux transports publics routiers de marchandises pour lesquels il n'existe pas de contrat type spécifique https://www.idit.fr/legislation/documents/Contrat_type_general_2017.pdf

[74] Cour de cassation, chambre commerciale, 1er juillet 1997, n° 95-12221

https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007037429&fastReqId=2136481825&fastPos=2

- full names and addresses, as well as telephone and fax numbers, the e-mail address of the sender and the recipient;
- full names and addresses, as well as telephone and fax numbers, the e-mail address of the loading and unloading places, where the latter differ from those indicated above;
- the name and address of the client;
- the dates and, if necessary, the loading and unloading times;
- the time limit for making the vehicle available for loading and unloading;
- the very exact nature of the goods, the gross weight of the shipment, the marks, the number of packages, objects or load carriers (pallets, rolls, etc.) that make up the shipment;
- where appropriate, the dimensions of packages, objects or load supports having special characteristics;
- if applicable, the linear footage of the floor or the necessary volume;
- the specificity of the goods when the latter requires provisions (dangerous goods, perishable goods, coveted goods

and / or sensitive etc.);

- the terms of payment (carriage paid or postage due);
- any other form of execution of the contract of carriage (delivery against reimbursement, disbursement, declaration of value, declaration of special interest on delivery, etc.);
- the number of the order and the references of the consignment, when this information is necessary for the proper performance of the contract;
- where applicable, the agreed ancillary services and their implementing rules;
- specific instructions in the event of impediment to delivery (new presentation, home delivery, warehousing, return, sale or destruction of the goods, etc.).

➢ **Data to be incorporated in the Transport document**

Text : *Arrêté of 9 November 1999 on transport or rental documents to be carried on board of goods road transport vehicles (art. 4).*

The consignment note must contain at least the following information:

- Date of establishment;
- Name, address and SIREN number or intra-Community identification number of the carrier;
- Date of taking over the goods;
- Nature and quantity, or weight, or volume of the goods for the grouped consignments, this information may be provided in a recapitulative statement;
- Name of the shipper or remitter;
- Complete address of the place of loading;
- Name of the recipient;
- Complete address of the place of unloading.

For cabotage operations, the consignment notes must also include:

- The registration number of the motor vehicle carrying out the transport;
- The date of unloading the goods.

For the operations of pre and post road transport combined transport, the company must submit any document to justify international and intermodal characters of the transport operation.

➢ **Data to be added in the Transport document**

Text : "General Contrat-type"

- Carrier's reservations

IDIT : **Governance-oriented analysis**

- Consignee reservation in case of apparent (at the time of delivery) or non-apparent (within 3 consecutive days following delivery of goods) loss or damage.
-

2.4.1.3.2 Belgium

National road carriage is governed by:

- Code de droit économique (Livre X, Titre IV « Contrat de transport », art. X.41 et s.)[75]
- Loi du 15 juillet 2013 relative au transport de marchandise par route (Mon. 18 févr. 2014)[76]

This law provides that the provisions of the CMR Convention are also applicable to the national carriage of goods by road (Article 51, §1)

- **Contract of carriage (name and form)**

Texts :

- Loi du 15 juillet 2013 relative au transport de marchandise par route (Mon. 18 févr. 2014)[77]
  - Arrêté royal du 10 avril 2016 relatif à la lettre de voiture électronique[78]
  - Arrêté ministériel du 23 mai 2014 pris en exécution de l'arrêté royal du 22 mai 2014 relatif au transport de marchandises par route (Mon. 15 juill. 2014)[79]
  - Arrêté royal du 22 mai 2014 relatif au transport de marchandises par route (Mon. 15 juill. 2014)[80]

Name : Consignment note (*Lettre de voiture*).

Form :

- Paper Consignment note : The law of 15 July 2013 provides that for all consignments a consignment note must be drawn up in accordance with the provisions of Articles 5 and 6 of the CMR Convention[81].

According to Ministerial Order of 23 May 2014 (art. 33, §1er), the first copy of the CMR consignment note is intended for the shipper, the second copy for the consignee and the third copy for the carrier. The second and third copies of the CMR consignment note must be on board the vehicle and accompany the goods; they must be presented at the request of the officers in charge of control (Law of 15 July 2013 33. § 4 ; Arrêté ministériel 23 mai 2014, art. 33. §1er).

- Electronic Consignment note : It has been authorized on an experimental basis during 3 years (2016-2019) for inland transport in Belgium, provided that it complies with the provisions of the E-CMR Protocol[82] and provided that the supplier of the electronic consignment note has been approved by the Belgian Ministry of Transport (Royal Decree of 10 April 2016 on the electronic consignment note).
-

Since 2017, the Belgian experiment has been extended to the intra-BENELUX freight transport (Belgium, Netherlands, Luxembourg)[83]: an e-CMR provided by a certified IT provider in Luxembourg, the Netherlands or Belgium can be accepted by the authorities of each State. All the data which must appear on the paper consignment notes in accordance with the requirements applicable in the BENELUX country where the electronic letter of car has been drawn up appear on the electronic

[75] Putzeys, Gehlen, Grigorieff, Rosseels, *Codes annotés – Droit des transports* (1er février 2019), p. 75 et s.
[76] https://www.code-de-la-route.be/textes-legaux/sections/lois/loi150713-tm/1903-loi-15-07-2013-tm#h4-titre-4-lettres-de-voiture
[77] https://www.code-de-la-route.be/textes-legaux/sections/lois/loi150713-tm/1903-loi-15-07-2013-tm#h4-titre-4-lettres-de-voiture
[78] https://www.code-de-la-route.be/textes-legaux/sections/ar/ar-100416/1924-ar100416
[79] https://www.code-de-la-route.be/textes-legaux/sections/am/am-230514-tm/1914-am-23-05-2014-tm
[80] https://www.code-de-la-route.be/textes-legaux/sections/ar/ar-220514-tm/1907-ar-22-05-2014-tm#h5-titre-5-lettres-de-voiture
[81] See 2.1.1.1.1. and following
[82] See 1.1.1. and following
[83] http://www.benelux.int/files/9315/0546/8122/M201712_FR.pdf

consignment note. The experiment concerns both transport between the Benelux countries and national transport, including cabotage.

- **Data to be furnished by the Principal before handing over the goods**

CMR Conv., art. 7 (see 2.1.1.1.2.)

- **Data to be incorporated in the Transport document**

CMR Conv., art. 6 (see 2.1.1.1.3.)

- **Data to be added in the Transport document**

See 2.1.1.1.4.

2.4.1.2.3. Netherlands

National road carriage is governed by:

- Burgerlijk Wetboek - Dutch Civil Code, Book 8 Transport law and means of transport, IV Road transport law, Title 8.13 Carriage by road[84]
- Dutch Supreme Court 5 January 2001, NJ 2001, 391: It is allowed for parties to choose for the application of the CMR on contracts of carriage of goods by road without any international aspect, for instance between a Dutch consignor (sender) and a Dutch carrier in relation to the transport of goods between two places within the Netherlands. By making such choice, parties are able to set aside the Dutch Civil Code entirely, including all its mandatory and semi-mandatory provisions, like those to be found in Title 8.13.2. This can be done also by means of a general agreement regulating al possible future contracts of carriage of goods by road between the same parties, provided that that agreement meets the requirements of Article 8:1102, paragraph 1.
- Professional Conditions of Carriage :
  - Stichting Vervoeradres General Transport Conditions (AVC2002)[85]

- **Contract of carriage (name and form)**

Name : Waybil l/Consignment note).

Form :
Paper Consignment note : Both, the consignor and the carrier, may draw up a document (waybill or consignment note) in regard of the transport of the relevant goods, and demand that this document or a possibly by the counterparty drafted document, is signed by their counterparty and handed over to them. The signature may be printed or replaced by a stamp or another feature of origin (Dutch Civil Code, art. 8:1119 Waybill / Consignment note).
Electronic Consignment note : While Dutch Civil Code does not expressly recognize the electronic consignment note, the Professional Conditions of Carriage commonly used (AVC2002) recognize the value of the electronic consignment note as well as any electronic communication :

- Definition of “Written” or ‘in writing: in writing or electronically (AVC2002, art. 1.8.)

[84] http://www.dutchcivillaw.com/legislation/dcctitle881313.htm
[85] https://www.sva.nl/sites/bva_sva/files/downloads/2018-02/6012%20General%20Conditions%20of%20Transport%20-%20A4%20web.pdf

- If data, including those relating to the consignment note, are exchanged electronically, parties shall not dispute the admissibility of electronic messages as evidence in the event of a mutual conflict (AVC2002, art. 2)
- Electronic messages have the same evidential value as written documents, unless these messages were not sent, saved and registered in the format as agreed on between the parties and in accordance with the security level and manner agreed on by parties (AVC2002, art. 2)
- A consignment note drawn up and signed electronically via the TransFollow platform has the same evidential value as the consignment note referred to in section 1. The electronic signature placed via the TransFollow platform is recognised as sufficiently reliable (AVC2002, art. 2)

But above all, since 2017, an e-CMR provided by a certified IT provider in Luxembourg, the Netherlands or Belgium can be accepted by the authorities of each State. The experiment concerns both transport between the Benelux countries and national transport, including cabotage[86].

- **Data to be added in the Transport document**

Text : Dutch Civil Code, art. 8:1119 "Waybill (consignment note)"
The paper or electronic waybill (consignment note) shall mention the following data:
a. the consignor, in which capacity only one person may be mentioned;
b. the goods received for transport;
c. the place where the carrier has received the goods for transport;
d. the place to which the carrier shall transport the goods pursuant to his obligation to do so;
e. the consignee, in which capacity only one person may be mentioned;
f. the carrier;
g. all other information that the consignor and carrier jointly deem fit.

2.4.1.2.4. Germany

National road carriage is governed by:

- Handelsgesetzbuch – HGB : Section §408(3) of the German Commercial Code[87]
- Professional Conditions of Carriage

- **Contract of carriage (name and form)**

Text : § 408 HGB (2) (3), Frachtbrief. Verordnungsermächtigung
Name : Frachtbrief
Form :
Either Paper Consignment note :
The Consignment note is issued in three original copies signed by the sender. The sender can require that also the carrier signs the Consignment note. Comply with reproductions of handwritten signatures by print or stamp. A copy is intended for the sender, one accompanied the goods, one keeps the carrier.
Either Electronic Consignment note :
An electronic Consignment note is an electronic record that has same functions such as the Consignment note provided that it is ensured that the authenticity and the integrity of the recording (electronic consignment note) are safeguarded.

[86] http://www.benelux.int/files/9315/0546/8122/M201712_FR.pdf
[87] https://www.global-regulation.com/translation/germany/387305/commercial-code.html

- **Data to be incorporated in the Transport document**

Text : § 408 HGB (1), Frachtbrief. Verordnungsermächtigung

1. place and date of issue;
2. name and address of the sender;
3. name and address of the carrier;
4. place and date of acquisition of the goods and the place designated for delivery;
5. name and address of the consignee and a possible sign-in address;
6. the usual name of the type of and the type of packaging for dangerous goods their intended according to the dangerous goods regulations, otherwise their generally recognized description;
7. number, marks and numbers of packages;
8. the gross weight or the different quantity of the goods;
9. the freight due for delivery and the costs incurred until delivery of the, as well as a note on the freight payment;
10. the amount of an on delivery cash on delivery of the goods;
11 instructions for customs and other official treatment of the material;
12. an agreement relating to the carriage on deck or in open, not with a tarpaulin covered vehicle.

In the Consignment note, other information can be entered, which the parties deem appropriate

2.4.1.2.5. United Kingdom

National road carriage is governed by:

- Professional Conditions of Carriage :
  - Freight Transport Association (FTA) Model Conditions for the Carriage of Goods by Road in the United Kingdom[88]

[88] http://www.bridgetimegroup.com/conditions_of_carriage.pdf

2.5. CUSTOMS DATA

Customs procedures and control methods are specified in the Union Customs Code (UCC) which entered into force on 1 May 2016. The UCC puts emphasis on fully electronic communication between the customs administrations and economic operators and between customs authorities in different Member States, in a paperless environment.

The Union Customs Code as laid down in the Regulation (EU) No 952/2013 allows using electronic transport documents or systems for some customs formalities (e.g. simplified transit), under the condition that certain data elements are contained, as specified in Annex B of the UCC Delegated and Implementing Act.

A Customs Data Model has been established in order to ensure the data harmonization for the exchange of information. This Data Model contains a data set encompassing data elements and definitions required by customs authorities throughout the EU.

Furthermore, DG TAXUD improved the existing national customs IT systems and adapted them to the new requirements set out by the new legislation. At the same time, a number of centralised EU-wide IT systems are being developed and deployed. The objective is to achieve a full digital environment and high level of harmonisation in the whole customs domain. Safety and Security information has been enhanced, mainly through the improvement of data quality, enlarging the reporting to multiple parties along the logistic chain. For this specific purpose, a new centralised system is being developed, gathering all safety and security information, including that coming from the maritime transport.

The Union Customs Code and the Implementing and Delegated Acts do not harmonise the way controls are carried out by customs. They cover exchange of information between authorities and between authorities and operators, but authorities of Members States are still free to require paper documents when controls are carried out.

POA 3 Analysis of Electronic Data Governance

An overview of the current outlook on information security and information sharing will be given. The first goal of this analysis is to provide an analysis of regulation, policies, case law and procedures for ensuring proper control of information security, record or document/information retention, data privacy. The second goal is to identify the legal or practical issues that could restrict the development of digitalization and data sharing in ST4W.

3.1. ELECTRONIC DATA REGULATIONS: LEGAL ENVIRONMENT OF ELECTRONIC DATA GOVERNANCE

The STW4 project aims to develop the deployment of an open source content management system based on a cloud that enables synchronization of data exchange between partners of supply chain and accessible by internal stakeholders from companies of the chain. In a cloud system or in any information system, the data is not fixed in a single and closed file but is available within a datacenter. It is necessary that such system can ensure security and traceability of those data. What types of data are affected by the project?

- Personal data
- Commercial data
- Goods data
- Vehicle data

The first part includes legislation and analysis as a whole with regard to the obligations and liabilities of transport stakeholders that they must comply with in terms of personal data and privacy, commercial data and trade secrets, electronic commerce, dematerialization of goods related transport documents, transport information systems and finally Cyber Security.

3.1.1. PERSONAL DATA AND PRIVACY

3.1.1.1. At International level

At international level, there is a **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28th of January 1981,** whose the purpose is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").
The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors. Moreover, appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination. It also provides additional safeguards for the data subject. This Convention has been ratified by Belgium, Germany, Netherlands, UK and France.

3.1.1.2. At European level

The **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector** (also known as “Directive on privacy and electronic communications”) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community. “Communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. “Location data” means any data processed in an electronic communications network,

indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (Article 2).
The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security.
Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time (Art. 9).

The **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).
This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. All relevant actors must ensure at all times compliance was applicable data protection rules and must be able to demonstrate compliance. It enshrines logic of accountability of all actors involved in the processing of personal data, as long as they concern European residents, whether or not these actors are established within the EU.

3.1.1.3. France

The **Law n°2018-493 on the protection of personal data** was promulgated on June 20, 2018 and published in the Official Journal on June 21, 2018. It is to adapt law to EU law following the GDPR. The New Data Protection Act replaces the a priori control mechanism – based on prior declarations and authorization by a posteriori control mechanism based on the data controller's assessment of risks related to data protection.

3.1.1.4. Germany

The Federal Data Protection Act (BDSG) of 30 June 2017 applies to the processing of personal data by public and private bodies which governs the exposure of personal data, which are manually processed or stored in IT systems.

3.1.1.5. Belgium

The **Law relating to the protection of individuals with regard to the processing of personal data** of 30 July 2018 (the Privacy Act) supplements or specifies some specific provisions of the GDPR. The law applies to any processing of personal data in the context of the activities of the establishment of a controller or a processor in Belgium, as well as to any processing of personal data of data subjects who are in Belgium by a controller or processor not established in Belgium where the processing activities are related to the offering of goods or services to data subjects in Belgium or to the monitoring of the behavior of data subjects in Belgium.

3.1.1.6. Netherlands

The **Dutch GDPR Implementation Act (AVG)** of 22 may 2018 contains rules on the implementation of the GDPR.

3.1.1.7. United Kingdom

The Data Protection Act 2018 achieved Royal Assent on 23 May 2018. It applies the EU's GDPR standards and makes provisions about the processing of personal data. It also implements the EU Law Enforcement Directive.

3.1.2. BUSINESS DATA AND TRADE SECRETS

3.1.2.1. At International level

In international law, trade secrets are protected by Article 39 of the **Agreement on Trade-Related Aspects of Intellectual Property Rights** (known as the TRIPS Agreement), annexed to the Agreement Establishing the World Trade Organization (WTO)), signed in Marrakech on April 15, 1994. This text defines trade secrets and requires States parties to protect it. The draft law meets an international obligation.

3.1.2.2. At European level

The **Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure** aims to standardize the national laws in EU countries against the unlawful acquisition, disclosure and use of trade secrets. The directive harmonizes the definition of trade secrets in accordance with existing internationally binding standards. A trade secret is a valuable piece of information for an enterprise that is treated as confidential and that gives that enterprise a competitive advantage. Innovative businesses are increasingly exposed to the unlawful misappropriation of their trade secrets (such as customer or supplier records, economic data, management methods, strategic plans, technical or technology know-how or, more generally, information or practices that are not protected by intellectual property rights).

3.1.2.3. France

The **Law n°2018-670 relating to the protection of trade secrets** implementing the Directive (UE) n°2016/943 of30 July 2018 transposes the directive 2016/943/UE. The L. 151-1 of the French Commercial Code defines trade secrets as information meeting all of the following three criteria: the information (i) is not generally known or readily accessible to persons familiar with this type of information because of their sector of activity; (ii) has real or potential commercial value; and (iii) has been subject to reasonable protection measures intended to preserve its secrecy.
Pursuant to the new §L. 151-4 of the French Commercial Code, a trade secret acquired without the consent of the trade secret holder is unlawfully acquired, whenever carried out by (i) unauthorized access to, appropriation of, or copying or, more generally (ii) any other conduct which, under the circumstances, is considered dishonest and contrary to commercial practices.
Conversely, the acquisition will be considered lawful when the trade secret is obtained as a result of independent discovery or creation, or of the observation, disassembly or testing of a product that has been made available to the public (L. 151-3).

3.1.2.4. Germany

IDIT : **Governance-oriented analysis**

The law transposing the Directive (UE) 2016/943 (« **Gesetz zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung** ») provides greater legal certainty when protecting business secrets. It implements a European directive (EU 2016/943), which guarantees uniform minimum protection for business secrets across Europe. This benefits companies that create economic value with ideas and innovations.

3.1.2.5. Belgium

This **belgium law transposing the directive concerning the protection of trade secrets from 30 july 2018** now expressly protects companies against the disclosure of these business secrets (by business partners, by former members of their staff, etc.) but also against their use by rapid and concrete means of action.
The use or disclosure of a business secret is considered illegal:

- If they breach a contractual obligation or a confidentiality agreement or if the business secret was acquired illegally.
- If, at the time of obtaining, using or disclosing the trade secret, a person knew or, having regard to the circumstances, should have known that the trade secret had been obtained directly or indirectly from another person who unlawfully used or disclosed it,
- More generally, if they result from unethical behaviors to “honest commercial practice”.

3.1.2.6. Netherlands

The Trade Secret Protection Act (Wet bescherming bedrijfsgeheimen) from the 17 October 2018 stipulates that the disclosure of a trade secret without the authorization of its holder is illegal in cases where:

- A person obtains, without authorization, access to confidential information;
- A person discloses confidential information;
- A person copies documents containing trade secrets, or from which confidential information can be deduced;

In addition, the disclosure to the public of a trade secret may be considered illegal if the information is disclosed without the consent of its holder.

3.1.2.7**. United Kingdom**

The Trade Secrets Regulations 2018 came into force on 9th June 2018. The acquisition, use or disclosure of a trade secret is unlawful where the acquisition, use or disclosure constitutes a breach of confidence in confidential information. Regulation 3 confirms that the existing UK law on confidential information will run in parallel with the rights conferred under the Directive. The remedies available at common law will therefore also be available to a trade secret holder who has brought proceedings under the Regulations.

3.1.3. ELECTRONIC COMMERCE: ELECTRONIC IDENTIFICATION AND TRUST SERVICES

3.1.3.1. At International level

The **UNCITRAL Model Law on Electronic Commerce 1996** purports to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce.

The **Model Law on Electronic Signatures 2001** aims to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. Pursuant to article 6§1, "where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement".

An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable (Art. 6§3).

The **UNCITRAL Model Law on Electronic Transferable Records 2017** aims to enable the legal use of electronic transferable records both domestically and across borders. The MLETR applies to electronic transferable records that are functionally equivalent to transferable documents or instruments.

3.1.3.2. At European level

The **Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014** on electronic identification and trust services for electronic transactions in the internal market (eIDAS) creates a new system for secure electronic interactions across the EU between businesses, citizens and public authorities. It aims to improve trust in EU-wide electronic transactions and to increase the effectiveness of public and private online services and e-commerce.

In accordance with article 3 of eIDAS regulation, "Electronic signature" means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

"Advanced electronic signature" means an electronic signature which meets the following requirements:

- It is uniquely linked to the signatory.
- It is capable of identifying the signatory.
- It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control.
- It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

"Qualified electronic signature" means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

The eIDAS regulation states that the simple signature, the advanced signature, and the qualified signature are all legally binding. The qualified signature will be recognized in all the states of the European Union, with independence from the state where it was issued.

"Trust service" means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services.

3.1.3.3. France

The Law n°2000-230 adapting the law of evidence to information technology and relating to electronic signature of 13 March 2000 recognizes the legal value of electronic documents and signature. It lays down the principle of equal probative evidence between an electronic-based writing and a paper-based writing. However, the law imposes two conditions for the electronic-based writing for it to have the same value as a paper-based writing: evidence of the writer's identity and evidence of the integrity of the message. Writing in electronic form is admissible as evidence in the same manner as a paper-based writing, provided that the person from whom it proceeds can be duly identified and that it has been established and stored in conditions calculated to secure its integrity.
Pursuant to Article 1367 of the Civil code (Decree n°2017-1416 on electronic signature – 28 September 2017), a signature which is required in order to perfect a juridical act identifies its own author. It demonstrates his consent to the obligations which stem from that act. Where it is placed on the act by a public official, it confers authenticity on it.

Where it is in electronic form, it must use a reliable process of identification which guarantees its relationship with the act to which it is attached. The reliability of the process is presumed in the absence of proof to the contrary where an electronic signature is created, the identity of the signatory is ensured and the integrity of the act is guaranteed on the conditions fixed by decree of the Conseil d'État.

3.1.3.4. Germany

The **German Digital Signature Act (SigG)** came into force on 22 May 2001. The application area of remote electronic signatures is limited because of its lack of legal recognition. In general, contracting parties can conclude a legally binding contract under German law through a mutual agreement that expresses the intention of both parties.
The German law requires a handwritten signature for certain declarations as formal requirement for a legally binding declaration to protect the contracting parties from imprudent decisions and to preserve evidence for court procedures. An electronic signature is accepted as legal equivalent to the written form if it is a qualified electronic signature according to the SigG. Whereas the SigG defines whether an electronic signature is qualified, it does not regulate the use of remote electronic signatures. It rather expects the signature creation device to be under control of the signatory.

Remote electronic signatures have not been accepted as equivalent to qualified electronic signatures yet. The eIDAS Regulation attributes the same legal binding effect to the remote electronic signature created by a qualified trusted provider as to a qualified electronic signature that has been created in the environment of the signatory. German law is not adjusted to the Regulation. As the eIDAS Regulation accepts the equivalence of qualified electronic signatures and remote electronic signatures the German courts need to accept their evidentiary value.

3.1.3.5. Belgium

The law of July 21, 2016, also called the Digital Act[89] came into force on September 28, 2016. Even if technically a European regulation does not require transposition into national law as is the

[89] JULY 21, 2016. - Law implementing and supplementing Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions within the internal market and repealing Directive 1999/93 / EC, inserting Title 2 in Book XII "Law of the electronic economy" of the Code of Economic Law and inserting definitions specific to Title 2 of Book XII and the implementing provisions of the law proper to title 2 of book XII, in books I, XV and XVII of the Code of

case for a directive, Chapter III of the regulation eIDAS relating to “trust services” requires legislative intervention at national level in order to ensure its implementation. Thus, the legislator precisely determines the sanctions applicable in the event of non-compliance with the provisions of the regulations and Belgian law relating to the aforementioned trust services. It also officially appoints the supervisory body and determines its powers:

- in the procedure for launching "qualified" trust services,
- in the control of the providers who offer them as well as during the transitional period allowing qualified providers under the reign of the 1999 directive to "regularize".

The Belgian legislator has also enshrined a complete and coherent body of rules aiming to provide a legal framework for the supply and use of electronic archiving services. When considering the conclusion, the transmission and the conservation of a legal act in an electronic process, it seems important to legally cover all the stages of the process, including the final stage which consists in the archiving of the act, and not only its signature, its dating and its sending. With the law of July 21, 2016, the Belgian legislator usefully and expediently frames the last link in the chain, which the European regulation has not done.

The Belgian rules are in line with the objectives and philosophy of the eIDAS regulation. They use the same principles as those decreed by these regulations for other trusted services (signature, stamp, time stamp, electronic registered mail). They aim to cover both the electronic filing of originally electronic documents and the electronic filing of paper documents (in the context of scanning).

Beyond the original regime relating to electronic archiving, Belgian law also devotes provisions relating to hybrid registered delivery, the revocation, suspension and expiration of qualified certificates of electronic signature and seal, to the party using a qualified electronic signature or a qualified electronic seal, at the end of the activities of a qualified trust service provider offering one or more qualified trust services and with the possibility of identifying a natural person who hides behind a pseudonym or electronic seal.

The envisaged provisions clearly aim to strike a balance between flexibility and security. Like the regime already applicable to other trust services under Regulation 910/2014, the legal framework relating to electronic archiving is envisaged as a “legal toolbox” allowing users to use this service in to manage their risks in relation mainly to data or documents of legal value. To this end, various presumptions are provided for in favor of electronic archiving services considered to be "qualified" within the meaning of the law as well as in favor of other qualified trust services within the meaning of the regulations.

3.1.3.6. Netherlands

The Netherlands has legally recognised e-signatures since 2003, since the Electronic Signatures Act. More recently, the introduction of eIDAS in July 2016 saw these regulations standardised across Europe.

Under Dutch law (Article 3:15a Dutch Civil Code) it highlights that contracts don’t need a handwritten signature to be seen as credible. They are seen as such as long as legally able individuals have reached an agreement (this can be by agreeing verbally, electronically or by physically signing).

Since July 2016, the eIDAS regulation has meant that all companies in the EU comply with each other’s e-Signature regulations Standardising them across Europe.

---

economic law. The legislator takes the opportunity to repeal the law of July 9, 2001 establishing certain rules relating to the legal framework for electronic signatures and certification services as well as the law of May 15, 2007 establishing a legal framework for certain trusted service providers.

A qualified electronic signature comes with a qualified certificate and is legally valid. Companies offering this must be listed as a Trusted Service Provider in the Netherlands[90] . According to **Article 25(2) and (3)**, a QES has the same legal effect as that of a handwritten signature.
However, according to **Article 25(1) of the eIDAS Regulation**, electronic signatures cannot be held inadmissible in court simply for failing to meet the guidelines of QES.
If a QES is legally recognized in one Member State of the EU it must be recognized in all Member States. Though Recital 49 allows national law to decide which type of electronic signature is required in any given circumstance.
A Decree of 22 February 2017,is laying down requirements regarding the provision of trust services, repealing the Electronic Signatures Decree .

3.1.3.7. United Kingdom

At first, e-Signatures in the UK were only regulated by the Electronic Communications Act 2000 (ECA 2000). However, on July 1, 2016, the electronic identification, authentication, and trust services regulation (eIDAS) came into force and complemented the aforementioned act. In lay terms, the eIDAS is a set of standards for electronic identification that is supported by the EU countries. And even though the UK is intended to leave the EU, there is no discussions about a repeal of the eIDAS regulation in the country.

Electronic Signatures in the United Kingdom have to meet one requirement: the process of e-Signing must indicate an **intention to authenticate**. There is no prescribed format for electronic signatures in the UK and, according to the eIDAS, it can generally be used in the following forms:

- Typewritten name
- Tick in a checkbox on a website or a simple button click (for instance, *I agree*)
- Scan of a handwritten signature
- Data in the electronic form with advanced level of security
- Digital signature that is created using Public Key Cryptography and Certificate Authority

The limitations to use, in turn, mostly concern documents that can't be signed electronically. In the UK such documents are deeds (for example, deeds for the Land Registry), which must be signed only by hand. This is because in some cases e-Signatures make documents impractical. For instance, when it would be harder to validate an e-Signature in comparison to a handwritten one, where you can appeal to a forensic handwriting expert.

3.1.4. CYBER SECURITY

3.1.4.1. At International level

The **Convention on Cybercrime of the Council of Europe** (Budapest Convention) of the 23th November 2001 is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Cybercrime designates all misuse of new technologies.

3.1.4.2. At European level

Directive NIS (Network and Information System Security) (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerns the implementation of measures intended to

[90] https://www.agentschaptelecom.nl/onderwerpen/elektronische-vertrouwensdiensten/trust-service-providers

ensure a high common level of security of networks and information systems within the European Union.

It identifies two typologies of industries subject to a set of obligations:

- Operators of Essential Services (OES) provide an essential service, the interruption of which would have a significant impact on the functioning of the economy or society. The NIS Directive affects the following sectors: Water; Energy; Digital infrastructure; Banking and financial market infrastructures; Health; and Transport.
- Digital Service Providers (DSP) - these are marketplaces, search engines and cloud service operators[91]. CSPs can be categorized according to the following organizations: Search engine ; Cloud IT services ; Online markets.

The NIS Directive requires OES and DSP to:

- Take the appropriate technical and organizational measures to secure their networks and information systems;
- Take into account the most recent developments and consider the potential risks with which their systems are confronted;
- Take appropriate measures to prevent security incidents or, at least, to minimize their impact in order to ensure continuity of service; and
- Notify the relevant competent authority of any security incident having a significant impact on the continuity of service without undue delay.
- Consequences of failure to comply with the NIS Directive

The Directive provides that DSP "remain free to take the technical and organizational measures they deem appropriate and proportionate to manage risks" as long as the measures provide "an appropriate level of security" and factor the requirements of the NIS Directive. The CSPs must ensure a level of security appropriate to the risk posed by the offer of the covered services, taking into account the following elements:

• Security sites and systems
• Incident management
• Business continuity management
• Monitoring, audit and test
• Compliance with international standards

An Implementing Regulation[92] further clarifies for the CSPs how they must comply with the NIS Directive.
In addition to information security and business continuity measures, the DSPs must establish incident response measures based on an assessment of the seriousness of the incident.

[91] The Directive does not concern CSPs considered to be small businesses or microenterprises (businesses employing less than 50 people whose annual turnover or whose total balance sheet is less than 10 million euros)

[92] COMMISSION IMPLEMENTING REGULATION (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

Member States are required to define their own rules on financial penalties and to take the necessary measures to ensure that they are implemented. Member States are likely to apply penalties similar to those of the GDPR (General Data Protection Regulation).

3.1.4.3. France

France has adopted an extensive legal framework on cybercrime and computer-related offences, starting with the Law no 88-19, 5 January 1988, on computer fraud ("Godfrain Law") and its amendments, as codified by Article 323-1 à 323-7 of the Penal Code. Law penalizes hacker attacks of systems and defines the offenses relating to "automated data processing systems" (STAD) and whose provisions were adopted by the Criminal Code. This law allows sanctioning any unauthorized intrusions into a computer system; sanctions vary depending on whether or not the intrusion had an impact on the system.

3.1.4.4. Germany

According to **Ausspähen von Daten §202 a**, anyone who gains unauthorized or other access to data that is not intended for him and that is specially secured against unauthorized access by overcoming access security will be punished with a custodial sentence of up to three years or a fine.

3.1.4.5. Belgium

Cybersecurity has increasingly received attention in Belgium in recent years, because of an increasing number of cybersecurity attacks on Belgian companies. Belgium introduced for the first time in 2000 a specific law on cybercrime. The **law of 28 November 2000 on computer crime** includes a series of provisions designed to fight against computer crime. The Penal Code introduces four new offenses for this purpose: forgery in the computer field (Article 210 bis), computer fraud (Article 504 ter.), data manipulation (Article 550 bis.) and piracy (article 550 ter.).

3.1.4.6. Netherlands

On 21 September 2018, the **Computer Crime Act III (Wet Computercriminaliteit III)** (the Act) entered into force on 01 March 2019. The Act aims to improve the efficiency of tackling cybercrime. The Computer Crime Act III provides law enforcement officials with a new power to access computer systems remotely by stealth.

3.1.4.7. United-Kingdom

The **Computer Misuse Act 1990** includes provision for securing computer material against unauthorized access or modification and for connected purposes. The offences are unauthorized access to computer material, unauthorized access with intent to commit or facilitate commission of further offences, unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer. The Act also makes it an offence to make, adapt, supply or obtain articles for use in unlawfully gaining access to computer material or impairing the operation of a computer.
Besides, the National Cyber Security Strategy provides a focal point for cyber activity across government and has already led to some notable innovation, such as the establishment of the National Cyber Security Centre (NCSC). The programme has also reduced the UK's vulnerability to specific attacks.

3.1.5. TRANSPORT INFORMATION SYSTEM

3.1.5.1. River Information Services (RIS)

RIS based on **Directive 2005/44 / EC** which defines binding rules on data communication and a minimum level for river information services with a view to the future implementation of RIS. The directive provides a European-level framework for the harmonized implementation of RIS and for compatibility and interoperability between current and future information systems in Europe. It specifies for example that which waterways RIS are compulsory (cross-border corridors, etc.)

3.1.5.1.1. At European level

The **directive 2005/44 / EC** and its regulations describe the general principles and conditions of planning, implementation and operation of river information services and associated systems. They are applicable to freight ships, passenger ships and pleasure craft. The three regulations of the commission (CEC, 2007a, 2007b and 2010) define the technical specifications of the main SIF technologies.
River information services (RIS / RIS) are harmonized IT services which take charge of traffic and transport management on inland waterways, particularly at the interface with other modes of transport. They are designed to improve the safety and efficiency of inland waterway transport by optimizing traffic and transport processes. The exchange of information takes place through a fast, demand-driven electronic transfer of data between the water and the coast, through the exchange of information in real time. The information is used in different systems and applications to improve the traffic and transport process. Information is shared on the basis of harmonized information and communication systems.
SIF aims to streamline the exchange of information between all stakeholders in inland waterway transport. Since 2005, the EU Framework Directive has established minimum requirements for the implementation of RIS and agreed RIS standards to allow cross-border compatibility of national systems.
Thanks to the exchange of information, transport operations (such as trip planning or the opening hours of locks) can easily be optimized and allow inland navigation to be better integrated into intermodal supply chains.

- ✓ **Fairway Information Services**

The Fairway Information Services contains geographic, hydrological and administrative data which are used by captains and fleet managers to plan, carry out and supervise voyages. This service provide dynamic and static information on the use and condition of the waterway infrastructure and assist in tactical and strategic navigation decision-making. They only contain data on the waterway infrastructure, not on boat movements, and therefore offer one-way information from the shore to the boat or to company offices. Waterway information services are mainly provided by standardized electronic navigation charts (ENC) and notices to skippers (NtS).

- ✓ **Tactical Traffic Information (TTI)**

There are two types of traffic information : tactical traffic images (TTI) and strategic traffic images (STI). The information provided by the tactical traffic image enables captains to make urgent decisions in real traffic situations. A tactical traffic image allows boat captains to organize navigation with other vessels, as it contains information on the position, speed, and direction of the vessels and the specifics of all targets detected by a radar or, if applicable, an Automatic Identification System (AIS).
The strategic tactical image is displayed on an electronic navigation map. On the other hand, a strategic traffic picture provides an overview of the traffic situation over a relatively large area. The

images are used primarily for planning and monitoring purposes, as a strategic traffic image can provide a user with information on expected vessel journeys, (dangerous) cargoes and requested arrival times (RTA) in defined points such as locks and terminals.

- ✓ **Traffic management**

Traffic management is performed by the waterway authorities aimed optimal use of infrastructure and ensuring a secure browsing. It can include the management of local traffic as well as the management of locks and bridges.
Management of local traffic is provided by the shipping support services (Vessel Traffic Services - VTS). The centers VTS / RIS is currently installed in strategic points along the waterways of the European network. These centers are implemented by the competent authorities to improve the safety and efficiency of vessel traffic and to protect the environment. The service offers the opportunity to interact with vessel traffic and to respond to traffic situations developing around the VTS centers. The information required by the local traffic management are collected using radar stations located on the banks and a system of automated identification system. The AIS provides other information, such as the identity and actual position of the boat. In addition, travel reporting systems provide information about ships, their cargo and planned trips. These sources of information offer to the direction of local traffic information necessary to signal and anticipate potentially dangerous traffic situations and increase the efficiency of traffic flow.
Lock and bridge management helps operators to plan the use of these facilities by providing strategic traffic image. These services help operators in the calculation of estimated arrival times and requested (Expected Time of Arrival and Requested Time of Arrival) ships. This enables optimal planning of lock operations, and thus, the safe passage of ships through the locks and bridges, often seen as obstacles to navigation. Lock planning can significantly reduce wait times. In turn, locks operators can inform each boat captain of time it has to happen, allowing them to adapt their speed and save fuel.

- ✓ **Accident prevention**

The accident prevention assistance records the data concerning ships and transport at the start of the voyage and updates them during the voyage. In the event of an accident, the responsible authorities are able to immediately provide data to the rescue and emergency teams. Electronic navigation charts and tactical traffic images provide the basis for coordination for lifeguards and nautical operations.

- ✓ **Information for transport logistics**

IT services for transport logistics facilitate the planning and execution of logistics services such as those that manage travel planning, transport in ports or terminals as well as goods and fleet management.
Trip planning includes optimal route planning, draft and estimated time of arrival of the boat. Ship captains and fleet managers need information on waterways to plan these operations.
Transport management refers to the management of the transport chain and is carried out by freight brokers and managers of transport services. Its objective is to improve the performance of the entire chartered fleet; monitoring the progress of committed transport; monitoring possible differences with regard to the reliability of this transport; and the possibility of invoicing logistics services.
Intermodal management of ports and terminals provides operators with the information they need on the estimated arrival times of the vessel and its cargo, in order to provide the resources necessary for the operations of the terminal or lock concerned. This arrival information supports the use of the entire terminal and facilitates the passage of boats through the terminal facilities. Thus, the transhipment time can be reduced. In addition, in situations where the capacities of the terminals are temporarily insufficient, the operator can inform each master of the requested arrival time. A

better management of time slots is possible following the exchange of the estimated arrival times and the requested arrival times.
Cargo and fleet management is based on information from loaded or empty vessels, including their actual position, the requested or estimated arrival times, the cargo transported or the cargo to be shipped and information on terminals.

- ✓ **Legal information**

River information services help to comply with inland navigation regulations, for border management (movements of persons controlled by immigration services, customs, etc.) and compliance with the provisions on traffic safety and respect for the environment.

- ✓ **Statistics**

RIS can be used to collect statistics on traffic and freight on inland waterways. As data collected for other services can be used, masters and terminal and lock operators do not have to provide special statistics. Electronic data collection facilitates processes for data providers and statistical offices. The statistics are useful for waterway management authorities, international organizations and companies involved in navigation and will be used to optimize strategic planning and monitoring.

- ✓ **Waterway charges and port taxes**

RIS can help reduce the cost of using infrastructure. A vessel's voyage information can be used to automatically calculate costs and initiate billing, thereby facilitating the processes of users and waterway authorities.

3.1.5.1.2. France

France transposed directive 2005/44 / EC by **decree 2008-168 of February 22, 2008 relating to harmonized river information services** on community waterways, which was codified by decree n ° 2013-253 of March 25, 2013 relating to the provisions of the fourth regulatory part of the Transport Code. The French legal framework for RIS is now included in articles D.4411-1 to 8 of the Transport Code. They are supplemented by a Decree of March 18, 2008.
Voies navigable de France (VNF) ensures coordination for the implementation and interoperability of RIS on the French network (art. D.4411-5 of the Transport Code). VNF ensures the exchange at national level, as well as the processing made necessary by these exchanges, with the managers and users of RIS. The same is true at international level with the authorities in charge of river information services notified to the European Commission. The terms of these exchanges are set by order of the Minister of Transport.

3.1.5.1.3. Germany

Under the Binnenschiffahrtsaufgabengesetz - BinSchAufgG, the controlling authority in charge of RIS in Germany is the Wasserstraßen - und Schifffahrtsverwaltung des Bundes (WSV)[93]. In so far as this is necessary for the operation of the inland navigation information services, in particular for traffic and traffic information, the services of the Bundes Wasserstraßen und Schifffahrtsverwaltung may collect, process and use the following data:

- Identification marks of a registered vessel or association
- Identification of the owner, the supplier, the charterer, the tenant, the debtor or the guide of a ship (last name, address ...)

[93] Inland Waterways Act - BinSchAufgG of 15.02.1956 as last amended by article 1 of the law of 25 April 2017

- from the port of departure and arrival, route, last departure and next port, estimated time of departure and arrival, also on the inland navigation facilities, position at the time of data collection, speed, direction of the journey, status, number of blue cones or lights and draft,
- Cargo data, including type of cargo, HS code, port of loading, port of destination and size of cargo (in tonnes) and, in the case of dangerous goods, name of the cargo, cargo code, class, packaging code and UN number.

3.1.5.1.4. Belgium

The Decree of the Flemish Government of 19 December 2008 lists in its Article 4 the navigable waterways and the ports concerned by the RIS. These are all Class IV or higher inland waterways connected by a Class IV waterway or above to a Class IV or higher waterway of another Member State and ports on the inland waterways. In accordance with Article 6 of the Decree, the Flemish Government has designated the competent authority responsible for implementing the obligations of the Decree and the exchange of information.
"De Scheepvaart" (The Navigation), "Waterwegen en Zeekanaal" (Inland Waterways and Sea Canal), the Navigation Assistance Division of the "Agentschap voor Maritieme Dienstverlening en Kust" (Maritime Service Delivery Agency) and of the Coast) and the port authorities ", act as competent authority within the framework of the article 3, § 1, 1 ° of the decree (article 2 of the decree of the Flemish Government executing the decree of 19 December 2008 relating to River Information Services on Inland Waterways).
The tasks of the competent authority designated by the Flemish Government are the same as those listed in the Order of the Government of the Brussels-Capital Region of 7 September 2005

3.1.5.1.5. Netherlands

The Netherlands has transposed Directive 2005/44 by **amending the Maritime Traffic Act and the Secretary of State Circulation[94],** Public Works and Water Management Regulations containing the designation of the competent authority and the transmission maritime transport services data related to the 2007 Shipping Data Decree 2007 (supply regime for 2007 maritime transport data)[95]. Several organizations have been designated as competent authorities under the Maritime Traffic Act. The management of the shipping lanes is entrusted to various governing bodies. These are the government (invested via the Rijkswaterstaat), the province, the municipality and / or another public entity, including for example the harbor masters[96]. Rijkswaterstaat is responsible for the management of the waterways at national level. In accordance with Article 40 of the Inland Navigation Act Harbor Masters of Port of Amsterdam NV and Rotterdam NV have also been designated as competent authorities. The Coast Guards are managers of the waterways for the coast of the Netherlands. The waterways managers are responsible for ensuring the safety and the fluidity of the traffic; Receiving, storing and providing shipping data by organizations and persons not involved in the navigation[97] and for the proper implementation of river information services (RIS), and therefore the AIS regarding the processing of personal data[98]

3.1.5.1.6. United-Kingdom

[94] Official publication: Staatsblad (Bulletin of laws and royal decrees); Number: 287; Publication date: 2007-08-28
[95] Staatscourant (Dutch Official Journal); Number: 192; Publication date: 04/10/2007;
[96] Art. 2 paragraph 1 of the maritime traffic law
[97] Art. 4 paragraph 1 of the maritime traffic law
[98] Art. 4 (4) of the Maritime Traffic Act

The Directive 2005/44 has **not been transposed** by the United Kingdom. With regard to River Information Services (RIS), the United Kingdom uses ECDIS for navigation purposes, but for cargo and information the approach is still conventional (in paper form). There is no Electronic Reporting Information ship.

RIS harmonize the exchange of information between managers and users of the waterway. Their use goes hand in hand with **AIS**. **AIS** supports and facilitates navigation and increases security.

3.1.5.2. Automatic Identification System (AIS*)*

The **Automatic Identification System** (AIS) is a radio data system on board vessels for the exchange of static, dynamic information and data relating to the voyage of vessels, this exchange occurring between vessels possessing the equipment and between these boats and the stations equipped ashore. On-board AIS devices transmit the vessel's identity, position and other data at regular intervals. By receiving this information, on-board or shore-based AIS devices present in the reception area can **automatically locate, identify and follow vessels equipped with AIS** on an appropriate display device such as radar or interior ECDIS

3.1.5.2.1. At International level

- ***SOLAS Chapter V safety of navigation, 1st July 2002***

The SOLAS Convention is published by the IMO (International Maritime Organization). SOLAS Chapter V refers to the Safety of Navigation for all vessels at sea.
Regulation 19 of SOLAS Chapter V - Carriage requirements for shipborne navigational systems and equipment - sets out navigational equipment to be carried on board ships, according to ship type. In 2000, IMO adopted a new requirement (as part of a revised new chapter V) for all ships to carry automatic identification systems (AISs) capable of providing information about the ship to other ships and to coastal authorities automatically.
The regulation requires AIS to be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size. The requirement became effective for all ships by 31 December 2004.
Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.
A flag State may exempt ships from carrying AISs when ships will be taken permanently out of service within two years after the implementation date. Performance standards for AIS were adopted in 1998.
The regulation requires that AIS shall:

- Provide information - including the ship's identity, type, position, course, speed, navigational status and other safety-related information - automatically to appropriately equipped shore stations, other ships and aircraft;
- Receive automatically such information from similarly fitted ships; monitor and track ships;
- Exchange data with shore-based facilities.

3.1.5.2.2. At European level

Since 1 December 2014, the CCNR has made it compulsory to equip ships with an Inland AIS device and an Inland ECDIS device or a comparable device for displaying charts.

Regarding the European Union, **Directive 2005/44** does not impose a formal obligation to establish AIS. However, it dictates that member countries must use transponders according to the Inland AIS standard if they want to introduce automatic announcement of boats on their network of inland waterways. The European Union has also published technical specifications for Inland AIS, the system used for inland navigation. **Commission Regulation (EC) No 2019/838 of 20 February 2019** concerns the technical specifications applicable to the vessel tracking and positioning systems referred to in Article 5 of Directive 2005/44 / EC relating to marine services River information (RIS) harmonized on Community waterways. It repeals Regulation (EC) No 415/2007.

Inland AIS is based on maritime AIS in accordance with IMO SOLAS regulations. It includes the main functionality of IMO AIS SOLAS while taking into account the specific needs of inland navigation. Only information relating to tracking and location as well as security should be transmitted using the Inland AIS. The provisions regarding the data contained in AIS messages may vary depending on the regulations in force in the state concerned or in the region concerned. The data transmitted by Inland AIS devices can be classified into different categories:

Static data relating to the boat include the following data:

- MMSI (the maritime mobile radiotelephone call number), the name of the vessel, the call sign and the ENI number. Some boats also have an OMI number;
- The type of boat, the dimensions (length and width) and the location of the GPS antenna on board are static data for all isolated boats (i.e. which are not part of a convoy pushed or towed), while these are trip-related data in the case of a convoy. The static data relating to the boat does not change, as long as its owner, nationality or other parameters are not changed. Static boat data is captured, configured and password protected during the installation process. If one or more fields devoted to static data relating to the boat contain erroneous data, this must be corrected by an approved specialized company.

The **dynamic data** relating to the boat are all the data relating to the movements of the boat, for example its position, its speed, its course and its navigation status. The dynamic data relating to the boat are automatically derived from the signals from sensors installed on board.
The trip data is the data that relates to the boat's current trip. These include the port of destination, the current penetration and the nature of the goods transported (The dangerousness of the goods is determined according to a number of blue cones). All the data mentioned under the point “data relating to the trip” is not compulsory in all countries.

The **information relating to traffic management** is intended for the specific use of inland navigation. This information is transmitted when necessary or on request by / to inland waterway vessels only.

3.1.5.2.3. France

Article R4241-50 of the Transport Code provides that special police regulations may also require the use of an automatic identification system on certain vessels. When the special police regulations, in application of article R. 4241-50, require the use of an automatic identification system (AIS), this system must be installed and used in accordance with the provisions of the **article A 4241-50-2 of the Transport Code.** AIS are only authorized for inland navigation approved and installed in accordance with the provisions of the **decree of February 2, 2011** relating to the approval of equipment and companies installing signaling lights, radar devices, speed indicators Inner AIS gyration and devices.
The Inland AIS device must be in good working order, it must operate continuously and the data entered must correspond at all times to the actual data of the boat or convoy. The Inland AIS device

must transmit at maximum power. The obligation of continuous operation does not apply to parked boats unless they are parked in the navigable channel or in other situations defined by specific police regulations; nor to law enforcement and customs vessels if the transmission of AIS data is likely to compromise the performance of police or customs operations.

3.1.5.2.4. Germany

Since December 2016 the use **of Inland AIS and Inland ECDIS is mandatory** for all waterways of class IV and above as well as for selected waterways of class III in Germany. This onboard equipment enables the mutual recognition, identification and display of nearby vessels and their course on an electronic navigational chart. The use of these systems supports onboard navigation and diminishes the risk of accidents; thus, it enhances safety and ease the navigation and contributes to the efficiency and attractiveness of inland navigation. In recent years, the Federal Waterways and Shipping Administration has set up additional shorebased AIS infrastructure along selected waterways. Today, a total of 3600 km of federal inland waterways are covered by shore-based AIS infrastructure.

In parallel with physically setting up infrastructure, the legislation procedure to adopt the legal basis for processing AIS data entered into force with the adoption of the 3rd amendment to the Inland Shipping (Federal Competences) Act in 2017[99].

3.1.5.2.5. Belgium

Article 4.07 of the Royal Decree of April 4, 2014 laying down the General Police Regulations for Navigation on the Inland Waters of the Kingdom, which lays down the rules on AIS in Belgium. Under this text, vessels must be equipped with an Inland AIS device to be permanently operational. The data entered must correspond at all times to the actual data of the vessel or convoy.
In Flanders, according to Decree 17.11.2017, all inland navigation vessels, regardless of their use (freight or passenger transport), are required to have an AIS device on board since 8 January 2018. The installation and operation of the river navigation system. Since the 1st January 2012, the AIS system is mandatory in the port area of the Port of Antwerp.

3.1.5.2.6. Netherlands

AIS has been mandatory since the 1st of December 2014 and on Dutch inland waterways since 1 January 2016. The introduction of AIS into Dutch inland navigation is the result of the European RIS rules.

3.1.5.2.7. United-Kingdom

With regard to River Information Services (RIS), the United Kingdom uses ECDIS for navigation purposes, but for cargo and information the approach is still conventional (in paper form). There is no Electronic Reporting Information ship.

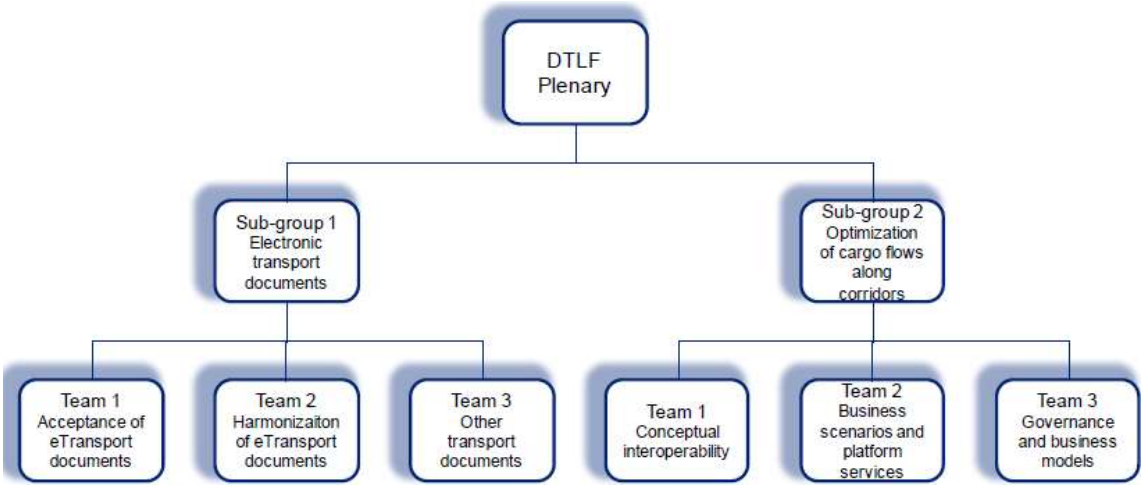
The tracking of the boat is therefore done by AIS. In road, the geolocation of the vehicle, therefore of the goods has long been a fact and this thanks to GPS. It is a regulated practice.

3.1.5.3 EU Project of a Federated network of service platforms

[99] https://www.gesetze-im-internet.de/binschg/BJNR203170956.html

In 2015, the Commission set up a Digital Transport and Logistics Forum (DTLF) where Member States and relevant transport and logistics operators can help each other to promote the electronic exchange of information in transport and logistics. The DTLF also offers the Commission advice and technical expertise when preparing legislative proposals and policy initiatives in the field of the digitalisation of transport and logistics.
The Forum is subdivided into two subgroups, dealing respectively with:

- Sub-group 1 (SG1): the digitalization and acceptance of transport documents[100]
- Sub-group 2 (SG2): the establishment of digital corridor information and management systems



Structure of the Digital Transport and Logistics Forum

The work of SG2 is relevant for STW4 since it aims to promote the creation of a federated network of service platforms: "*This network aims to offer services in the logistics chain that require data sharing. This should encourage innovation, reduce the costs of accessing services for customers and providing services for service platform operators. It will also help meet societal challenges such as cybersecurity, security and sustainable development*".

The objective of SG2's work is to interconnect existing platforms and harmonise the services they offer. ☞ Creation of a **federated network of platforms** for data sharing with two main features:

- ➢ One single entry point for organisations : Business and Authorities (Scope: B2A and B2B)
- ➢ Platform interoperability

The objective is to create interoperability between different platforms, even when each platform is realised with different technology. So it's about establishing a neutral governance structure ensuring trust, safety, and security for data sharing via multiple providers of platform services, including peer-to-peer solutions.

[100] See 3.2.3.5. : Electronic freight transport information Regulation (*eFTI Regulation*)

3.1.6. DEMATERIALIZATION OF GOODS RELATED TRANSPORT DOCUMENTS

3.1.6.1. Legal framework of the Consignment Note (contract of carriage transport document)

With regard to the contract of carriage, information relating to the transport (shipper, consignee, place of pick-up, place of delivery, ...) and the goods (nature, dimensions, number, weight, ...) are recorded in a particular document ("Transport document") which materializes the transport contract. This is the "Consignment Note" or, more rarely and only in maritime or river transport, the "Bill of Lading".

This document serves primarily to formalize the contract of carriage, but it is also required by the supervisory authorities to verify the compliance of the transport with the various regulations. It contains an important part of the information required by the authorities, and they also constitute proof of the legitimate possession of the goods.

3.1.6.1.1. Mode specific international Conventions

There is currently no international convention uniformly applicable to all modes of transport which would unify the legal regime of the transport contract, in particular as regards the possibility of using a dematerialized consignment, regardless of the mode of transport used. The only conventions in force are unimodal international conventions that apply to a single transport mode:

- ✓ Inland Waterway Transport (IWT): Budapest Convention on the Contract for the Carriage of Goods by Inland Waterway (CMNI) Budapest 2000 (CMNI)

- ✓ Road Transport: Convention on the Contract for the International Carriage of Goods by Road (CMR), 19 May 1956 + Additional Protocol to the Convention on the Contract for the International Carriage of Goods by Road (CMR, Geneva 19 May 1956) concerning the E-Consignment note, Geneva 27 May 2008 (E-CMR Protocol)

The CMR Convention can certainly apply to a road + inland waterway transport, but on the condition that road transport is international. It does not therefore apply to inland transport unless the State concerned has decided and has provided for it in its legislation (this is the case in Belgium).
In addition, for the CMR Convention to apply end-to-end, there must be no intermediate reloading. In other words, this convention applies only when the truck, in which the goods are or on which the container is located, is loaded onto the inland navigation vessel, which is never seen in practice. .

3.1.6.1.2. Not uniformly ratified International Conventions

The CMNI and CMR (supplemented by the E-CMR Protocol of February 20, 2008) allow the use of a dematerialized consignment note since they recognize a value equivalent to the paper consignment note. However, if almost all European states have ratified CMNI[101], not all have ratified the E-CMR Protocol.

E-CMR Protocol has been ratified by 25 States[102], including several over the past three years. Among the States covered by the ST4W Project, only France (2016), Netherlands (2009) and the UK (2019) are Parties to the E-CMR Protocol. Belgium and Germany are not parties.

[101] Excepté le Royaume-Uni, ce qui est normal dans la mesure où le Royaume-Uni n'a pas de voie de navigation intérieure commune avec un autre Etat européen et n'est donc pas concerné par cette convention internationale.
[102] Biélorussie (2019), Bulgarie (2010), Danemark (2013), Espagne (2011), Estonie (2016), Finlande (2019), France (2016), Iran (2017), Lettonie (2010), Lituanie (211), Luxembourg (2017), Moldavie (2018), Pays-Bas (2009), Pologne (2019), Portugal (2019), République

With regard to these no-Party States, it can be noticed that:

- ✓ Belgium: Since 2017, on an experimental basis, an E-Consignment note provided by a certified IT provider in Luxembourg, Netherlands or Belgium can be accepted by the authorities of each BENELUX State[103]. However, this experiment is not valid in the case of an E-Consignment note issued in another state (in France for example).

- ✓ Germany: In practice, operators do not use E-Consignment note because authorities of other Member States, such as neighbouring Belgium, do not. Truck drivers do not wish to take risks and therefore are only willing to perform the transport when receive the transport document in a paper format[104]. Germany has joined in 2018 the Czech Republic, Greece, Romania and Serbia to test E-Consignment note in cross-border transport as part of a project funded by the European Commission. The pilot program was planned to finish in August 2019. However, only one German company was involved in this project.

The use of an E-Consignment note in an international transport crossing a State which is not Party to the E-CMR Protocol shall not affect the existence or the validity of the contract of carriage which shall remain subject to the provisions of the CMR Convention (CMR Convention, art. 4). But the E-Consignment won't be accepted by the supervisory authorities of the no Party State.

If we take the example of a transport between France and the Netherlands, which are both State Parties, the E-Consignment note will not be accepted by Belgian authorities because Belgium is not a Party to E-CMR Protocol. On the other hand, the e-consignment note may be used between France and Spain, France and Luxemburg, France and Switzerland. The lack of ratifications of the E-CMR Protocol thus hampers the use of the E-Consignment note in international road carriage of goods. However, there seems to be a move towards ratification of the E-CMR Protocol at European level.

3.1.6.1.3. Non-mandatory international Conventions

In the States where CMNI and the E-CMR Protocol have been ratified, the use of the E-Consignment note is only a possibility recognized by these instruments, leaving the operators free to use it or not. If obstacles or difficulties prevent the use of the E-Consignment note (especially in the case of checks), operators will tend not to use this possibility.

In addition, the imperative nature of the provisions of certain international conventions must be put into perspective. Thus, the CMNI recognizes the validity of the electronic signature of the transport document, but only if it is not prohibited by the law of the State where the transport document was issued[105]. In practice, it applies only if the national legislation of the State under which the contract was concluded allows the use of the electronic means for the conclusion or evidence of a transport contract.

On the other hand, the E-CMR protocol does not include such clause and it is directly applicable if the respective State is a party to the protocol.

---

tchèque (2011), Roumanie (2019), Russian Federation (2018), Slovaquie (2014), Slovénie (2017), Suède (2020), Suisse (2009), Tadjikistan (2019), Turquie (2018), United Kingdom of Great Britain and Northern Ireland (2019).

[103] E-CMR Pilot : Décision du Comité de Ministres Benelux relative à un projet pilote intra-Benelux portant sur la lettre de voiture électronique (2017)

[104] Commission staff working document – Impact assessment, SWD(2018) 183 final, 17 May 2018, p. 13 https://eur-lex.europa.eu/resource.html?uri=cellar:810e3b10-59bb-11e8-ab41-01aa75ed71a1.0001.02/DOC_1&format=PDF

[105] CMNI, art. 11, §2

Finally, these conventions regulate only the contractual relation between the commercial parties involved when they choose to use the contract of carriage in an electronic form.

Furthermore, these conventions do not necessarily require the national authorities of Member States to accept electronic transport documents when performing enforcement tasks, as the conventions regulate only the relationships between the commercial parties involved.

3.1.6.1.4. International Conventions not applicable to domestic transport

The CMNI and the E-CMR Protocol are not intended to apply to inland transport but to international transport. It should be noted that the CMNI allows States Parties to declare, at the time of signature of this Convention, that they will also apply it to inland waterway transport. However, almost none of the countries involved in the ST4W project made such a declaration. The Netherlands has made a declaration to this effect when ratifying the CMNI, but CMNI provisions apply only if the parties to the contract of carriage have agreed to it[106]. These provisions are therefore of conventional application and not imperative.

In fact, regardless of the country in which they are established, the parties to an internal transport contract may contractually agree that the carriage will be subject to the provisions of the CMNI or E-CMR Protocol. Certain General Conditions of Transport so provide. However, another condition remains necessary for the parties to be able to use an E-Consignment note : the national legislation of the country where the transport takes place must recognize the validity of the latter.

3.1.6.1.7. National laws (State's Legislation / National Law) fragmented and insufficiently clear as to the validity of the Electronic Transport Document

- **Inland Waterway Transport**

- ✓ France: The dematerialization of the Consignment note and the Declaration of loading (specifically French control document and intended for VNF) are authorized by the national legislation only if these documents can be presented at the request of the control Authorities[107]. But to our knowledge, French operators do not use an E-Consignment note.

- ✓ Belgium : Law of May 5, 1936 on river chartering is deemed quite obsolete and does not even deal with the Consignment note (only with the Bill of lading). This law is rather adapted to afreightment rather than transport contract. And it isn't adapted to container's carriage but rather to bulk transport. It is currently subject to a broad reform of maritime and inland waterways navigation law (Transport Code project). Except articles 5 and 33, Law of May 5, 1936 is a suppletive law. So, Belgian operators may submit their transport contract (in their General Conditions of Transport) to other provisions, for example to CMNI rules[108], or Professional Conditions of Carriage, for example CBRB Conditions of Carriage[109].

[106] Dutch Civil Code, art. 8.889
[107] C. transp., art.R4461-2
[108] Ex : SOMEF S.A. http://www.somef.be/wp-content/uploads/2016/12/CONDITIONS-GENERALES-DE-VENTE-SOMEF.pdf
[109] Centraal Bureau voor de Rijn- en Binnenvaart (CBRB) Conditions of Carriage. These conditions have been developed by the Centraal Bureau voor de Rijn- en Binnenvaart (Netherlands). Belgian and Duch Carriers are referring to CBRB Conditions of Carriage in their General Conditions.
Ex :
VANUDEN Shipping Terms & Conditions, art. 2.2. d http://www.vanudenshipping.com/termsandconditions
ANTWERP PORT SHUTTLE General Terms, http://www.apsantwerp.be/en/static_pages/terms_and_conditions
HUTCHISON Ports Belgium, art. 2.3. http://www.europeangatewayservices.com/uploads/ENG_Purchase_conditions_TCT_Belgium.pdf

- ✓ Germany : In theory, the E-Consignment note is authorized by national legislation[110]. German police never performs cargo related inspections and therefore does not require a transport document at all[111].

- ✓ Netherlands : In theory, the E-Consignment note is authorized by national legislation to the extent that the parties can agree to apply the provisions of the CMNI to an internal transport[112]. But, according to an ECORYS Study[113], currently, the CMNI consignment note is either in paper form or digitalized in PDF format, etc. There is no digital format yet like E-CMR[114]. Dutch Police requires, based on Regulation 11/1960[115] that ships have paper documentation on board indicating what cargo is on board the ship[116].

- ✓ United Kingdom : There does not appear to be any specific regulation on the transport document[117].

It follows from this information that some national laws do not refer to the electronic Transport Document (Belgium) and that while others seem to allow in theory the use of an E-Consignment note in inland navigation, this possibility does not appear sufficiently clearly stated, which may imply a lack of legal certainty for operators.

One step forward would be to achieve, at European level, the application of the provisions of the CMNI to the inland transport of the Member States, as has been done by certain European regulations in other modes of transport. The electronic Consignment note would thus become formally valid and the supervisory Authorities would be forced to adapt and accept it.

With regard to the General Conditions of Carriage developed by Professional Organizations, they tend to accept the use of EDI:

- IVTB / ICLT / CICT 2010: "*In writing*" *shall include, unless otherwise agreed upon by the parties concerned, the case that the information is contained in electronic, optical or similar media of communication, including, but not limited to telegram, telecopy, telex, electronic mail or electronic data interchange (EDI), provided that the information is available in a manner that it can be used for later reference*" (§1.8.)
- "BV 2016" provide for the application of the CMNI to the Contract of Carriage between Dutch ports, but also in case of national transport within other states (whether or not party to the CMNI) (BV 2016 art. 2.2 ; Toelichting op de Reisbevrachtingsvoorwaarden 2013, art. 2[118])
- The CBRB Conditions of Carriage define the term "In writing" by "*In writing: in each manner in which data can be provided whereby the data is stored, can be verified and can serve as evidence*." (art. 2.9.) and they state that "*The document of carriage can be issued in every format*." (art. 4.1.).

[110] Handelsgesetzbuch, § 408[3]: *Dem Frachtbrief gleichgestellt ist eine elektronische Aufzeichnung, die dieselben Funktionen erfüllt wie der Frachtbrief, sofern sichergestellt ist, dass die Authentizität und die Integrität der Aufzeichnung gewahrt bleiben (elektronischer Frachtbrief)*.
[111] Commission staff working document – Impact assessment, SWD(2018) 183 final, 17 May 2018, p. 13
[112] Dutch Civil Code, Articles 8: 889 "Free choice for the application of the Budapest Convention (CMNI)"
[113] ECOSYRIS, State of play and barriers to the use of electronic transport documents for freight transport - Options for EU level policy interventions, Sept. 2018 https://publications.europa.eu/en/publication-detail/-/publication/b187493e-0349-11e9-adde-01aa75ed71a1
[114] ECOSYRIS, *Annexes*, p. 402
[115] Council Regulation No. 11/1960 concerning the abolition of discrimination in transport rates and conditions (*See 4.1.*)
[116] ECOSYRIS Study, p. 402 ; Commission staff working document – Impact assessment, SWD(2018) 183 final, 17 May 2018, p. 13
[117] No response given by Stakeholders in ECORYS Study
[118] https://www.sva.nl/sites/bva_sva/files/downloads/2017-12/Engels%20BV%202016%20Toelichting%20final.pdf

However, even if the General Conditions of Carriage provide for the possibility of using EDI, it still needs to be accepted by national Legislation and supervisory Authorities.

- **Road Transport**

- ✓ France: The E-Consignment note is provided and authorized by the regulations[119].

- ✓ Belgium: The Consignment note must in principle be in a paper form since it must be drawn up in accordance with the provisions of the CMR[120]. Nevertheless, the use of the E-Consignment note has been recently authorized on an experimental basis from 2016 to 2019 for inland road transport[121]. This is still the case currently under an agreement between the BENELUX states[122].

- ✓ Netherlands: Although the provisions of the Civil Code do not expressly recognize the possibility of dematerializing the Consignment note, General Conditions of Carriage developed by Professional Organizations[123] (which apply in domestic transport as well as in international transport if parties have agreed) recognize the validity and value of the E-Consignment note. In the Netherlands, the E-Consignment note is commonly used because TransFollow (e-CMR's historical solution) was created in 2013 by the professional bodies Transport Logistics Nederlands (TLN) and Evo-fenedex. In addition, under the agreement binding the BENLUX Countries, an E-Consignment note provided by a certified IT provider in one of these States must be accepted by the Authorities of each State, whether in international transport intra-BENELUX or inland transport[124].

- ✓ Germany: The E-Consignment note has the same value as a paper Consignment note and is in principle accepted for inspection unless there is reason to believe that it has been manipulated[125].

- ✓ United Kingdom: According to the answers given by the Stakeholders in the context of the ECORYS study[126], the E-Consignment note is not authorized and the national legislation requires a manual signature.

Apart from that of the United Kingdom, the legislation of the states covered by the ST4W project seems rather well adapted to the use of the E-Consignment note in domestic road transport. However, we do not know whether the use of the E-Consignment note is common in all these states.
In France, it seems that the E-Consignment note is mainly used for transport of grouped parcels (i.e. parcels coming from various shippers and intended for several recipients) where it is necessary to establish many Consignment notes. The low use of the E-Consignment note in the truckloads / ful loads (*transport par lots complets*) can be explained by an absence of need on the part of the

[119] Arr. 9 nov.1999 relatif aux documents de transport ou de location devant se trouver à bord des véhicules de transport routier de marchandises ; Art. 3.4. of the « General contrat-type ».
[120] La Belgique applique les dispositions de la CMR à ses transports intérieurs. Loi du 15 juillet 2013 relative au transport de marchandise par route, art. 29. § 1er
[121] Arrêté royal du 10 avril 2016 relatif à la lettre de voiture électronique
[122] E-CMR Pilote : Décision du Comité de Ministres Benelux relative à un projet pilote intra-Benelux portant sur la lettre de voiture électronique (2017
[123] Stichting Vervoeradres General Transport Conditions (AVC2002)
https://www.sva.nl/sites/bva_sva/files/downloads/2018-02/Weg%20en%20Wagen%20-%20special%20november%202016.pdf
[124] Décision du Comité de Ministres Benelux relative à un projet pilote intra-Benelux portant sur la lettre de voiture électronique, M (2017) 12 http://www.benelux.int/files/9315/0546/8122/M201712_FR.pdf ; ECOSYRIS, *State of play and barriers to the use of electronic transport documents for freight transport - Options for EU level policy interventions : annexes*, 2018, p. 266 https://publications.europa.eu/en/publication-detail/-/publication/8e10f21a-0346-11e9-adde-01aa75ed71a1/language-en/format-PDF/source-search
[125] Handelsgesetzbuch, § 408[3]
[126] ECORYS Study, page 398

carriers. For the truckload carriers, the transition to E-Consignment note would not be sufficiently relevant to the constraints (agreement with DO on an application) and the investments it requires.

3.1.6.2 Legal framework of the Consignment Note (contract of carriage transport document)

3.1.6.2.1. Legal framework of the Dangerous Goods Certificate

As regards the specific transport of dangerous goods, which is particularly controlled at the documentary level, there are two international conventions (ADR in road transport, ADN in IWT) which have been made applicable to international and internal road and river transport by the Directive 2008/68 / EC[127]. This is an example of European harmonization which could be used for transport documents other than those required for dangerous goods.

ADR and ADN enable the use of Electronic Information Processing (EFT) and Electronic Data Interchange (EDI) to replace paper documentation : "*The use of electronic data processing (EDP) or electronic data interchange (EDI) techniques as an aid to or instead of paper documentation is permitted, provided that the procedures used for the capture, storage and processing of electronics data meet the legal requirements as regards the evidential value and availability of data during transport in a manner at least equivalent to that of paper documentation*"[128].

The information that is required by ADR or ADN (UN number, security instructions, etc.) can therefore be dematerialized.

However, ADR and ADN add that « *When the dangerous goods transport information is given to the carrier by EDP or EDI techniques, the consignor shall be able to give the information to the carrier as a paper document, with the information in the sequence required by this Chapter* »[129]. This provision, which requires the shipper to be able to provide the carrier with the information in paper format, is likely to encourage shippers to do so from the outset.

National laws are not always consistent. For example, in France, the decree of May 29, 2009 provides that it is the responsibility of the remitter of the goods to ensure that the Dangerous Goods Certificate appears in the ship's documents[130], whereas the Dangerous Goods Certificate is not included in the list of documents to be on board[131]. Despite the possibility of dematerialization, for reasons of accessibility and practicality, the dangerous goods documentation (Dangerous Goods Certificate, Emergency arrangements appropriate to the consignment, Container Packing Certificate) is in practice generally provided to the carrier in paper format. It seems that the dematerialization of the transport document is mainly practiced in the transport of bulk, but no of containers where the paper document continues to predominate[132]. This is explained by the heterogeneity of containerized goods and the diversity of the contractors.

It must be concluded from these provisions that international and national regulations lack clarity and legal certainty as to the possibility of using EDI in the transport of Dangerous Goods by inland waterways.

[127] Directive 2008/68/CE du Parlement européen et du Conseil du 24 septembre 2008 relative au transport intérieur des marchandises dangereuses
[128] ADN and ADR, 5.4.0.2
[129] ADN and ADR, 5.4.0.3
[130] Decree of May 29, 2009, Appendix III, 2.1.1
[131] C. transp., Article A4241-33
[132] ECORYS study, answers given by Stakeholders, p. 348

3.1.6.3. Legal framework of the Loading Declaration

In France, the Loading Declaration is a paper or electronic declaration which is intended to the establishment of river transport statistics in application of Regulation (EU) N° 2018/974 of 4 July 2018 on statistics of goods transport by inland waterways[133]. It is also used for the establishment of invoicing of Voies Navigables de France (VNF) tolls. For each transport, the Carrier must establish and transmit a Loading Declaration to VNF[134]. It must be established prior to the trip, either by dematerialized way or by means of a paper form which will have to be endorsed at the passage of the first and last lock control.
On an experimental basis, from 1 January 2019 to 31 December 2020, the Declaration of Loading must be established in a dematerialized form for journeys made wholly or partly on part of the French waterways (Seine and Escaut routes : 80% of total inland waterway freight traffic). Throughout the duration of this experiment, a Declaration of Loading which is not made by dematerialized way will be assimilated to a lack of transmission. The dematerialized declaration is made on the internet (via computer or smartphone) in the VELI tool launched by VNF in 2013. 97% of carriers are currently carrying out their online loading declaration[135].
Eventually, a new data collection system could be developed. VELI could be replaced by an even simpler system, where data would be collected directly without reporting formalities and could be shared with the actors in the supply chain, according to their needs and especially with their respective agreements. An evaluation will be made at the end of 2020 of the obligation to use VELI. This could lead to extending this obligation to the entire French inland waterway network.

Not all European states use a Loading Declaration to fulfill their obligations under Regulation (EU) N° 2018/974. For example, Belgian authorities use RIS data: The STA-messages, which are based on the xml-messages from the River Information Services (RIS) and completed with some specific statistical information.

[133] Previously : Regulation (EC) n° 1365/2006 of the European Parliament and of the Council of 6 September 2006 on statistics of goods transport by inland waterways and repealing Council Directive 80/1119/EEC
[134] C. transp., art. L.4461-1, R.4461-1
[135] *Obligation de déclaration électronique Veli : un premier bilan*, Navigation Ports & Intermodalité, 12/2019, p. 27

3.2 DATA SHARING: IDENTIFICATION OF THE LEGAL OBSTACLES OR CHALLENGES

IDIT looked for restrictions / obstacles (regulatory, jurisprudential or other) to dematerialization and data sharing between actors in the transport chain. And what regulatory changes can be expected on these issues.
In particular, it is a question of knowing if the various international and national regulations allow the dematerialization of documents and information linked to transport and if the electronic format is accepted throughout the transport chain.

3.2.1. LEGAL OBSTACLES OR CHALLENGES IN TERMS OF GEO-TRACKING

3.2.1.1 General Data Protection Regulation

The GDPR is the new European regulation on data protection, it is the result of a long work carried out by the G29 (European working group on data protection) and entered into force on May 25, 2018. A through this regulation, the european legislator wanted to create a reinforced and harmonized data protection framework taking into account recent technological developments. The treatments implemented on this date must be brought into compliance with all of the provisions.

3.2.1.1.1 Personal data

Today, these data are therefore considered to be markets. Some data in itself does not represent a significant market value but it is the processing of a large set of data that generates a profit. It is a two-sided market which includes free resources for users in exchange for data collection; data which will be used for commercial purposes by the harvesters. However, **personal data is part of personality rights, that is to say rights that ensure the individual the protection of the attributes of his personality** (privacy, image, personal data). If these rights were property like any other, personal data could be the subject of transfer contracts (to be sold for example). However, we cannot speak of data ownership.
Obviously in practice, the harvesters have the possibility of deriving economic benefits from the data subject to the respect of certain rights of the data subject.
In the transport and logistics sector, they can include:

- Commercial data
  - Prospecting data (name, email addresses, telephone, business cards, personal information, etc.)
  - Customer data (same)
- Operational data related to transport activity and subcontracting:
- Geolocation data

Many logistics companies collect information about their drivers, including their location, speed and duration of their journeys. However, this telemetric information is considered to be personal data and therefore subject to the requirements of the regulations. This does not mean that logistics companies will no longer be able to use telemetry data but rather that they will have to be more careful about how they do it.

- Pickup / delivery data
- HR Data
  - Data concerning employees (name, address, personal info, CV, photo, copy of identity card, social security, etc.) Including certain data deemed sensitive (Social Security number, criminal record, health data)
- IT Data
  - User identifiers (codes, logins, passwords)
  - Technical identifiers (IP address)

- Biometric data (digital access control)
- CCTV data (video surveillance)

3.2.1.1.2 Processing

- Upstream, it is necessary to identify **the legal basis for the processing**. Processing is only lawful if at least one of the following conditions is met:
- **The data subject has consented to the processing** of his data for one or more purposes. Regarding the validity of such consent:
    - It must be given freely: the person must be offered a real choice
    - It must be specific: it must correspond to a single processing, for a determined purpose
    - It must be informed: the controller must provide information relating to his identity, the purposes pursued, the categories of data collected, the existence of a right to withdraw consent
        - It must be unequivocal: it is given by a declaration or any other clear positive act (no ambiguity)

- The processing **is necessary for the execution of a contract** to which the data subject is a party or for the execution of pre-contractual measures taken at the latter's request;
- Processing is **necessary to comply with a legal obligation** to which the controller is subject

For example, the generalization of Linky meters, which remotely collect daily household electricity consumption data, is the result of a legal obligation to modernize networks which meets European directives. Therefore, consent is not mandatory.

- The processing is **necessary to safeguard the vital interests of the data subject or natural person**;
- Processing is **necessary for the performance of a task of public interest** (public service) or falling within the exercise of public authority vested in the data controller ;
- The processing **is necessary for the purposes of the legitimate interests pursued by the controller** or by a third party. Interest is considered legitimate:
    - As soon as the data controller is able to pursue this interest in compliance with the data protection legislation,
    - It must be legal (in accordance with EU law and the countries concerned),
    - It must be necessary for the realization of the interest pursued
    - Be formulated in sufficiently clear terms and does not affect the interest and fundamental rights and freedoms of the person concerned (balancing).

The legitimate interest could, for example, be justified when there is a relevant and appropriate relationship between the data subject and the controller. Example of legitimate interest: economic interest, fraud prevention, security.

- **The general obligations of the controller**:

In the context of transport, we can consider that the subcontractor carrier or the freight forwarder who charters to a carrier may be responsible for processing as soon as the data they transmit to their substitute identify the individual / consumer (last name, first name of client…)

- **Identify the main activities that require data collection and processing** (management of prospect customers, training, recruitment, payroll management, badges and access management, sales statistics, etc.)
- **Keep a detailed register - art. 30.** In this register, it is necessary to create a file for each activity listed, specifying:

- Purpose of the processing (what is the purpose of the processing?)

Ex: customer loyalty

- Another example: I collect information about my customers when I make a delivery, or I need it to edit invoices. These operations constitute processing, the purpose of which is customer management.
- Categories of data used (identity, family, economic or financial situation, bank data, connection data, location data)
- Categories of people concerned (employees, customers, prospect)
- Recipients of the processing to which the personal data have been or will be communicated, including the subcontractors
- Transfers of personal data to a third country or international organization
- Data retention period

- **Implementation of appropriate technical and organizational measures to ensure a high level of data security (data protection by design and data protection by default) – GDPR art. 24 & 25**
    - The Regulation introduces a concept *"privacy by design"* (art. 25. 1), it is a principle of protection of personal data and privacy from conception. It is therefore important to put in place the necessary measures to avoid any loss, disclosure or modification of the data and that the computer processing tools cause little or no harm (we want to minimize the risk of data loss or hacking). Indeed, security breaches have consequences for those who entrust their personal data. Ex: if information is hacked or lost, it can be used to fraudulently enter the customer's home.

Among the technical and organizational measures used, it is invited to resort, for example, to implementing measures such as:

- Data protection policies (charter disseminated by the company, clauses in employment contracts, training, awareness, etc.)
- Alert systems (complaint handling / response time, violation notification process)
    - In terms of data security and confidentiality "*Privacy by default*[136]*"* :

Set up **pseudonymization** or data encryption processes, use anonymity, data minimization. Pseudonymization differs from anonymization. It is a technique of replacing a name or any other personal data with a pseudonym so that the data can no longer be attached to an individual without being cross-referenced with other information. Personal data is **anonymous** or rather made anonymous, when it is no longer possible to identify a person, that is to say that we removed all possible links to find this person. Today, there are several anonymization techniques. If we succeed in proving that thanks to the anonymization technique used we can no longer identify the person and that it is irreversible then all the legislation relating to the protection of personal data will not be applicable because the anonymized data will not be no longer considered personal data.

- **Develop an information systems security plan** (secure premises, secure destruction system for paper documents, update antivirus and software, use complex passwords and change them regularly)

- **Data backup and recovery procedures in the event of an incident.**

[136]It designates the data controller as guarantor of the highest level of confidentiality of the personal data concerned of individuals.

The GDPR sets out **a principle of responsibility**: "*Any person who has suffered material or moral damage as a result of a violation of these regulations has the right to obtain from the controller or subcontractor compensation for the damage suffered*". An approach to anticipating the overall level of security can be supplemented by an insurance approach: it is necessary to find out about insurance policies (civil liability, damage covered, etc.) and about services for the insured (assistance in the event of a disaster, crisis management, etc.).

- **Conduct a data protection impact assessment (AIPD) - Art. 35**

When a type of processing is likely to generate a high risk for the rights and freedoms of natural persons, the controller, performs before the processing, an impact analysis of the planned processing operations. Such an impact assessment is required in cases where:
The treatment corresponds to one of the cases considered by the GDPR, that is to say when it is:

- A systematic and in-depth assessment of personal aspects concerning natural persons based on automated processing (profiling) on the basis of which decisions are taken which produce legal effects with regard to or affecting a natural person in a significative way
- Large-scale processing of sensitive data
- Assuming systematic large-scale surveillance.

When the treatment has the object or effect and meets at least two of the nine criteria[137], in this case, it will also be necessary to conduct an impact analysis:

- Assessment of personal aspects or rating of a person (Financial Scoring[138])
- Automated decision making
- Systematic monitoring of people (remote monitoring)
- Processing of sensitive data (health, biometrics etc.)
- Data processing concerning vulnerable persons (minors)
- Large-scale processing of personal data (e.g. profiling)
- Crossing a dataset
- Innovative uses or the application of new technologies (connected objects)
- The exclusion of the benefit of a right, service or contract (black list)

Must be subjected to impact analysis:
- Road behavior surveillance cameras: they fall within the scope of "systematic surveillance" and "innovative use"
- Tachographs on board road transport vehicles
- Biometric access control (premises / timetable controls)
- Video surveillance of a warehouse storing goods in which handlers work

- **Report any personal data breach**

× **Drafting of a contract between the data controller and its processor**

The term subcontractor is a false friend. In contract law, it designates the realization in whole or in part of a contract for the rental of works (of which transport is part). In the context of the GDPR, the processor is the natural or legal person who processes personal data on behalf of the data controller. In transport, the subcontractor who has been subcontracted a transport contract, or the transporter who has been chartered by a freight forwarder, if they come to handle personal data, will be considered as subcontractor in the sense of the Regulations. Similarly, IT service providers, such as hosting providers, IT security providers, act as subcontractors.

[137] From G29 guidelines
[138] **Credit scoring** is a tool that allows banks to assess the risk represented by the loan applicant. In other words, it allows the credit institution to guarantee the creditworthiness of the loan applicant.

Processing by a subcontractor is governed by a contract or other legal act in which the object and duration of processing will be defined, the nature and purpose of the processing, the type of personal data, the categories of data subjects, and the obligations and rights of the controller.
The processor undertakes to follow all the instructions and only the instructions of the controller.

- **Implementation of measures guaranteeing the security and confidentiality of the data entrusted to them**

The controller must only use subcontractors with sufficient guarantees for the implementation of appropriate technical and organizational measures in order to comply with the requirements of the Regulation (art. 28).

That implies :
- An obligation of transparency and traceability:
  - ✓ Establish with your client a contract or other legal act specifying the obligations of each party and incorporating the provisions of article 28 of the European regulation.
  - ✓ List in writing the instructions of your client concerning the processing of his data in order to prove that you act "on the documented instruction of the data controller".
  - ✓ Ask for written authorization from your client if, as a subcontractor, do you use a subcontractor yourself.
  - ✓ Make available to your client all the information necessary to demonstrate compliance with your obligations and to allow audits to be carried out (on the basis, for example, of the CNIL's standards for the issuance of labels in terms of 'audit).
  - ✓ Keep a register that identifies your customers and describes the treatments you perform on their behalf.

- Taking into account the principles of data protection by design and data protection by default:

You must provide your customers with the necessary guarantees so that the processing you carry out on their behalf meets the requirements of European regulations and protects the rights of the persons concerned. This means in particular that: from their design, your tools, products, applications or services that you offer to your customers, effectively integrate the principles relating to data protection / and by default, your tools, products, applications or services guarantee that only the data necessary for the purpose of the processing are processed with regard to the amount of data collected, the extent of their processing, the retention period and the number of people who have access to it.

- An obligation to guarantee the security of the data processed:

This implies an obligation of confidentiality, of notifying the customer of any breach of his data, of taking measures to guarantee a level of security adapted to the risks,

- An obligation of assistance, alert and advice :

If a customer's instruction constitutes a breach of data protection rules, it is necessary to inform them immediately.
When a person exercises his rights (access, rectification, deletion, portability, opposition, not to be the subject of an automated individual decision, including profiling) the subcontractor must, as far as possible, help the client to respond to this request.

- × **Designation of a data protection officer (DPO ou Data PrivacyOfficer)**

The DPO is in charge of ensuring the security of personal data and ensures that the company complies with the legislation on personal data. He is the referent for the data controller and the processor; he must therefore have legal and technical skills (Art.37 GDPR).

The designation of the DPO is compulsory:
- When the processing is carried out by a public authority or public body;
- When the company performs large-scale data processing of sensitive data (biometric data or health data) or personal data relating to criminal convictions and offenses;
- When the activities of the data controller or the processor, require regular and systematic large-scale monitoring of the persons concerned[139].

3.2.1.2 Geo-tracking in Inland Waterway Transport

3.2.1.2.1 RIS / inland ais and protection of personal data: risks of invasion of privacy

"If the advantages of new technologies are undeniable, as these advances are integrated into economic and social life, they find their limits in the risks of invasion of privacy and individual freedom" (Deboosere, Dessouroux, 2012).

- **RIS**

Directive 2005/44 requires Member States to ensure that the processing of personal data associated with the application of RIS takes place in compliance with European rules on the protection of individual freedoms and fundamental rights. The RIS system works in two directions. Both the competent authorities and inland navigators benefit from the information provided by the information services. Since the inland navigation sector is largely made up of individual companies, the protection of personal data and the protection of privacy in the application of RIS require special attention. For example, the confidentiality of personal information can be compromised because, due to the signals transmitted by on-board equipment, the location of a ship is precisely known. When this data is processed in combination with data that a person can link to this vessel, this affects confidentiality. In order to protect personal data and privacy, the processing of personal data in the framework of RIS must take place **in accordance with European rules on the protection of personal data**.

- **AIS**

AIS is a boat identification system that provides data to identify the boat and determine its position. No detailed information concerning the cargo carried is transmitted. The information transmitted by AIS messages is essentially limited to information that would be visible directly on the boat concerned.
AIS is an open radio transmission system. This means that messages transmitted by AIS devices can be received and viewed by anyone using an AIS device. This is due to the fact that **the AIS has been designed for the exchange of data concerning navigation between an unlimited number of boats and so that everyone can receive messages**. The competent authorities are required to observe the regulations in force concerning the protection of confidential data. It is easy to receive AIS data using AIS receivers and AIS devices. **However, the publication of AIS data on the Internet without authorization from the data sender (and therefore their owner) is prohibited in most European countries.** In some countries, even the mere receipt of AIS data is prohibited for those not involved.
Is "personal data", any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, a online identifier, or one or more specific elements specific to his physical,

[139] Regular monitoring is monitoring that takes place at specific periods, recurring or repeated monitoring at fixed times. The notion of "systematic" implies monitoring taking place via a system or according to a method. For example, the use of tachographs and surveillance devices will certainly require the appointment of a delegate.

physiological, genetic, psychic, economic, cultural or social identity[140]. Even if the position of the barge itself cannot be considered as personal data (as specified in the EU data protection regulation) it becomes so when linked to other information of identification on the persons on board. In these circumstances, the AIS data can be qualified as personal data because the relationship between the ship and the boatman and (if applicable) his family is very linked. When using AIS, the signals sent are neither protected nor encrypted. It's a system that doesn't respect privacy. Because an inland waterway vessel is inextricably linked to the boatman / skipper, some data sent via AIS is personal data. The GDPR regulation therefore applies to their processing and **the sharing of this data is only allowed with the explicit consent of the individual.**

The same goes for the crews and their qualifications. Under the inland waterway workers qualifications directive[141], personal data can only be processed for the purpose of implementing, applying and evaluating the directive (exchange of information between authorities and production of statistics). The re-use of this data for other purposes or its sharing (controlled) with third parties is prohibited without the express consent of the data subject. The restrictions obviously do not apply when the person involved (the captain or member of the crew) voluntarily shares the data with other people.

However, this information may be used or misused by third parties. The risks of invasion of privacy linked to the use of AIS manifest themselves more or less in the following situations:

- reception and subsequent use of AIS data by unauthorized third parties (The chances of unauthorized third parties receiving AIS data are high, given the technical nature of AIS.) ;
- Re-use of AIS data by authorized parties for purposes other than those for which the data was originally collected and intended

Protection of sensitive commercial data

Open information from the AIS raises fears of commercial espionage. Shipping companies and charterers want to remain as discreet as possible about commercial data and information. Apart from the automatic transmission of certain data such as the destination of the ship or its ETA (Estimated Time of Arrival, or fear of arrival time), they fear a risk of commercial espionage: knowledge of the ports of origin or destination, certain cargoes or navigation speeds are indeed available to competing shipowners.

Data sharing requires taking measures to ensure the protection of sensitive commercial data, which is a concern of stakeholders in the waterways sector.

The RIS directive clearly states that "the introduction of an RIS must not lead to the uncontrolled processing of economically sensitive market data by operators" . The channel authorities may collect this data for the purpose of vessel tracking (for example for security reasons), but it is not intended to share this data with third parties.

In the private sector, specific arrangements can be put in place for data to be shared horizontally between several shippers or between several barge operators since the sharing of data can potentially lead to market abuse or commercial practices limiting competition.

There are various reasons why players in the sector refuse to share their data, in particular for reasons of liability. For example, on the basis of travel plans and traffic patterns, it is possible to create a fairway to calculate the expected arrival times or to plan locking operations. Changes (for example, during locking operations) may occur and cause delays. Potential suppliers refuse to share this data in order to limit their liability.

There is a customer-supplier relationship between a barge, a shipper and other logistics players (for example, a logistics operator or a terminal operator). The global treaties regulating these contracts do not always include data protection provisions . However, most contracts with customers require a certain level of confidentiality regarding the details of the cargo carried and the specific customer served.

[140] GDPR art.4

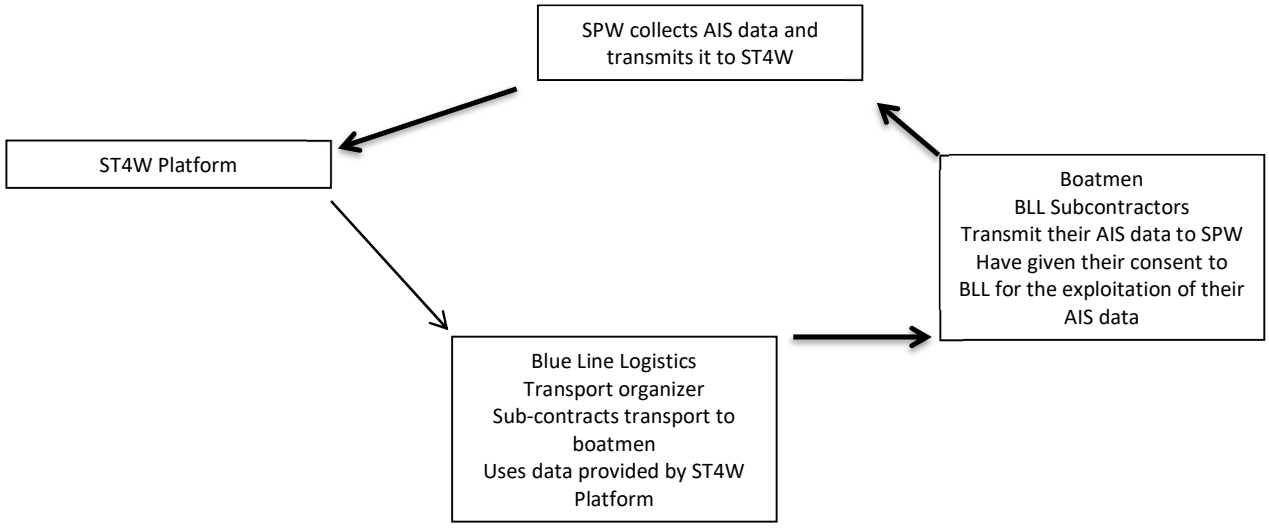
[141] Directive (EU) 2017/2397 of the European Parliament and of the Council of 12 December 2017 on the recognition of professional qualifications in inland navigation

In conclusion, data sharing poses certain legal and business concerns regarding privacy, liability and commercial sensitivity. In some cases, these can be overcome by making specific contractual arrangements (for example, by giving consent for data sharing). In any case, there must be some form of governance to support such arrangements and the technology to support it. However, this is currently lacking.

Conditions à respecter (voir interview avec VBH au bureau)

3.2.1.2.2 ST4W - March 10, 2020 - Conference call with the Wallonia Public Service

Yves DE BLICK
Jean Louis BOUTRY - (SPW) - Systèmes RIS (SIF)
Céline REUTER (SPW)
Marion HIDALGO, Valérie BAILLY-HASCOËT , Gaëlle BONJOUR (IDIT)



A practical case was presented around two questions:

- the provision of boat geolocation data by an administration (here the Wallonia Public Service) to ST4W for use by a transport organizer (Blue Line Logistics).
- the status of the operators present as a data controller or processor. It was clarified that such a qualification depends on the level of intervention of the operator in the processing of users' personal data.

These questions will condition the legal obligations and the applicable liability regime.
SPW sees several objections: The boat is identified by its MMSI number[142] (Maritime Mobile Service Identity) which is personal data (DP) insofar as it makes it possible to identify the boatman (even indirectly). The GDPR is therefore applicable (even if a pseudonymization[143] technique would be used).
SPW is under no obligation to obtain the agreement of the boatman to collect AIS data insofar as it is a legal obligation (Directive 2005/44) for the boatman to be geo-located. However, if SPW agrees to transmit this data to ST4W, the consent of the boatmen will be required (since this is a new

[142] The MMSI is associated with a single registration, it allows a secure identification of the ship and its owner
[143] Technique of replacing a name or any other personal data with a pseudonym so that the data can no longer be linked to an individual without being cross-checked with other information

processing of personal data). SPW does not wish to engage in this collection of consents. Upstream, it is therefore necessary to seek a legal basis for the processing. The concept of "legitimate interest" has been addressed as a potential legal basis. The legitimate interest could be justified when there is a relevant and appropriate relationship between the data subject and the controller (eg legitimate interest: economic interest).
In addition, SPWI considers that it is not part of its public service mission to provide data intended for commercial exploitation. It has been specified that as a data controller, SPW cannot reuse its data for processing which would be different from that for which it has already collected data, the purposes and means of which have been determined for a particular processing.
Finally, he does not want to take any risks in relation to the use that could be made of this data.
However, he agreed to take steps with the Walloon Region to consider the possibility of transferring only the data of the boatmen involved in the ST4W project. This in a purely experimental framework and in the secure framework of the ST4W project.
Regarding the transfer of AIS data from all boats, SPW believes that this can only be done under the cover of a "legal umbrella" possibly resulting from the work of the RIS COMEX (RIS Corridor Management Execution) project.

The tracking of the boat is therefore done by AIS. In road, the geolocation of the vehicle, therefore of the goods has long been a fact and this thanks to GPS. It is a regulated practice.

3.2.1.3 Geo-tracking in road carriage

The employer who uses geolocation must respect several rules, in particular with regard to the GDPR. The employee's refusal to be geolocated is allowed in certain cases.

3.2.1.3.1 France

The legitimacy of the processing of personal data from a geolocation device is assessed in the light of the principle of proportionality as it results from Article L. 1121-1 of the Labor Code. Based on this article, the Court of Cassation[144] considered that a geolocation, implemented without limit, is disproportionate. Consequently, the evidence from the disproportionate.
Geolocation devices can be installed in vehicles used by employees to:

- Monitor, justify and invoice a transport service for people, goods or services directly linked to the use of the vehicle;
- Ensure the safety of the employee, the goods or the vehicles in his charge, and in particular find the vehicle in the event of theft;
- Better allocate resources for services to be performed in dispersed places, in particular for emergency interventions ;
- Incidentally, monitor working time, when this cannot be achieved by another means[145];
- Respect a legal or regulatory obligation imposing the implementation of a geolocation device due to the type of transport or the nature of the goods transported;
- Check compliance with the rules for using the vehicle.

However, the CNIL makes a distinction between employees for whom "the use of a vehicle is only a means of accomplishing their mission" and employees in the transport of people or goods whose

[144] Cass Soc. 26/11/2002 Pourvoi n°00-42401

[145] *Cass. soc. 19 dec. 2018, n° 17-14631 :* about a geolocation control system set up by an employer to control the working time of its employees, newspaper distributors. The device made it possible to record, every 10 seconds, the location of the employee by means of a mobile box which he carried on him.

conditions of performance are governed by specific regulations requiring, in particular, employers to hold precise information on the activity of drivers through the use of tachographs. The establishment of a geolocation system can thus complement the mandatory control systems, which, in view of the lack of autonomy of the employee in the organization of his work, does not pose obvious risks. violations of the rights and freedoms of the employees concerned.
The geolocation system must be entered in the register of processing activities kept by the employer.
The information prior to the installation of a geolocation system is multiple. On the one hand, the employer must respect the information-consultation procedure of employee representative institutions. On the other hand, Employees must be informed of the installation of this device. Each employee must be informed:

- The identity of the data controller
- Purposes pursued,
- The legal basis of the device (obligation stemming from the code
- From work for example, or legitimate interest of the employer),
- Recipients of data from the geolocation system,
- His right to object on legitimate grounds,
- The duration of data storage,
- His rights of access and rectification,
- The possibility of lodging a complaint with the CNIL.

This information can be done by means of an addendum to the employment contract or a memorandum.
Employees can object to the installation of a geolocation device in their professional vehicle, as long as this device does not comply with legal conditions. They must have access to the data concerning them recorded by the tool (dates and times of circulation, journeys made, etc.).
Employees must be able to deactivate the collection or transmission of geographic location outside working hours.

- **Access to data**

Access to the information in the geolocation device must be limited to the authorized personnel of the departments concerned, the employer and the authorized personnel of a client or principal with whom a service is justified[146].
In principle, the information obtained by geolocation should not be kept for more than two months. However, they can be kept for one year when they are used to optimize rounds or for the purposes of proof of interventions carried out, when it is not possible to provide this proof by other means. Finally, they can be kept for five years when they are used to monitor working time.

- **Geolocation of independents**

With regard to self-employed workers such as those who provide services through digital platforms, recent case law indicates that the use of a geolocation device by the platform may be an indication of the existence of a power platform control and therefore a subordination link, characteristic of the employment relationship, allowing to reverse the simple presumption of non-wage earning provided for in favor of individual entrepreneurs by article L.8221-6-I of the code work.
It is this aspect that was taken into account by the same Social Chamber of the Court of Cassation to estimate that a courier was in a permanent legal subordination relationship with regard to the Take Eat Easy platform, which operated on him a power of control through a geolocation system allowing the real-time monitoring of his position, as well as the accounting of the total number of kilometers traveled (Cass. soc. 28 Nov 2018, n ° 17-20.079) . Similarly, such a power of control was detected by the Paris Court of Appeal in the use by the company Uber of a geolocation system for transport

[146] the name of the driver must not be communicated to a client or principal, since this information is of no interest to these people, unless this information is of particular and essential interest.

vehicle drivers (VTC), regardless of the motivations put forward by the (CA Paris 10 Jan 2019, n ° 18/08357). Admittedly, this index of control of the entrepreneur's activity is not sufficient in itself to characterize the link of subordination specific to the employment contract, but it was each time used to justify the judge's decision.
For the time being, the geolocation of users (deliverers, VTC) carried out by the platforms seems to be apprehended by case law only from the angle of "requalification". But beyond this social issue, intermediation platforms must also endeavor to secure both the conditions of service and the processing of personal data of these users with regard to IT and freedoms law and GDPR. If the CNIL has not yet addressed the issue of processing implemented by delivery or transport platforms, it nonetheless published on October 11, 2018 a list of the types of processing operations for which an analysis of data protection impact (AIPD)[147] is required. Among these is "Large-scale location data processing" such as mobile applications allowing the collection of geolocation data from users.

3.2.1.3.2 Belgium

Belgian law does not specifically address the issue of geolocation, however, there is strict privacy protection that employers must take into account. The right to respect for private life, recognized by Article 8, 1 ° of the ECHR [148]and by Article 22 of the Constitution, must be guaranteed for the entire duration of the employment contract and not only at the time of recruitment and of the dismissal.
Although the geolocation of employees by the employer is not specifically regulated, the employer must comply with the law of July 30, 2018 relating to the protection of individuals with regard to the processing of personal data[149]. Article 8 of the ECHR and article 22 of the Constitution must also be respected. Finally, the general data protection regulations (GDPR) must also be observed.

- **Principles to be respected**

If there is no legislation expressly regulating the question of geolocation, the Data Protection Authority issued an opinion on September 7, 2005 according to which geolocation of vehicles is only authorized subject to compliance with the principles of finality, proportionality , transparency and admissibility.
An automobile geolocation system can only be set up with the prior agreement of employees, who also have a right of withdrawal at any time.
The company must specify in a "*geo-policy*" annexed to the labor regulations[150] :

[147] Guidelines on data protection impact assessment (AIPD) and how to determine if the processing is 'likely to cause a high risk' for the purposes of Regulation (EU) 2016/679 (Working Party "Article 29" on data protection) https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf
List of types of processing operations for which a data protection impact assessment is required (CNIL) https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements- AIPD-with-requise.pdf
[148] European Convention on Human Rights and Fundamental Freedoms.

[149] http://www.ejustice.just.fgov.be/mopdf/2018/09/05_1.pdf#Page10

[150] In a judgment of November 14, 2011, the Ghent Labor Court, on the other hand, ruled that the installation and use by the employer of a geolocation system in a worker's vehicle was illegal. In casu, the employer had simply included in its work regulations a statement that all of the workers' vehicles were equipped with a GPS tracking system. The Court considered that this single mention was clearly not sufficient to meet the requirements of purpose (article 4 of the Privacy Law) and of information of the person concerned (article 9 of the Privacy Law). The Court therefore concluded that the employer had committed a contractual breach vis-à-vis his worker and could be liable on this account to an indemnity towards this worker if he had suffered damage.

- The objectives pursued by the geolocation system (the same as those declared to the Commission for the protection of privacy) ;
- The list of people monitored in the company, as well as the nature of the data collected and their maximum retention period ;
- Persons authorized to access data inside the company (the accounting department or human resources) as well as outside (the federal police or the justice system) ;
- The type and frequency of controls planned to combat misuse of data, as well as the procedure and sanctions applicable in this area.

The control must be done for a **legitimate purpose**
A system making it possible to locate staff members precisely must meet specific, explicit and legitimate purposes which justify their installation and use, for example in terms of occupational safety, in terms of the protection of service vehicles , to meet well defined professional needs concerning transport and logistics or, to be able to knowingly exercise control over the personnel, therefore with a view to controlling the professional use of service vehicles and the proper execution of the work regime.

The control must **be proportionate**
Even if the aim pursued by the control is legitimate, the interference in the worker's private life must still be relevant and minimized. Permanent and systematic control is in principle disproportionate. To meet the proportionality criterion, the control must only take place during working hours and on the condition that the worker can activate and deactivate the means of control (for example at the end of his working day).
Proportional control implies that if the desired result can be obtained by other means, which do not affect the privacy of the worker, these means must be preferred. The employer can, for example, if he suspects abuse, request a detailed report from the worker or question clients about the presence or absence of the worker in their company.
This type of control also implies that the data collected cannot be kept longer than necessary.

The control must **be transparent**
Under the terms of article 74 of the law of July 30, 2018, the processing of personal data may, inter alia, be carried out only with the consent of the data subject, or when this processing is necessary for the execution of the contract to which the person is a party.
This means that if the geolocation system set up by the employer is necessary for the activity of the company (for example at a cash transport company), the worker's consent will not be necessary. On the other hand, in all other cases (for example for transporters), it will be necessary to obtain the agreement of the worker on the installation of the geolocation system. This agreement must be obtained in writing, through a geo-policy or an annex to the employment contract. The GDPR strengthens the principle of consent. This must now be enlightened, unequivocal, free, specific and personal and implies a positive act on the part of the worker. This consent can, for example, be given by checking a box or signing a clause. The worker also has the possibility to withdraw his consent at any time.
The employer is required to communicate the following information beforehand:

- The legal basis for data processing. In the event of geolocation, it is likely to be the legitimate interest of the company or of third parties [151];
- Who is the subject of the control ;
- The extent to which there is control ;

In a judgment of March 2, 2016, the same Court considered that no legal provision authorizes the employer (and his attendant, in this case a private detective) to place a geolocation system in the clean vehicle of the worker without his agreement, even without being informed.

[151] & Obligations added by the GDPR

- The objectives pursued by the control ;
- The nature of the abuses that can lead to control ;
- The duration of the control ;
- The data processed ;
- If the data is sent outside the European Union ;
- What are the rights of the worker, in particular the right to consult data, the right to lodge a complaint with the Data Protection Authority, the right to limit the processing of data;
- The procedure which will be followed after the check.

In companies where the coordination of company vehicles is not subject to a particularly tight schedule (as in the cleaning company here), the introduction of GPS positioning must be well thought out.

3.2.1.3.3 Germany

Under German law, the collection of location data by a telecommunications service provider requires the consent of the data subject, unless these data are anonymized[152] (which may be the case when he provides his employee with a smart device and / or the technical infrastructure to use it.)

Under article 26 of the Federal Data Protection Act (BDSG), an employee's personal data may be collected, processed or used for employment-related purposes when necessary for decision-making. before hiring, to execute or terminate his employment contract. The interests of the parties will be weighed, taking into account the processing purposes in question. In summary, employees should not be geolocated when they are in a private area and should not be observed continuously during their working hours.

The processing and analysis of the location data collected must be limited to the specific needs of the employer for control or organizational purposes, that is to say, for the coordination of work processes. Location data should always be stored in an anonymous form, to avoid the creation of individual profiles.

Employees must be informed of the collection and processing of their personal location data and the purposes pursued. In the absence of transparency, the employer is required to delete personal data relating to employees and is liable to a fine of up to € 50,000.

In Germany, the works council has the right to co-determine the rules for the operation of the company and the conduct of employees. The provisions of the data protection law do not preclude the prerogatives of the works council as soon as a technical device allows objectively controlling the behavior or performance of employees, regardless of whether the employer uses them for these purposes. fine or not. The conclusion of an agreement between the works council and the employer specifying the principles and the scope of application of the associated data processing is therefore required to constitute a legal basis for the collection and analysis of data.

3.2.1.3.4 Netherlands

In the Netherlands, control of workers is not prohibited. However, employers must consider the privacy of employees. Employee control is authorized if it meets the conditions of the General Data Protection Regulation (GDPR) and the GDPR Implementation Act (UAVG)[153].

• The employer has a legitimate reason (legitimate interest). This interest must prevail over the employees' interests in matters of confidentiality.

[152] Dry. 98 of the Telecommunications Act (Telekommunikations-gesetz or "TKG")

[153] Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) https://wetten.overheid.nl/BWBR0040940/2020-01-01

• Control must be necessary. In other words, there is no other way to achieve the goal that is less intrusive for the privacy of employees.
• The employer informs the employees of what is authorized and what is prohibited, that control is possible and how it is done. This can be done, for example, with rules of conduct or a protocol.
• The employer takes into account the employees' right to confidential communication. For example when checking an email or a phone.
• The employer requests the prior approval of the works council (OR) for a (secret) control system.
• The employer must then carry out a data protection impact assessment (DPIA). This is the case, for example, if the employer uses video surveillance for this purpose structurally and / or for a longer period. If the impact study reveals a high risk; the employer must consult the Dutch Data Protection Authority before starting the staff audit. This is called prior consultation.

Secret control, without the employees' knowledge, is normally not allowed. The employer can only use secret control under certain conditions. In addition to the conditions for "normal" control, the following additional conditions apply to secret personnel control:

• The employer reasonably suspects that one or more employees are behaving in a manner that is punishable or prohibited.
• Despite all kinds of efforts, the employer is not able to put this behavior
• Secret control is incidental.
• The employer always informs the employees involved of the secret control afterwards. Even if the audit did not prove that the suspicion was justified.

In case of deployment of a GPS system, the employer needs the approval of the works council. In principle, the employer cannot use the personnel monitoring system without the agreement of the works council.

3.2.1.3.5 United kingdom

In the UK, the primary rule is that vehicle tracking is legal as long as drivers and other employees know they are being tracked, this means that businesses are allowed to install tracking devices on their vehicle fleet, but they must inform all of their personnel immediately and acquire consent for collecting data. There are no exceptions to this law, other than in law enforcement and government agencies in which covert trackers may be needed for investigations.
The Information Commissioner’s Code of Practice for Employees is clear on how the employee should be treated : it is clearly stated that the employee has the right to know about any methods used to monitor them. It also favours methods with the least intrusion of privacy and suggests that employees should only be monitored during working hours, with the option of switching off surveillance tools during private time.
Most of the laws that affect vehicle tracking involve the privacy and protection of an employee and their personal data. There are the two pieces of legislation that affect vehicle tracking, The Human Rights Act 1998, and The Data Protection Act 1998.
Article 8 of the The Human Rights Act says that everyone has the right to respect for their private and family life, and their home etc. This is particularly important when considering vehicle tracking and employees. The tracking device must have a confidentiality button allowing the driver to deactivate the tracking of the vehicle outside working hours. This helps to protect privacy and helps make sure that the vehicle tracking device is only in place to track the vehicle, for business purposes, and not the individual, for any other purpose.
The Data Protection Act 1998 is in place to protect all essential data collected by companies and to specify that all employees have a right to know about the information being stored and processed

about them. The Data Protection Act dictates that all personal data must be processed lawfully and fairly while the personal data has to be obtained for specified and lawful reasons.
The Act states that personal data should be :

- Processed fairly and lawfully
- Obtained only for specified and lawful reasons
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer that necessary, to fulfil it's purpose
- Processed along the lines of the individual's human rights
- Protected against unauthorised or unlawful use, loss or destruction
- Kept within the European economic area

Managers have a responsibility to distinguish and state whether the information is business or personal and whether the company is using it lawfully to improve their business with the consent of their employees. As long as a company is within the boundaries of the law, doesn't share personal employee data or use data without consent, it is completely legal for a company to track their business vehicles and drivers.
In the recent regulation, the EU and UK government increased the penalties for failing to protect personal data. Companies can still store personal employee data on secure servers and use it to improve their business, but they need to check whether the proper consent to gather, store and process that data was gathered. As of 25th May 2018, businesses must ensure that the consent given for all data – even that collected before the change – meets the new protocols. In other words, employees will have to re-consent to their data being used in any capacity.

The new principles relating to the processing of personal data dictate that personal data are:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest. Scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures.
- The controller shall be responsible for, and be able to demonstrate compliance with the previous six principles.

Various tools already exist so that river transport seizes all the opportunities offered by the digitalization of logistics chains and the dematerialization of administrative procedures. However, if their technical implementation is proven, they remain certain obstacles to their general application.

3.2.2. Protection of sensitive data commercial

While scanning and automation via RIS / AIS systems help improve the efficiency of transport systems, they make them more vulnerable to cyber attack due to their increasing complexity and interconnection.
To reduce these risks, the Directive on security of network information (NIS) [154]was adopted in July 2016. This directive encourages collaboration between Member States and aims to develop their capacity to quickly investigate incidents and raise awareness of vulnerabilities among national authorities.
Apart from the risks of cyber, the invasion of privacy, the protection of commercial data and the lack of interoperability are all obstacles to the exploitation of data.

3.2.2.1 Obstacles in terms of data exploitation

"If the advantages of new technologies are undeniable, as these advances are integrated into economic and social life, they find their limits in the risks of invasion of privacy and individual freedom" (Deboosere, Dessouroux, 2012).
Directive 2005/44 requires Member States to ensure that the processing of personal data associated with the application of RIS takes place in compliance with European rules on the protection of individual freedoms and fundamental rights. The **RIS system** works in two directions. Both the competent authorities and inland navigators benefit from the information provided by the information services. Since the inland navigation sector is largely made up of individual companies, the protection of personal data and the protection of privacy in the application of RIS require special attention. For example, the confidentiality of personal information can be compromised because, due to the signals transmitted by on-board equipment, the location of a ship is precisely known. When this data is processed in combination with data that a person can link to this vessel, this affects confidentiality. In order to protect personal data and privacy, the processing of personal data in the framework of RIS must take place **in accordance with European rules on the protection of personal data**.

AIS is a boat identification system that provides data to identify the boat and determine its position. No detailed information concerning the cargo carried is transmitted. The information transmitted by AIS messages is essentially limited to information that would be visible directly on the boat concerned.
AIS is an open radio transmission system. This means that messages transmitted by AIS devices can be received and viewed by anyone using an AIS device. This is due to the fact that **the AIS has been designed for the exchange of data concerning navigation between an unlimited number of boats and so that everyone can receive messages**. The competent authorities are required to observe the regulations in force concerning the protection of confidential data. It is easy to receive AIS data using AIS receivers and AIS devices. **However, the publication of AIS data on the Internet without authorization from the data sender (and therefore their owner) is prohibited in most European countries.** In some countries, even the mere receipt of AIS data is prohibited for those not involved.
Even if the position of the barge itself cannot be considered as personal data (as specified in the EU data protection regulation) it becomes so when linked to other information of identification on the persons on board. In these circumstances, the AIS data can be qualified as personal data because the relationship between the ship and the boatman and (if applicable) his family is very linked. When using AIS, the signals sent are neither protected nor encrypted. It's a system that doesn't respect privacy. Because an inland waterway vessel is inextricably linked to the boatman / skipper, some data

[154] Directive (EU) 2016/1148 on security of network and information systems (NIS Directive)

sent via AIS is personal data. The GDPR regulation therefore applies to their processing and **the sharing of this data is only allowed with the explicit consent of the individual.**
The same goes for the crews and their qualifications. Under the inland waterway workers qualifications directive[155], personal data can only be processed for the purpose of implementing, applying and evaluating the directive (exchange of information between authorities and production of statistics). The re-use of this data for other purposes or its sharing (controlled) with third parties is prohibited without the express consent of the data subject. The restrictions obviously do not apply when the person involved (the captain or member of the crew) voluntarily shares the data with other people.
However, this information may be used or misused by third parties. The risks of invasion of privacy linked to the use of AIS manifest themselves more or less in the following situations:

- reception and subsequent use of AIS data by unauthorized third parties (The chances of unauthorized third parties receiving AIS data are high, given the technical nature of AIS.) ;
- Re-use of AIS data by authorized parties for purposes other than those for which the data was originally collected and intended

3.2.2.2 Challenges for data sharing : protection of sensitive commercial data

Open information from the AIS raises fears of commercial espionage. Shipping companies and charterers want to remain as discreet as possible about commercial data and information. Apart from the automatic transmission of certain data such as the destination of the ship or its ETA (Estimated Time of Arrival, or fear of arrival time), they fear a risk of commercial espionage: knowledge of the ports of origin or destination, certain cargoes or navigation speeds are indeed available to competing shipowners.

Data sharing requires taking measures to ensure the protection of **sensitive commercial data**, which is a concern of stakeholders in the waterways sector.

The RIS directive clearly states that "the introduction of an RIS must not lead to the uncontrolled processing of economically sensitive market data by operators"[156]. The channel authorities may collect this data for the purpose of vessel tracking (for example for security reasons), but it is not intended to share this data with third parties.
In the private sector, specific arrangements can be put in place for data to be shared horizontally between several shippers or between several barge operators since the sharing of data can potentially lead to market abuse or commercial practices limiting competition.
There are various reasons why players in the sector refuse to share their data, in particular for reasons of liability. For example, on the basis of travel plans and traffic patterns, it is possible to create a fairway to calculate the expected arrival times or to plan locking operations. Changes (for example, during locking operations) may occur and cause delays. Potential suppliers refuse to share this data in order to limit their liability.

There is a customer-supplier relationship between a barge, a shipper and other logistics players (for example, a logistics operator or a terminal operator). The global treaties regulating these contracts do not always include data protection provisions[157]. However, most contracts with customers require a certain level of confidentiality regarding the details of the cargo carried and the specific customer served.

[155] Directive (EU) 2017/2397 of the European Parliament and of the Council of 12 December 2017 on the recognition of professional qualifications in inland navigation
[156] recital 10
[157] in particular the CMNI relating to the contract for the carriage of goods by inland waterway

In conclusion, data sharing poses certain legal and business concerns regarding privacy, liability and commercial sensitivity. In some cases, these can be overcome by making specific contractual arrangements (for example, by giving consent for data sharing). In any case, there must be some form of governance to support such arrangements and the technology to support it. However, this is currently lacking.

3.2.3. LEGAL OBSTACLES AND CHALLENGES IN THE USE OF ELECTRONIC TRANSPORT DOCUMENTS

T he shared use of freight transport information (FTI) requires the dematerialization of the documents on which this information usually appears. It therefore implies the legal recognition of the value of the Electronic Freight Transport information (e-FTI), whether by the judge or the Competent Authorities.

Goods related Transport Documents[158] (Consignment note, Dangerous Goods certificate, etc.) have both Business to Business (B2B) and Business to Administration (B2A) functions / use:

• B2B: evidencing a contract of carriage, proving ownership, acceptance, etc.
• B2A: used for governance and inspection: a transport document is handed over at inspection to an officer upon request of that officer.

The scope of the ST4W project is limited to domestic transport (within one State) or possibly intra-Community transport (between two EU states). Movements of goods between Member States do not require any customs documents (for VAT compliance for ex.)[159].

There is no International or European uniform legal framework yet providing for the validity of the electronic Transport Documents and requiring Competent Authorities to accept regulatory information in an electronic form.

Regulation (EU) No 910/2014 *on electronic identification and trust services for electronic transactions in the internal market* (eIDAS Regulation) provides a horizontal EU legal framework for the acceptance of electronic documents by Member States' authorities, but only as evidence in legal proceedings. It does not impose an obligation on Member States' (enforcement) authorities to accept electronic documents as evidence for other regulatory purposes, such as compliance with various legislative provisions, including as concerns the conditions for the transport of goods;

As a result, national legislation is fragmented and insufficiently clear as to the validity of the Electronic Transport Document. Competent Authorities still often require the production of paper transport documents and operators still produce these documents in paper format.

3.2.3.1. Risks incurred in case of check by competent authorities

According to the survey conducted by the Digital Transport and Logistics Forum (DTLF) between April 2017 and February 2018, overall interviewees believe most limiting barriers hindering the acceptance and use of e-fTD (electronic freight transport documents) are legal and regulatory

[158] This analysis does not deal with "Transport related documents" (information on the means of transport from a safety perspective : Vehicle Registration Certificate) or "Personnel related documents" (information on the qualifications and nationality of personnel operating a mean of transport and / or handling the cargo).
[159] With regard to international transport, there are some initiatives at a European level for a single window (EU Single Window Environment for Customs), but also at a national level. As an example, in France, French Customs launched a national single window (Guichet Unique National du dédouanement - GUN), to make sure that all administrations which may be involved in an international transport will be connected in order to dematerialize all documents.

barriers[160]. Among legal and regulatory barriers, respondents believe most hindering issues are related to the lack of appropriate legislative frameworks in the EU Member States on the acceptance by the authorities of e-fTD[161]

Notwithstanding the recognition of the legal value of the electronic transport document by the majority of international and national legislation, competent authorities often continue to require the production of paper documents[162], especially for reasons of distrust or difficulty of understanding the electronic document. With regard to the transport contract document, some authorities are wary of the risks of manipulation / falsification of electronic documents and, in case of doubt, may require a paper document. With the lack of interoperability of standards, the requirement of paper documents as part of the control is indeed the major bottleneck to dematerialization mentioned by Stakeholders in ECORYS's study[163]. To avoid the risk of electronic documents being declared noncompliant by authorities or not accepted by their partners, the transport operators, as well as the other commercial parties involved, prefer to print, carry and exchange paper cargo documents, in spite of all the inconvenience and cost this implies. The concordance between theory and practice does not seem self-evident.

This problem concerns the transport contract document (Consignment note) and especially the dangerous goods documents (Dangerous Goods Certificate, safety instructions).

In addition, some European regulations have not been adapted to dematerialization. In particular, *Regulation No. 11/1960 concerning the abolition of discrimination in transport rates and conditions*[164] requires, for control, the production of a transport document giving the details[165] of each consignment of goods within the Community. It specifies that the Transport document will be made in duplicate and shall be numbered. One copy shall accompany the goods; the other copy shall be retained by the carrier for two years, reckoned from the date of carriage, and shall be filed in numerical order. It makes responsible the carrier of the good establishment of this document (Reg. 11/1960, art. 6).

Nb : In IWT, the most cited reason for partially or entirely paper-based transport operations is not the risk incurred in case of check by competent authorities, but the fact that business counterparts do not use e-fTDs (electronic freight transport documents)[166]. In road transport, the most cited reasons are the facts that electronic documents are not accepted by relevant national and cross-border authorities[167].

3.2.3.2. Risks incurred under the contract of carriage regime

[160] *Towards paperless transport within the EU and across its borders - Report*, Digital Transport and Logistics Forum (DTLF), Sub group 1: electronic transport documents, 2018 (p. 183, question 55)

[161] P. 183, question 56

[162] Cette information provient de l'étude ECOSYRIS. Dutch Police requires, based on Regulation 11 (1960) that ships have paper documentation on board indicating what cargo is on board the ship.

[163] ECOSYRIS Study, A*nnex – Stakeholder consultation report* (*3.3.2. Drivers of the overall problem*, p. 20) https://publications.europa.eu/en/publication-detail/-/publication/f2ee0cc1-0343-11e9-adde-01aa75ed71a1/language-en/format-PDF/source-search Les personnes interrogées dans le cadre de cette étude ont précisé que le défaut d'acceptation du document de transport électronique par les banques ou les assurances n'est pas significatif.

[164] Regulation No 11 concerning the abolition of discrimination in transport rates and conditions, in implementation of Article 79 (3) of the Treaty establishing the European Economic Community https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31960R0011&from=EN

[165] Name and address of the consignor, nature and weight of the goods, place and date of acceptance of the goods for transport, place at which the goods are to be delivered, …

[166] *Towards paperless transport within the EU and across its borders - Report*, Digital Transport and Logistics Forum (DTLF), Sub group 1: electronic transport documents, 2018 (p. 177, question 43)

[167] *Towards paperless transport within the EU and across its borders - Report*, Digital Transport and Logistics Forum (DTLF), Sub group 1: electronic transport documents, 2018 (p. 167, question 13)

This risk stems from the previous one. The legal and conventional framework of the contract of carriage makes the Principal (shipper, freight forwarder, consignee) liable for the consequences (blocking, delay, demurrage) resulting from the insufficiency of the documents or the information which must appear on them. This risk may encourage the Principal to provide paper documentation in order to avoid any risk of blockage related to the use of electronic documents.

- ✓ Conditions générales CONTARGO (art. 4.2.) : « The customer is responsible for the accuracy of the information supplied by him and for the accuracy of any translations as well as for the completeness of the paperwork. CONTARGO does not have the duty to check the information, or any statements made, or the paperwork, for accuracy and/or completeness. The customer is liable for all consequences which arise from the absence, the incorrectness, the inaccuracy or incompleteness of information or from late or incomplete transfer of information, even if no blame or fault is present; the same shall apply with regard to statements which are made. » (art. 4.4.) : "If a means of transportation is halted or prevented from commencing a journey as a result of the lack, inaccuracy or incorrectness of the declaration or the accompanying documents, nonobservance of import, export and transit regulations or other legal regulations on the part of the customer and resulting official measures, or if the loading units are seized or other disadvantages arise as regards orderly dealing with the transportation, the customer shall be liable to CONTARGO for all resulting delays, damage, demurrage, detention, costs, fines, forfeits and other disadvantages as the joint and several debtor, regardless of whether the customer is himself at fault or not."

- ✓ Conditions générales SOMEF (art. 4.4.) : « *Si le bateau est arrêté par mesure administrative ou de police, à raison de documents insuffisants ou de documents qui ne sont pas dressés dans la forme réglementaire, de déclaration inexacte ou insuffisante dans lesdits documents, l'expéditeur et respectivement le destinataire sont responsables de tous risques, dangers, dommages, pertes de temps et frais quelconques qui pourraient en résulter.* »

- ✓ Pays-Bas : Dutch Civil Code, Article 8:911 Provision of required documents and information

- 1. The consignor (shipper) must compensate the carrier for the damage suffered by the latter because documents or information, which had to be provided by the consignor (shipper) because they are required for the transport or for the fulfilment of customs or other formalities which have to be performed prior to the moment that the goods are delivered, are, for whatever reason, not sufficiently present.
- 2. The carrier must exercise due diligence (reasonable care) so that the documents which have been handed to him, shall not get lost or attended incorrectly. Damages due by him in this respect shall not exceed those which, in case of the loss of goods, are due pursuant to Articles 8:903 up to and including 8:906.
- 3. The carrier is not obliged, but nevertheless entitled to check whether the information given to him is correct and complete.
- 4. If at the end of the period within which the documents and information meant in paragraph 1 should have been present, these documents and information are not, for whatever reason, sufficiently present, then Article 8:908, paragraph 2, 3, 4 and 5 shall apply accordingly, except in case of a time charter.
- 5. If, because the documents and information meant in the present Article are not sufficiently present, the carriage of goods of the involved party or of another consignor

(shipper) is prolonged during the relevant voyage due to a delay of the start or the progress of that voyage, then the compensation (damages) shall not be less than the amounts of the demurrage charges for the number of hours with which the carriage has been prolonged.

- ✓ Belgium : Persons interested in the road transport may be punished administratively or criminally if they have not established the consignment note (carrier) or have not ensured that it has been established (shipper) (Law of 15 July 2013, art. 43. §2, art. 46. §1er).

In addition, certain general conditions of operators that accept the use of EDI include clauses limiting their liability for confidentiality. This can also be a barrier to using EDI.

Ex : CONTARGO, art. 34.5.: "In the absence of agreement to the contrary, CONTARGO is not obliged to invariably treat all order data as confidential".

3.2.3.3. Each carrier issues a "living" Transport Document

Each carrier prepares its own transport document because the regulations require it, but also because this document materializes the transport contract. The carrier includes the description of the goods and the obligations to which he is bound. The transport document also contains the carrier's general conditions. But, throughout the transport, other information is inserted in the transport document:

- ✓ Dates and hours of boat or vehicle's arrival at destination
- ✓ Dates and hours of beginning and end of loading operations
- ✓ Dates and hours of beginning and end of the unloading operations
- ✓ Actual and set temperatures when taking over the load and when the load is transferred out of the sphere of responsibility of the Carrier
- ✓ Principal and Carrier's reservation at loading
- ✓ Consignee's discharge and reservation at unloading

This information may be inserted by different people: Freight forwarder, Consignor, Carrier, Consignee. It is therefore necessary that dematerialization allows everyone, at each stage of the transport, to insert the required or necessary information with a secure identification of the person who inserts them. And it is also necessary that only concerned and authorized persons have access to each data.

3.2.2.4. The Bill of lading could be hardly dematerialised

A Bill of Lading (BL) is issued only on Principal's request.
In the current state of the law, the BL can hardly be dematerialised because it constitutes an ownership title over the goods being transported. The enterprise that owns the original copy of the BL is the owner of the goods. This original copy of the BL is negotiable (≠ Consignment note). A Bill of Lading is such a document, mostly used when goods are traded during transport (e.g. commodity trading of bulk cargo). In practice, the BL is used for an entire shipment of bulk cargo[168], not for containers or pallets.
And the consignee must present it to the carrier in order to get the goods or to modify the transport ("right of disposal").

[168] See for ex. CG SOMEX S.A., art. 4.20, al. 3 : « *Sauf convention contraire, l'établissement d'un connaissement ne vaut que pour un lieu de chargement et un lieu de déchargement avec le transport du tout.* »

Because of this particular function, the BL is usually in a paper format. It can be envisaged that it is dematerialized in order to use the information that is contained in it, but the importance of its negotiable nature will undoubtedly mean that paper bills of lading will continue to exist unless we can maintain this particular function.

3.2.3.5. Electronic freight transport information Regulation (eFTI Regulation)

The Commission has recognised the need to speed up the acceptance of electronic transport information in a number of policy-setting documents such as the *2011 White Paper on Transport*, the *2015 Digital single market Strategy* and the EU *eGovernment action plan for 2016 to 2020*.

The work of SG1 focuses on replacing existing paper documents accompanying goods flows with data, with a view to achieve complete paperless logistics. Business to Business (B2B) exchanges do not fall within the scope of SG1, the perimeter is primarily Business to Administration (B2A).

Based in particular on the conclusions of the study carried out by ECORYS[169] and an online survey[170], DTLF concluded that to advance in the dematerialization, necessary action need to be undertaken in the following three focus areas:

- the acceptance of electronic transport documents by all stakeholders, and particularly by national authorities;
- the possible harmonization of these documents at data elements level and across all transport modes, and of contract of carriage transport documents in particular. Instead of an electronic document approach, which is considered too rigid, a data centric approach (to allow defining "data sets") and business process driven artefacts is considered highly desirable and will thus be taken. The idea is that data which is stored by IT back office systems may be re-used and complemented to produce different documents and support various formalities. For this, it is necessary to use common formats. Agreement on a common data dictionary would facilitate transport.
- the development of possible common IT infrastructures /environments to support the electronic exchange of this data, both among the private stakeholders and, in particular, with the authorities.

On the basis of substantive preparatory work, involving an Impact Assessment, extensive stakeholder consultations, as well as drawing on work and recommendations by DTLF, the European Commission has drawn up a *draft* ***Regulation of the European Parliament and of the Council on electronic freight transport information (eFTI Regulation)***[171] .

[169] ECOSYRIS, State of play and barriers to the use of electronic transport documents for freight transport - Options for EU level policy interventions, Sept. 2018 https://publications.europa.eu/en/publication-detail/-/publication/b187493e-0349-11e9-adde-01aa75ed71a1

[170] Online questionnaire "Digital Transport and Logistics Forum (DTLF) – Use of digital transport documents by businesses" between April 2017 and February 2018. The key objective of this survey is to understand the current state of play regarding the use of electronic documents in transport.

[171] COM (2018) 279 final, 17 May 2018 :
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0279 ;
Impact assessment :
https://eur-lex.europa.eu/resource.html?uri=cellar:810e3b10-59bb-11e8-ab41-01aa75ed71a1.0001.02/DOC_1&format=PDF
Adopted at first reading by Parliament: 29 January 2019
End 2019 / early 2020: adoption of the final text by the Parliament and the Council
Sept / Oct 2019: Start of trilogue discussions (parliament, council and commission)
2020-2023: Preparation & adoption of technical specifications
2024/2026: entry into force.

The general objective of this Regulation is to establish a uniform legal framework for the digital transmission of information relating to the transport of goods and thereby contribute to greater efficiency in the transport sector.

On April 7, 2020, the Council has adopted its position at first reading. The legal act now needs to be adopted by the European Parliament at second reading before being published in the Official Journal (expected June 2020). It shall apply only four years from its entry into force.

eFTI Regulation primarily concerns **B2A data exchanges for Goods. B2B data exchanges for Goods won't be in the scope of this Regulation. However, "**the acceptance by competent authorities of information in electronic form with common specifications would ease not only communication between competent authorities and economic operators but, indirectly, also the development of uniform and simplified **business-to-business** electronic communication across the Union" (*Regl., recital 4*).

eFTI Regulation concerns "**regulatory information requirements**" that is a requirement to provide regulatory information.

Regulatory information means information, whether or not presented in the form of a document, that is related to the transport of goods in the territory of the Union, including of goods in transit, which is to be made available by an economic operator concerned in accordance with the provisions referred to in Article 2(1) (see below) in order to prove compliance with the relevant requirements of the acts laying down those provisions (Regl., art. 3.1.).

Regulatory information are those required by :

- Council Regulation No. 11/1960 which deals with the Transport Document specifications ☞ **Consignment note**
- Regulation (EC) No 1072/2009 on common rules for access to the international road haulage market : Transport Document attesting the characteristics of the cabotage transport ☞ **Consignment note**
- Directive 2008/68/EC which provides for the application to inland waterways transport and road transport of the provisions of the Regulations annexed to the ADN and ADR (Chapter 5.4. : Dangerous Goods Transport Document) ☞ **Dangerous Goods Certificate**

eFTI Regulation will list the National Laws that require regulatory information (Part B of Annex I, expected June 2021).

The Regulation won't apply to controls by customs offices, as provided for in the applicable Union provisions. The Union Customs Code as laid down in the Regulation (EU) No 952/2013 already contain provisions allowing fulfilment of reporting formalities by means of electronic information communication (e.g. simplified transit), including as regards the cargo and, respectively, the transport operation.

If an economic operator concerned would like to transmit the information required to the Competent Authorities electronically, it will be able to do so by means of electronic freight transport information (eFTI) platforms certified by the national authorities.

"**Economic operator concerned" means a transport or logistics operator**, or any other natural or legal person, who is responsible for making regulatory information available to competent authorities in accordance with the relevant regulatory information requirements (*Reg., art. 3.14*).

IDIT : **Governance-oriented analysis**

"**Electronic freight transport information" or "eFTI"** means a set of data elements that are processed by electronic means for the purpose of exchanging **regulatory information** among the economic operators concerned and between the economic operators concerned and competent authorities (*Reg., art. 3.4*).

In the years following the entry into force of the eFTI Regulation, the Commission will assess possible initiatives with a view in particular to establishing the obligation for economic operators to make available electronically regulatory information to competent authorities (June 2028), in accordance with this Regulation (Règl., art. 16.1).

Where economic operators concerned make regulatory information available electronically to a Competent Authority, they shall do so on the basis of data processed in **a certified eFTI platform** and, if applicable, by a certified eFTI service provider. The eFTI Regulation will establish the functional requirements applicable to these eFTI platforms. Those requirements will ensure, in particular, that all eFTI data can be processed solely in accordance with a comprehensive rights-based access-control system that provides assigned functionalities, that all competent authorities can have immediate access to that data in accordance to their respective regulatory enforcement competences, that the processing by electronic means of **personal data** can be carried out in accordance with RGPD and that the processing of **sensitive commercial information** can be carried out in a way that respects the confidentiality of that information.

This eFTI Regulation won't prevent the BtoB use of eFTI platforms, or prevent the use of additional functionalities on eFTI platforms, provided that this does not adversely affect the processing of the regulatory information that falls within the scope of this Regulation, in compliance with the requirements of this Regulation.

"**eFTI platform**" means a solution based on information and communication technology (ICT), such as an operating system, an operating environment, or a database, intended to be used for the processing of eFTI (*Reg., art. 3.10*)

Shippers and logistics service providers (eg freight forwarders) have a variety of choices to meet their logistics needs. Although inland waterway transport has a strong position in some markets (eg bulk freight), its position in others is weak or threatened by the development of other competing modes of transport. For example:

- Autonomous driving and grouping of trucks should reduce the costs of the road transport and increase its flexibility;
- The new rail corridors and the next generation of freight trains are expected to reduce technical and organizational obstacles to freight rail transport (competitive advantage over river transport).

Many of these developments are driven by digitalisation and different kinds of intelligent transport systems. If nothing happens, river transport may be delayed.

POA 4: RECOMMANDATIONS

POA4 consists of the implementation of recommendations aiming to streamline and facilitate exchanges by optimizing regulatory competitiveness as well as proposals for the improvement of administrative and customs procedures.

In order to achieve this, we asked for help from our partners. A working group has been formed. Given the rather broad scope of GOA (legal aspects in the broadest sense of the word), it was decided by the meeting participants to focus the recommendations in POA 4 only on the following aspects: Issues and regulations regarding GDPR; Electronic documents, Uptake and regulation; Cybersecurity; Complexity of regulations regarding the supply chain + Covid 19. These four main points have been added to the questionnaires for the interviews.

Two major problems emerge from the analysis of the interviews:

- ✓ a lack of confidence in the sharing of personal data and ;
- ✓ an administrative burden linked to the lack of interoperability.

4.1 ISSUES AND REGULATIONS REGARDING GDPR

Sharing data through the ST4W application poses certain legal and business issues: Regarding privacy, liability and commercial sensitivity.

4.1.1 Observation of a trust issue

Analysis of stakeholder interviews shows that, while data sharing is generally accepted (especially in Germany), doubts remain regarding data security and privacy.

- *"Many things are not subject to GDPR, because some aspects are laid down in contracts. Terminals or logistics service providers, for example, regulate the sharing of data with inland shipping companies in a private law context and this falls outside of GDPR. This concerns data that can be traced back to privacy-sensitive matters (including location data)."*
- *"In The Netherlands and it appears that resistance to sharing data can mainly be found among the small vessel owner-operators (owning operating one small vessel) who live on board of the vessel as well. There is a deep-seated distrust to share data and a desire to keep a grip on things. In any case, there must be some form of governance to support such arrangements and the technology to support it. This is, however, lacking at this time."*
- *"Using AIS is mandatory, but data is not protected"; "**It would be a good idea to include ship data in GDPR regulation***"
- *"AIS tracking sometimes is an issue. If the skippers are living on board of the vessel, tracking and tracing might relate to privacy issues in the minds of the skippers."*
- ***"AIS should be closed and for the use of pre-chosen parties (authorities, ports, locks, certain shippers, etc.) only."** ; "An interesting case is also the usage of AIS for the collecting of port This is not the goal of AIS, and therefore **extra agreement** by the skippers is needed",*
- "*The scope of GDPR is not clear. The skippers could be concerned about being tracked (because the vessel is their home) but he thinks the tracking solution offers by ST4W or in the context of an EU project should be less of a concern than AIS MarineTraffic with which you can already follow any vessel. Furthermore, tools such as ST4W could end up be better regulated than MarineTraffic*."

4.1.2 To restore confidence

Even if the position of the barge itself cannot be considered as personal data (as specified in the EU data protection regulation) it becomes so when linked to other information of identification on the persons on board. In these circumstances, the AIS data can be qualified as personal data because the relationship between the ship and the boatman and (if applicable) his family is inextricably linked. When using AIS, the signals sent are neither protected nor encrypted. It's a system that doesn't respect privacy. Because an inland waterway vessel is inextricably linked to the boatman / skipper, some data sent via AIS is personal data. The GDPR regulation therefore applies to their processing and **the sharing of this data is only allowed with the explicit consent of the individual.**

To restore confidence in data sharing, the Commission has unveiled a **proposal for a Regulation on data governance**[172] aimed at promoting the availability of data for use, increasing trust in intermediaries and strengthening sharing mechanisms across the EU. The instrument would respond to the following situations:

• The provision of public sector data for reuse: This is data subject to third party rights (data that may be subject to data protection legislation, intellectual property rights or that contains business secrets or other information commercially sensitive). The proposed EU? regulation does not create any right to re-use data held by public bodies. However, it defines a set of harmonized basic conditions, compliance with which would allow such reuse (the requirement of non-exclusivity, for example). Public sector bodies allowing this type of reuse should be technically equipped to ensure that data protection, privacy and confidentiality are fully preserved. Member States will need to establish a single point of contact to help researchers and innovative companies select appropriate data, and they will be required to put in place structures that will support public sector bodies with technical solutions /advice and legal assistance.

• Data sharing between companies with the help of a "personal data sharing intermediary":
The draft regulation allows the sharing of personal data via a data sharing service provider to help individuals exercise their rights under the GDPR and thus increase confidence in the sharing of personal and non-personal data and reduce transaction costs associated with sharing data between businesses (B2B) as well as between individuals and businesses (C2B). These providers will have to meet a number of requirements:

- ✓ Remain neutral with regard to the data exchanged;
- ✓ Do not use this data for other purposes;
- ✓ Assume a duty of loyalty towards the people who use this data (when the data sharing service provider offers services to natural persons).

The aim of this approach is to enable data sharing services to operate in an open and collaborative way, while giving individuals and legal entities the means to act through a better overview and better control of their data.

• Allow the use of data for altruistic reasons: The proposal provides for the possibility for organizations that practice data altruism (data made available voluntarily by individuals or companies, for the common good), to register as a 'data altruistic organization recognized in the EU"

[172] Proposal for a regulation of the European Parliament and of the Council on European data governance (act on data governance); COM (2020) 767 final
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0767&from=FR

in order to build confidence in their activities. A common European data altruism consent form will be developed in order to reduce the costs associated with the collection of consent and to facilitate data portability (when the data to be made available is not held by the person).

In some cases, these (consent forms?) can be overcome by making **specific contractual arrangements** (for example, by giving consent for data sharing). One possible solution could be the establishment of a **privacy policy**. This would aim to provide skippers **with clear and comprehensive information on the processing of personal data to be carried out.** This document will be an opportunity for the data controller to demonstrate an accountability approach by highlighting (in application of the principle of Accountability):

- ✓ Identify the DPO and his contact details;
- ✓ Collect an informed consent respecting privacy: The data, here geolocation, is only collected for reasons of parcel traceability. The co-contractor is informed about the purpose of the data collected, recipient (s) of the data, data retention period
- ✓ Inform about rights of the co-contractors (rights of access and rectification, limitation of processing, right of opposition for legitimate reasons to the processing of their personal data, etc.)
- ✓ Inform the obligations of the controller and the processors in the event of a data breach

4.2 ELECTRONIC DOCUMENTS, UPTAKE AND REGULATION

The lack of digitalization threatens the overall competitive position of inland waterway transport companies. Digitalization is one way to improve the competitiveness of inland waterways transport. New logistics planning concepts are implemented (in Europe, globally? Based on digitalization?). Inland waterway transport must be an integral part of these planning concepts or it risks losing its competitive position in multimodal chains. For example:

- Shippers and logistics service providers use the concepts of **synchromodal planning**: constantly choosing the right modality and transport service based on logistics needs, service availability, costs, deadlines and (in some cases) environmental constraints - taking into account of real-time conditions of the infrastructure (eg delays). Inland waterway transport can only be part of these planning concepts if carriers are able and willing to share the data required for such concepts (eg ETA)
- In supply chains, the vision of the physical internet will result in increased consolidation of shipments through **smart hubs**. Inland waterway transport can only be part of this vision if carriers can work seamlessly with these smart hubs and shippers embracing this vision.

4.2.1 AN ADMINISTRATIVE BURDEN

The stakeholders point out that there is an administrative burden that adds additional costs and inefficiencies to their operations.

- ➢ *"Troubles with electronic documents are widespread over the total transport sector. Every EU member state implements their own way of doing this, which makes electronic documentation not suitable for all international transport. IWT still has a lot of documents on paper on board. This is based on an old EU regulation and interpreted different by each member state."*

- ➢ *"When looking at BICS, it is first important to understand that BICS is only a system to implement ERI. On the Rhine, it is mandatory to report by electronic document. BICS is a software solution to make such an electronic report. On other fairways, this is not mandatory. In the EU, there are multiple national mandatory reporting systems and software solutions. However, it is not mandatory in the whole of the EU. BICS software is freely available, but not all fairway authorities have the needed software to accept BICS reports. Although this is*

mandatory by EU regulation, this is still not implemented union wide. BICS is usable for all types of vessels and cargo, because it is a broad software solution" ; "Regulation could help the sector more, but mainly ***standardisation in data exchange is vital."***

4.2.1.1 The European Union's response

The European Union's response lies in the new regulation, eFTI Regulation - electronic Freight Transport Information[173] .The aim of this text is to encourage the digital switch-over of freight transport and logistics in order to reduce administrative costs, improve the enforcement capacities of competent authorities and strengthen the efficiency and sustainability of transport. It establishes a legal framework for electronic communication between the economic operators concerned and the competent authorities of regulatory information relating to the transport of goods in the territory of the Union. To this end, it:

- sets the conditions on the basis of which the competent authorities are required to accept regulatory information when it is made available electronically by the economic operators concerned;
- sets the rules applicable to the provision of services linked to making regulatory information available to the competent authorities by electronic means by the economic operators concerned (eFTI certified platform).

The regulation is intended to enable compliance with regulatory information requirements by electronic means rather than using paper documents. However, it does not end the possibility of presenting this information on paper.
The documents that must be accepted by the national authorities in their electronic version from 21 August 2024 are as follows: the consignment note for rail, road and river transport[174]; the consignment note in road cabotage[175]; the combined transport document for trucks, trailers, semi-trailers, swap bodies and containers (road-rail, road-inland waterway, road-sea)[176]; the dangerous goods road, rail and inland waterway transport document (ADR, RID, ADN)[177]
The documents required by national regulations and containing information identical to those required by the above European regulations must also be accepted[178].
The dematerialization of these important documents will of course not become compulsory in 2024 but will eliminate a major obstacle to digitalisation insofar as the supervisory authorities will no longer be able to require their presentation in paper version. This will certainly have a favorable impact on the dematerialization of documentation in transport and data exchange.

4.2.1.2 The Central Commission for Navigation on the Rhine (CCNR): An example to follow on all the waterways of the European Union in terms of IWT dematerialization?

- "*In the countries bordering the Rhine (NL, DE, FR, BE, Swiss), BICS is used for electronically sharing of documents on containerships, ships with dangerous goods, tankers, and bigger passenger vessels. It is suitable for all types of vessels, but not yet mandatory for all types. A safety recommendation would be to include all types of vessels. Specifically, all vessels should be required to electronically report the number of persons on board, as a safety measure for the first responders during incidents."*

[173] regulation (EU) 2020/1056 of July 15, 2020 on electronic information relating to the transport of goods
[174] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.P_.1960.052.01.1121.01.FRA&toc=OJ:P:1960:052:TOC

[175] https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1598002628668&uri=CELEX:02009R1072-20130701
[176] https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1598002283262&uri=CELEX:01992L0106-20130701
[177] https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1598003531197&uri=CELEX:02008L0068-20190726
[178] These national regulations must be communicated to the European Commission by 21 August 2021 at the latest and will appear in Annex I, part B of Regulation (EU) 2020/1056

Since **1st January 2010**, the Central Commission for Navigation on the Rhine (CCNR) has gradually introduced electronic reporting requirements on the Rhine for vessels or convoys carrying containers. Electronic reporting facilitates data interchange between vessels and sector traffic centres compared with reporting by radio telephony or in writing. Electronic reporting is integral to River Information Services (RIS) and facilitates:

- strategic traffic-related information,
- traffic management,
- the prevention of accidents,
- statistics,
- the implementation of requirements.

This measure is helping to modernise inland navigation and promote the use of new technologies. It also reduces the administrative burden.

This (electronic reporting?) is a process that works (and has just been extended)[179]. The idea would be to extend the process to all types of transport by river, on the one hand and on the other hand to other European rivers.

4.2.2 DATA SECURITY

However, while digitalisation and automation processes help improve the efficiency of transport systems, they also make them more vulnerable to cyber-attacks due to their increased complexity and interconnection.

4.2.2.1 Cybersecurity

- *"As regards cybersecurity, in general the danger lies in sabotage of physical processes (e.g. breaking into production processes, shutting down cranes) and in taking data hostage (e.g. ransomware APMT in the Port of Rotterdam in 2017). The greatest innovation in data and digitization is not seen among inland shipping companies or infrastructure managers, but rather at the terminals and logistics service providers."*

There are various reasons why industry players refuse to share their data, particularly for reasons of liability. For example, based on travel plans and traffic patterns, it is possible to create a fairway to calculate expected arrival times or to plan lockout operations. Changes (for example, during lockout operations) may occur and cause delays. Potential suppliers refuse to share this data in order to limit their liability.

[179] The electronic reporting requirement provided for in article 12.01 of the RPR, which can be processed today via radiotelephony, in writing or electronically, must be carried out electronically with effect from **1st December 2021**. The electronic reporting requirement, which previously only applied to convoys and vessels carrying containers on board, will be extended to the types of vessel indicated below.

- Vessels carrying goods covered by the ADN under article 12.01(1)(a) of the RPR;
- Vessels of a length exceeding 110m under article 12.01(1)(d) of the RPR;
- Cabin vessels under article 12.01(1)(e) of the RPR;
- Seagoing vessels under article 12.01(1)(f) of the RPR;
- Vessels with an LNG system aboard under article 12.01(1)(g) of the RPR;
- Special transport operations as construed by article 1.21 under article 12.01(1)(h) of the RPR.

To reduce these risks, the Network Information Security (NIS) Directive (Directive (EU) 2016/1148 on security of network and information systems (NIS Directive) (adopted in July 2016) encourages collaboration between Member States and aims to develop their capacity to promptly investigate incidents and sensitize national authorities to vulnerabilities. The RIS Directive clearly states that "the introduction of a RIS must not lead to the uncontrolled processing of economically sensitive data relating to the market by operators"[180].

Channel authorities may collect this data for the purposes of vessel tracking (eg for security reasons), but it is not intended to share this data with third parties. In the private sector, **specific arrangements can be put in place for data to be shared horizontally between multiple shippers or between multiple barge operators as data sharing can potentially lead to market abuse or business practices restricting competition.** There is a client-supplier relationship between a barge, a shipper and other logistics players (for example, a logistics operator or a terminal operator). The global treaties regulating these contracts do not always include provisions on data protection (in particular the CMNI relating to the contract for the transport of goods by inland waterway). However, most contracts with customers require a certain level of confidentiality with respect to the details of the cargo being carried and the specific customer served.

4.2.2.2 Covid-19: An accelerator for innovation

- *"Regarding COVID-19, the pandemic has increased the acceptance of electronical documents in the business to business sectors. In IWT, it is mainly the case with liquid bulk carriers. For instance, after delivering the load, the skipper is presented with a clearance document "losverklaring". Before covid, it was mandatory to pick this up in person. Currently, this document is electronically exchanged to ensure personnel safety. So in this case, COVID has been an accelerator for innovation. "*

In its roadmap presented on 9 December 2020, the Commission recalls that greenhouse gas emissions from the transport sector have increased over time and today represent up to a quarter of the total emissions attributable to the transport sector in EU. The biggest challenge facing the sector is therefore to significantly reduce its emissions and become more sustainable. In particular, the Green Deal for Europe calls for a 90% reduction in greenhouse gas emissions from transport, so that the EU becomes a climate neutral economy by 2050. The Commission identifies ten key areas which will guide its work in the years to come. With the right level of ambition, all the measures set out in this strategy can help reduce emissions from the transport sector by 90% by 2050. And in particular, concerning ST4W : Make connected and automated multimodal mobility a reality. The EU must take full advantage of smart digital solutions and intelligent transport systems (ITS). The aim is also to make Europe a world leader in the development and deployment of connected, cooperative and automated mobility (CCAM) services and systems.

[180] recital 10