KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

RNE Data Study

Consultancy study for RNE

Charlotte Ducuing, Orian Dheu and Aliki Benmayor

KU Leuven Centre for IT & IP Law - imec

March 2022

RNE data study

Charlotte Ducuing,[1] Orian Dheu[2] and Aliki Benmayor[3]

[1] Charlotte Ducuing is a doctoral researcher at CiTiP – KU Leuven, charlotte.ducuing@kuleuven.be

[2] Orian Dheu is a doctoral research at CiTiP – KU Leuven, orian.dheu@kuleuven.be

[3] Aliki Benmayor is a researcher at CiTiP – KU Leuven, aliki.benmayor@kuleuven.be

Contents

1. Defining 'data'

Before discussing the legal frameworks applicable to data in general (Part II) and railway law more specifically (Part III), the notion of 'data' should be clarified. Overly referred to in policy documents but also in legal frameworks, it remains difficult to delineate clearly 'data' and to distinguish this notion from neighboring ones. The notion of data is essentially a technical one (1.1) which has made its way to EU law (1.3). In the digital era, data *as such* should be distinguished from products and services in digital form where data constitutes the building block(s) (1.2).

1.1. Data v information

The ISO/IEC 2382-1:1993 (then replaced by ISO/IEC 2382:2015) standard equates data with "a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing. Data can be either created/authored by people or generated by machines/sensors, often as a 'by-product'. Examples: geospatial information, statistics, weather data, research data, etc." The ISO definition of data is often referred to or used as a source of inspiration, including by policy and law-makers.

This definition includes both machine-generated data, data generated by humans, computable (or digital) v *analogue data.* It is of technical nature for two reasons. First, data are defined technically as a set of bits and bytes which represent information. Second, data are defined by reference to the types of processing which can be made.

Data is defined as the *syntactic* level of information which should be distinguished from the semantic level. The semantic level refers to the meaning and makes part of the content layer. For instance, the name of a person or media content qualify as information at its semantic level. In contrast, the syntactic level refers to the signs and how they relate to each other and makes part of the code layer. Concretely, the syntactic level consists of a succession of bits and bytes.[4]

It is however not always easy in practice to draw the line between the syntactic and the semantic level – or between 'data' and 'information'. Data are defined at the syntactic level, but they are valuable in the data economy only because *information* and *knowledge* can be created out of them. The distinction between the syntactic and the semantic level of data / information is not clear-cut in EU law, as discussed further in section 1.3.

1.2. Data as such v digital 'something'

Data should be distinguished from products and/or services based on or constituted by data, while making the distinction is not always easy. Indeed, data are often valuable *per se* precisely because they can contribute to digital objects and services at a later stage of their lifecycle.

In this respect, data should be notably distinguished from the following notions.

Notion + source	Definition	Comments

[4] Herbert Zech, 'Data as a Tradeable Commodity' (*European Contract Law and the Digital Single Market: The Implications of the Digital Revolution*, August 2016).

1.2.1. 'Digital asset' International Institute for the Unification of Private Law (UNIDROIT)[5]	'Digital assets' are defined as objects which have value ascribed to them", and are "transferable and, in many cases, designed to be transferred", for instance crypto-tokens in a blockchain context.	• Digital assets, such as crypto-tokens, are *constituted by* data but *different from* such data. The persistency of digital assets – which makes them suitable for transactions – is precisely achieved because data constituting them change in a transient manner.
1.2.2. Computer program or software Computer Program Directive[6]	Software functionally defined as a set of instructions to computers in order to obtain a certain result.[7]	• Software are *constituted by* data or, in other words, they are in digital form, especially when not on a tangible support.
1.1.1. Database Database Directive[8]	A database is "a *collection* of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (emphasis added).	• Databases are both *constituted by* data and they *include* data. • The connection between data and databases is therefore particularly close. This is all the more true when the *sui generis* legal protection afforded to databases makers is applicable. The legal protection indeed extends to the prevention by the database maker of unauthorized extraction and/or reutilization of the whole of substantial parts of the *data* y third parties. The scope *rationae materiae* of the protection extends not only to the database but also, therefore, to some extent, to its content, namely data.
1.1.2. Digital service Consumer Sale of Goods Directive[9] and the Digital Content Directive[10]	Under EU consumer law (and for the purpose of consumer protection), digital services are • either "a service that allows the consumer to create, process, store or access data in digital form; • or a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service".[11]	• Digital services are activities conducted in the digital environment and related to data but they do not constitute the provision of data *as such.* • However, the distinction between the two is not always clear in practice, as visible with the example of a digital service consisting in "the continuous supply of traffic data in a navigation system", in the Consumer Sale of Goods Directive.[12] The service consists indeed here in the continuous provision of data *as such,* in which case it can be equated with 'data'. This illustrates the fact that data can be provided either as a good (imitating sales or lease contract) or as a service, i.e. consisting in the continued provision of a data stream.

[5] Digital Assets and Private Law Working Group, Issues Paper, Study LXXXII – W.G.1 – Doc. 2, November 2020, para 38-39.
[6] Directive 2009/24/EC on the legal protection of computer programs, OJ L 11116.
[7] See WIPO, https://www.wipo.int/wipo_magazine/en/2008/06/article_0006.html
[8] Directive 96/9/EC on the legal protection of databases, OJ L 77/20, Art. 1(2).
[9] Directive (AU) 2019/771 on certain aspects concerning contracts for the sale of goods […], OJ L 136/28, 'Consumer Sale of Goods Directive'.

1.1.3. Digital content Digital Content Directive and the Consumer Sales of Goods Directive.	Digital content consists in "data which are produced and supplied in digital form".[13] While this definition would seem to simply equate 'digital content' with 'data (as such)', the term 'content' rather points to the semantic content of the (aggregation of) data, namely to *something* provided in a digital form and not to the data *as such*. This is confirmed, first, by the examples provided in the Digital Content Directive (although it is sometimes unclear whether they refer to 'digital content' or to 'digital service') such as computer programmes, applications, e-books, audio files, video files.[14] Second, this interpretation is indirectly confirmed by Art. 2(1) which refers to the situation where consumers would provide "personal data" in exchange for the supply of, *i.a.,* digital content, endorsing a distinction between the two notions.	• The notion of 'digital content' is particularly broad and imprecise. It seems to encompass other notions related to digital 'something'. These characteristics are seemingly related to the objective of the Directives, namely to protect consumers online, while many different types of transactions may be taking place. • Digital assets (as defined by UNIDROIT, see above) such as crypto-tokens for instance, could qualify as digital content, in the sense that they are constituted by data but the core of what they are lies in the content of the data, in the 'something' made of data, rather than in the data *as such*.

1.1.4. Conclusion

Data are heterogeneous, since every information can be turned into 'data'. From the legal perspective, what matters is to distinguish data *as such* from 'something in digital form', although sometimes difficult in practice. The distinction between data and 'digital something' can only be made *in concreto* and it should be contextual rather than essentialist. Indeed, the very same data could be used as data *as such* in a case while as a building block for a 'digital something' in another case.

To bring clarity, the ELI-ALI Principles for a Data Economy[15] distinguish data as such from two other types of data or, said otherwise, other types of cases where data are used for a different purpose:

- 'Functional data' are data which perform certain functionalities such as a computer program or software;

[10] Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136/1, 'Digital Content Directive'.
[11] Digital Content Directive, Art. 2(2) and Consumer Sale of Goods Directive, Art. 2(7).
[12] Consumer Sale of Goods Directive, Rec. 14.
[13] Consumer Sale of Goods Directive, Art. 2(6) and Digital Content Directive, Art. 2(1).
[14] Digital Content Directive, Rec. 19. See also the Proposal from the EC for a Directive on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final, Art. 2(1). The lack of clarity on the distinction between 'digital content' and 'digital service' can be traced back to the Proposal from the EC, which inserted data-related services as 'digital content'.
[15] Neil Cohen and Christian Wendehorst, Principles for a Data Economy, ELI final Council Draft, American Law Institute ('ALI') and European Law Institute ('ELI'), 2021 (*not yet approved by ELI membership).* https://principlesforadataeconomy.org/fileadmin/user_upload/p_principlesforadataeconomy/Files/Principles_for_a_Data_Economy_ELI_Final_Council_Draft.pdf (last visited 29th November 2021), 23.

- ‘Representative data’ are data which represent something else that “the value inherent in the information recorded”, such as cryptocurrencies or more generally digital assets as defined by UNIDROIT (see above).

Neither ‘functional’ nor ‘representative’ data shall make part of the scope of this study.

1.2. The notion of ‘data’ in EU law

This section aims to clarify the notion of ‘data’ in EU law, through the study of a list of definitions of (certain types of) data, with a focus on transport and more specifically on the railways. Increasingly used in EU legislation, the term ‘data’ is not granted a uniform definition. While this is understandably related to the respective different regulatory objectives of the pieces of legislation, this may cause interpretation issues but also over-expectations.[16] EU law refers not only to ‘data’ in general but also to specific types of data. The challenges identified in sections 1.1 and 1.2 to delineate ‘data’ from neighbouring notions are also present in EU law, which the following list of definitions of data illustrates.

Notion + source	Definition	Comments

[16] On the (over?-)expectations of the EU law-maker to create a ‘data law’, see Charlotte Ducuing, ‘The Regulation of “Data”: A New Trend in the Legislation of the European Union?’ (*CITIP blog*, 6 April 2021) <https://www.law.kuleuven.be/citip/blog/the-regulation-of-data-a-new-trend-in-the-legislation-of-the-european-union/> accessed 19 November 2021.

1.2.1. **Personal data'** Data protection law (see in particular GDPR, Art. 4(1))[17]	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	• The definition of 'personal data' calls for many interpretation comments, which are beyond the ambit of this study. It is notoriously broad in scope and the determination of what qualifies as 'personal data' is *contextual* and even *situational:*[18] it depends *i.a.* on the (material, technical and organizational) means at the disposal of the data controller to identify individuals. This means that data are not personal *per se.* Data can simultaneously qualify as 'personal' *and* 'non-personal', depending on who processes data and how. • Personal data is defined by reference to 'information' and to the ability to create a link to individuals. This is the reason why personal data is often said to refer, at least in part, to the semantic level of information, namely the *content of information.*[19] • 'Personal data' can take many forms and does not necessarily take the form of a set of bits and bytes (cf. ISO definition).
1.2.2. 'Non-personal data' Free Flow of Non-Personal Data Regulation ('FFNPDR', Art. 3(1))[20]	'Data' means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679. Then the term 'non-personal data' is used in the FFNPDR (see Art. 2(2), 8(1)(a) and (3)). Rec. 9 provides examples of 'non-personal data', such as "aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines".	• The definition of 'non-personal data' is a negative one, namely by reference to the GDPR notion of 'personal data'. Given the characteristics of the notion of 'personal data' (see above), regulating 'non-personal data' by contrast is challenging.[21]

[17] 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, OJ L 119/1.

[18] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40, 40.

[19] Josef Drexl, 'Data Access and Control in the Era of Connected Devices - Study on Behalf of the European Consumer Organisation BEUC' 2018 <https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf>.

[20] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303/59.

[21] For further developments on this see Charlotte Ducuing, Lidia Dutkiewicz and Yuliya Miadzvetskaya, 'Legal and Ethical Requirements (TRUSTS Trusted Secure Data Sharing Space)' (2020) 6.2 40–44.

1.1.1. Computer data Cybercrime Directive (Art. 2(b))[22]	'Computer data' means a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function.	• In the digital environment, Cybercrime Directive can already be considered as an 'old' piece of legislation. The wording 'computer data' is nowadays often replaced with 'digital data' or simply 'data'. • The definition of 'computer data' under the Cybercrime Directive encompasses both data representing facts and information and data playing a role in the operation of a programme. • Recent policy and legislative instruments are concerned with the economic value of 'mere' or 'raw' data, namely data *as such* (thereby excluding data playing a role in the operation of a programme). However, the Cybercrime Directive is concerned with the protection of data, and more generally, of IT systems, against illegal interference, which explains the broad scope of the notion of 'computer data'.
1.1.2. **'Data'** Data Governance Act Proposal ('DGA proposal')**[23]**	'Data' is defined by the DGA proposal as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording".[24]	• This definition is particularly broad. In particular, the notion of 'compilation' is undefined and unclear. Whether it refers to *i.e.* databases, aggregation of data or to something akin to 'digital content' (see above) remains an open question at the stage of the proposal from the EC. • As it stands, the definition of 'data' in the DGA proposal may thus encompass not only 'data' in the ISO sense (see above) but also 'things' in digital form (see above), which raises many questions.[25]
1.1.3. 'Document' and 'data' Open Data Directive and DGA proposal (Chapter III)	Under the Open Data Directive, 'document' is defined as "(a) any content whatever its medium (paper or electronic form or as a sound, visual or audiovisual recording); or (b) any part of such content".[26] The notion of 'data' is not defined as such in the Open Data Directive. However, *specific kinds of data* are defined, namely "research data", "dynamic data" (see above) and "high-value datasets". For, respectively, the three notions, 'data' is equated with 'document'.[27]	• Traditional object of the (PSI Directive[28] as recast by the) Open Data Directive is the "document", which should be made available for reuse by public sector bodies ('PSBs'). However, the notion of 'data' has become increasingly prominent. This is particularly visible with the Open Data Directive but also with the DGA proposal (see Chapter II, which aims to complement the Open Data Directive). • This results in a risk of inconsistency between the Open Data Directive and the DGA proposal.[29] • This may also point to a 'data-mania' in PSI and Open Data legislation. Data, as a trendy term, seems to have overshadowed the daunting 'document'. This example should warn against the 'newness' of data-related legislation, which may sometimes merely consist in a rebranding of outmoded terms.[30]

[22] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218/8.
[23] European Commission, Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act), COM(2020) 767 final ('DGA proposal').
[24] DGA proposal, Art. 2(1).

[25] For further discussion on this, see Julie Baloup and others, 'White Paper on the Data Governance Act' (Social Science Research Network 2021) SSRN Scholarly Paper ID 3872703 <https://papers.ssrn.com/abstract=3872703> accessed 21 November 2021.

[26] Directive (EU) 2019/1024 on open data and the re-use of public sector information, OJ L 172/56 ('Open Data Directive').

[27] Open Data Directive, Art. 2(8) (9) and (10).

[28] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, OJ L 345/90 ('PSI Directive').

[29] This topic is further is discussed in Baloup and others (n 22) s 3.2.

[30] On this, see Ducuing (n 13).

1.1.4. 'Dynamic data' Open Data Directive and in the ITS Directive ecosystem	The notion of 'dynamic data' is defined in the Open Data Directive as "documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data".[31] See in the ITS Directive ecosystem:[32] - Under Commission Delegated Regulation (EU) 2017/1926/EU on the provision of EU-wide: 'dynamic travel and traffic data' is defined as "data relating to different transport modes that changes often or on a regular basis […]".[33] And - Under Commission Delegated Regulation (EU) 2015/40/EU: 'dynamic road status data' is defined as "road data that change often or on a regular basis and describe the status of the road […]".[34]	• In both the Open Data Directive and in the ITS Directive ecosystem, dynamic data are defined as data that change frequently. The Open Data Directive definition even mentions the "volatility" of data as an explanation. • The dynamic – or volatile – character of data however logically implies that the data (within the ISO meaning of the term as bits and bytes) would *not be the same.* • The expression "dynamic data" seems to rather point to a data *stream*, which is implicit with the reference to "data generated by sensors" in the Open Data Directive definition. •
1.1.5. **ITS types of data** ITS Directive ecosystem (*i.e.* including delegated acts adopted under the ITS Directive)	The ITS Directive ecosystem refers to a number of specific types of data, such as: - "Traffic data", defined as "data on road traffic characteristics" which are further listed in the Annex of the Commission Regulation (EU) 2015/962/EU;[35] and - "Historic traffic data", defined as "traffic characteristics depending on the hour, day, season based on previous measurements, including rate of congestion, average speeds, average travel times", which are further listed in the Annex of the Commission Regulation (EU) 2017/1926/EU.[36]	• 'traffic data' and 'historic traffic data' (among many others) are the object of data access regulations. Both are defined following the *semantic level,* namely the information conveyed. • This illustrates concretely how the syntactic and the semantic level are closely related with data and information. Very often, data are *regulated as* sets of bits and bytes but *because of* the semantic content.

[31] Open Data Directive, Art. 2(8).
[32] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJ L 207/1 ('ITS Directive').
[33] Commission Delegated Regulation (EU) 2017/1926 of 31 may 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services, OJ L 272/1, Art. 2(7).

[34] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services, OJ L 157/21, Art. 2(7).

[35] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services, OJ L 157/21, Art. 2(8).

[36] Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services, OJ L 272/1, Art. 2(14).

1.1.6. 'Real time data' New PRR	The New PRR introduces the notion of 'real-time data', namely 'real-time data relating to the arrival and the departure of trains'.[37] The notion is however not defined. However, 'real time data' is manifestly linked to the semantic level, namely to the type of information conveyed (information about arrival and departure of trains).	The absence of a definition for 'real time data' raises a number of questions. • First, does it include disruptions and delays? It would seem logical that it does. The added-value of *real-time* data (compared to planned data, in the parlance of the TAF and TAP TSIs) lies precisely in such data. • The distinction between 'real-time data' (to be provided by IMs under the circumstances as per Art. 10(1) and 'real-time travel information' (Art. 9(3)). It follows from the spirit of the New PRR and of railway law more generally that (real-time) travel information are elaborated by RUs (and provided by them to the beneficiaries pursuant to Art. 9) *based on* real-time data stemming from IMs. • On the link between 'real time data' under the new PRR and TAP TSI, see below.
1.1.7. TAF & TAP TSIs notions: 'data', 'message', 'information'	The TAP and TAF TSIs refer to mainly three types of neighbouring notions: - Data - Message - Information There is no definition of such notions,[38] which are closely connected. "Message" is equated with "data element". Messages consist in two data sets: control data defined "through the mandatory message header of the messages of the catalogue" on the one hand, and "information data" defined "by the mandatory / optional content of each message and mandatory / optional data set in the catalogue".[39]	• The distinction between 'message', 'data' and 'information' is not always clear in TAF and TAP TSIs. When analyzing 'data regulation' in the railways, the three notions should therefore be taken into account. The link between 'real-time data' (New PRR) and the TAP TSI: • In principle, the New PRR and TAP TSI should have close connections. Especially, TAP TSI should provide for "more detailed requirements" on travel information (see New PRR, Rec. 13), and especially more *technical* requirements as for the modalities under which information should be exchanged.[40] • However, the absence of a definition for 'real-time data' in the New PRR and the diverging vocabulary used in the TAP TSI raise the question which concrete sections of the TAP TSI provide for "more detailed requirements". • TAP TSI does indeed not explicitly refer to 'real-time data [relating to the arrival and the departure of [passenger trains]. • As for the real-time character, TAP TSI does not explicitly refer to "real-time data [relating to the arrival and the departure of [passenger] trains]". The wording "up to date data" is used to refer to "up-to-date timetable data" (point 4.2.1) that the RU shall exchange. As for the semantic level, it would seem that point 4.2.15 (Train running information and forecast) and/or point 4.2.16 (Service disruption information)) are in line with 'data relating to the arrival and the departure [of passenger trains]'.

1.1.8. Conclusion

The notion of 'data' is not provided with a harmonized definition in EU law. The word 'data' should therefore be approached with care. Especially, the following should be kept in mind:

- The distinction between 'data' (as sets of bits and bytes) and 'information' (the semantic content conveyed by data) is often blurred;
- 'Data' is sometimes used as a proxy for approaching objects, such as data streams or data sources;
- The definition or, failing that, the meaning of data depends on the *ratio legis* of the legal framework at stake;
- Finally, 'data' has become a fashionable term, which tends to be over-used in EU legislation, with the risk of further obscuring its meaning.

2. The regulation of 'data'

As discussed in Part I, data are heterogenous. They are used for a great variety of purposes and in different contexts. Inquiries about the legal status of data are closely related to the *use* of data *as a good or commodity with economic value in the data economy*. This results in two main observations. First, the legal analysis shall be targeted at data in their new function as an object of economic value rather than analyzed in the abstract. Second, enquires (Same issue here) about the legal status of data as an object of value – or about rights related to data – is a rather new phenomenon. On the one hand, the law – and particularly EU law - is adapting to this new reality. But on the other, data are inevitably affected by existing legal frameworks designed in the past for different purposes and with different objects, resulting in a legal patchwork. This in turn leads to a feeling of misalignment between economic and social practices – using data as a valuable commodity – but the law generally not endorsing the commodification phenomenon. The misalignment can be captured in the – wrongly but often-asked - question "who owns [a certain type of] data?", which displays the implicit view that data *is or should be owned.*

Against this background, the present part aims to present the legal frameworks applicable to data as an object of economic value. Given that several legal frameworks are potentially applicable to data. it does neither claim to be exhaustive, nor comprehensive, but merely attempts to provide an overview of the various legal frameworks and how they apply to data.

Where appropriate, reference is made to the specific context of RNE data ecosystem, and particularly to the TIS data ecosystem as an illustration.[41] For the purpose of this study, the TIS data ecosystem of RNE is summarized by Figure 1.

[37] Regulation (EU) 2021/782 of the European Parliament and of the Council of 29 April 2021 on rail passengers' rights and obligations, OJ L 172/1 ('the New PRR'), Art. 10(1). The New PRR is applicable as from 2023.

[38] Commission Regulation (EU) No 1305/2014 of 11 December 2014 on the technical specification for interoperability relating to the telematics applications for freight subsystem of the rail system in the European Union and repealing the Regulation (EC) No 62/2006, OJ L 356 12.12.2014/438 ('TAF TSI' as consolidated), See in particular in Appendix II, Glossary. Commission Regulation (EU) No 454/2011 of 5 May 2011 on the technical specification for interoperability relating to the subsystem 'telematics applications for passenger services' of the trans-European rail system, OJ L 123 12.5.2011/11 ('TAP TSI' as consolidated), Point 8 (Glossary).

[39] TAF TSI, Point 4.2. (Functional and technical specifications of the subsystem).

[40] See also the scope of TAP TSI, Point 2.1.

[41] https://tis.rne.eu/

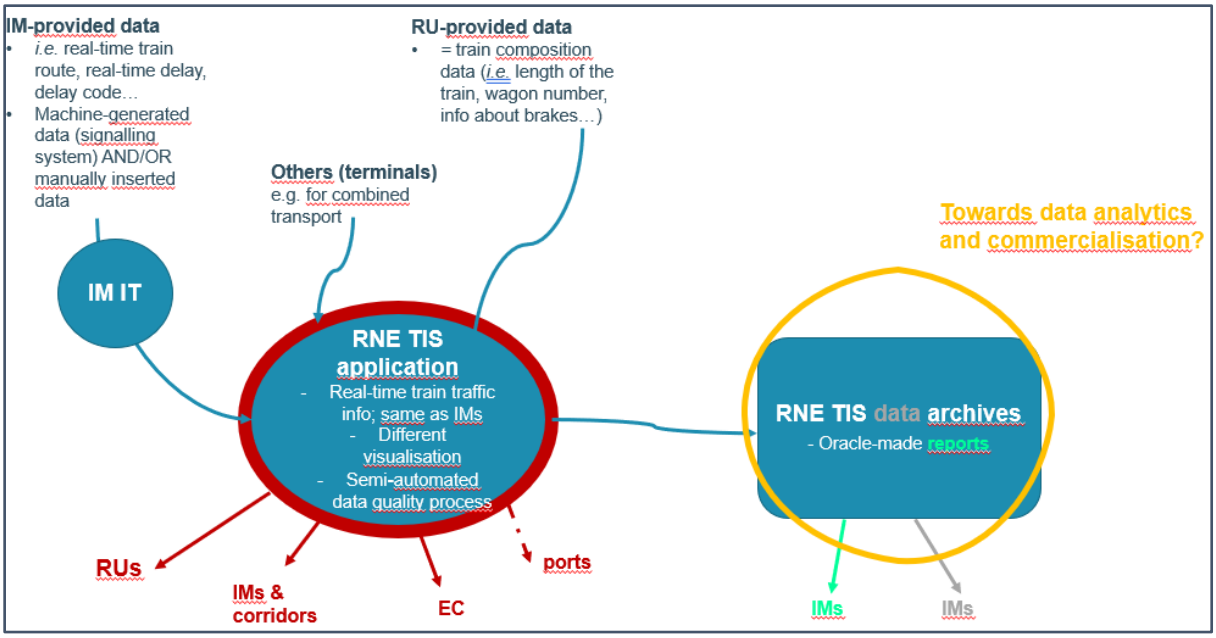


Figure 1 – TIS data ecosystem of RNE

The first section introduces the legal frameworks applicable to objects other than data, but which can have an influence on the processing of data as an object of economic value. The second section enquires about legal frameworks applicable or potentially applicable to data as an object of economic value, both *lex generalis* and more specifically legislation concerning transport data. The third section examines prospective regulation of data as an object of economic value, since 'data law' is still law in the making. Finally, the fourth section discusses a scholarly proposal made by the European Law Institute ('ELI') and the American Law Institute ('ALI') to regulate data as an object of economic value in the data economy, with a more specific focus on how it could apply to RNE and RNE data.

2.1. Legal frameworks indirectly influencing data[42]

2.1.1. *Sui generis* database protection

EU law provides for a specific legal protection granted to "makers" of certain databases, namely "collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means".[43] The maker is the "person who takes the initiative and the risk of investing".[44] The criteria for the protection consist in "qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents".[45] The 'obtention' [of data] refers to "the act of gathering [the data] to be included in the database". The obtention of data should not be confused with the *generation* of data.[46] 'Verification'

[42] This section is inspired by Charlotte Ducuing, 'D4.5 – Legal Aspect for Smart Contract Adoption' (In2Dreams 2018) Deliverable 38–64.

[43] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20 ('the Database Directive'), Chapter III.

[44] Database Directive, Rec. 41.

[45] Database Directive, Art. 7(1).

[46] The CJEU ruled that the investment in the obtaining of the contents refers to "the resources used to seek out *existing materials* and collect them in the database but does not cover the resources used for the creation of materials which make up the contents of a database" (emphasis added), see *i.a.* Fixtures Marketing Ltd v Oy Veikkaus Ab, ECJ 9 November 2004, case C-46/02, ECLI:EU:C:2004:694, para. 34. This distinction between the

refers to "the checking, correcting and updating of data already existing in the database". Finally, 'presentation' refers to "acts such as digitizing (scanning) analogue files or creating a thesaurus".[47] The investment must thereby concern the database itself rather than the creation of "independent material" (*i.e.* data).[48] However, drawing the line between the two is difficult in practice.[49]

The database *sui generis* protection granted by the Database Directive is the legal framework in EU law that is the closest to a protection of 'data' as such. Indeed, the rights afforded to the database maker extend to the *contents* of the database. The maker may prevent unauthorized extraction and/or reutilization of the whole or substantial parts of the data by third parties,[50] albeit subject to 'first sale' exhaustion.[51] "Extraction" is defined as "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form".[52] "Re-utilization" is defined as "any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by online or other forms of transmission […]".[53] In contrast, extraction of *non-substantial parts* of the database and/or reutilization of the data or mere consultation of a database are *not* protected. Constant availability of data sources may be found to constitute substantial reutilization.[54] In contrast, the extraction or reutilization of individual datasets should not require the maker's prior authorization.

Not all databases are the object of the *sui generis* protection. Protection depends on the extent (both in terms of quality and quantity) of the investment *specifically* made in the making of the database – rather than in the data themselves. While this calls for *in concreto* legal analysis, it is notoriously difficult to determine whether a database is protected or not, considering also the absence of a registration system. Similarly, the extent of the activities protected under the *sui generis* legal regime is difficult to determine in practice, *i.e.* what shall be deemed "a substantial part" of a given database.[55]

In line with the general principles of intellectual property law, the *sui generis* protection of databases is for a limited period, namely fifteen years. However, this term runs as from the "date of *completion* of the making of the database" (emphasis added).[56] But databases are often dynamic and ever evolving

obtaining and the generation of data is justified by the *ratio legis* of the *sui generis* protection of databases, namely to "promote the establishment of storage and processing systems for existing information and not the creation of materials capable of being collected subsequently in a database" (ibid).

[47] P Bernt Hugenholtz, 'Data Property: Unwelcome Guest in the House of IP', *Paper presented at Trading Data in the Digital Economy: Legal Concepts and Tools* (2017) 7–8.

[48] Case C-46/02, Fixtures Marketing Ltd v Oy Veikkaus Ab, 9 November 2004, ECLI:EU:C:2004:694, para 30-40; case C-203/02, The British Horseracing Board Ltd and Others v William Hill Organization Ltd, 9 November 2004, ECLI:EU:C:2004:695, para 25-36.

[49] Ivan Stepanov, 'Introducing a Property Right over Data in the EU: The Data Producer's Right – an Evaluation' (2020) 34 International Review of Law, Computers & Technology 65, 71. See also Alain Strowel, 'Chapter 6: Big Data and Data Appropriation in the EU', *Research Handbook on Intellectual Property and Digital Technologies* 122–123.

[50] Database Directive, Art. 7(1).

[51] Database Directive, Art. 7(2)(b).

[52] Database Directive, Art. 7(2)(a).

[53] Database Directive, Art. 7(2(b).

[54] Case C-202/12, Innoweb v. Wegener ICT Media, 19 December 2013, ECLI:EU:C:2013:850, para 23-54.

[55] As identified by I. Stepanov, the large quantities of data processed in the Big Data economy would often amount to substantial extraction and/or reutilization of databases contents, typically from a *quantitative* perspective, Stepanov (n 8) 71.

[56] Database Directive, Art. 10.

so that they can never (or hardly ever) be considered fully completed. Consequently, the *sui generis* legal protection of databases can extend indefinitely , so long as investment is made in the database.[57]

Finally, the Database Directive protects lawful users of databases *made available to the public* against restrictions imposed by the makers to database use not covered by exclusivity rights. Concretely, lawful users should not be prevented by the maker (*i.e.* contractually) from extracting and/or reusing insubstantial parts of the contents of the database, irrespective of the purpose.[58] Such provision is applicable only with respect to databases made available to the public (*i.e.* via an internet website available to the general public).

Guidance for RNE -

- Subject to *in concreto* analysis, (some of the) RNE databases can be protected under the *sui generis* protection of databases.
- Data streams to data users (qualifying as extraction), where appropriate, could therefore require RNE's the prior consent.
- Similarly, data streams feeding TIS (*i.e.* from IMs IT systems) could require prior consent of the database maker(s), subject to *in concreto* analysis. The *same* data transferred on an ad hoc basis would not be protected under the *sui generis* legal protection of databases.

2.1.2. Copyright

The 'Infosoc Directive',[59] as recently complemented and revised by the Digital Single Market Directive,[60] harmonizes certain aspects of copyright (or 'droit d'auteur') protection. Copyright protection does not apply to 'data' but to 'works', expressed in a form and vested with originality. Originality implies that the work expresses the author's own intellectual creation by making free choices.[61] The right holder – namely, the author – can enforce his/her rights against any infringing third party (*erga omnes* effect).

The rights of the author can be divided into two types:

[57] See the Database Directive, Art. 10(3).

[58] Database Directive, Art. 8. As a result of this provision, as interpreted by the CJEU in case C-30/14, Ryanair v PR Aviation, 15 January 2015, ECLI:EU:C:2015:10, makers of databases *not* eligible to the *sui generis* protection paradoxically have a broader room of manoeuvre to (contractually) restrict the use of their databases than makers of databases protected under the *sui generis* protection.

[59] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167/10 ('the InfoSoc Directive').

[60] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130/92 ('Digital Single Market Directive').

[61] Case C-5/08 Infopaq International A/S v Danske Dagblades Forening, 16 July 2009, ECLI:EU:C:2009:465, para 36-39; case C-145/10 Eva-Maria Painer v Standard
VerlagsGmbH, Axel Springer AG, Süddeutsche Zeitung GmbH, Spiegel-Verlag Rudolf Augstein GmbH & Co KG, Verlag M. DuMont Schauberg Expedition der Kölnischen Zeitung GmbH & Co KG, 1st December 2011, ECLI:EU:C:2011:798, para 88-93.

- Moral rights, if provided under national law.[62] Moral rights include at least the rights of paternity and integrity of the work.
- Economic rights, which are harmonized by EU law. They consist of the exclusive rights of reproduction, communication to the public and distribution. In contrast to moral rights, economic rights are assignable and transferable.

Rights of authors are not absolute. They are subject to exceptions and limitations that are partially harmonized in EU law, such as the time limitation of the rights, the exhaustion of the exclusive right of distribution through the first sale or equivalent transfer of ownership, and the list of optional exceptions that Member States can adopt pursuant to Art. 5 of the InfoSoc Directive. The Digital Single Market Directive adds new exceptions for 'text and data mining'.[63]

Guidance for RNE -

- Data as such cannot be protected under copyright as they lack originality.
- However, copyright can play a role in data processing environments, subject to *in concreto* legal analysis. *I.e.* can be protected by copyright the structure of databases, computer programmes and visualization webpages.

2.1.3. Computer program (software)

The EU formulated specific legislation for the protection of computer programs, the Software Directive[64], which protects computer programs under copyright law as literary works. In accordance with the general principles of copyright protection as mentioned above, protection is granted to the expression, in any form, of a computer program that is original.[65] A 'computer program' covers programs in any form, including those which are incorporated into hardware. It also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage.[66]

Computer programs rely on data, but the protection does not cover ideas and principles which underlie any element of a program, including those which underlie its interfaces. On that basis, to the extent that algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected under the Software Directive.

Guidance for RNE -

- Data as such cannot be protected under the Software Directive.
- In the environment of RNE data, some of the software can be protected under the Software Directive (as transposed in national law).

[62] Moral rights are not harmonized in EU law. They derive from the Berne Convention for the Protection of Literary and Artistic Works, 1886, Art. 6 bis.

[63] See the Digital Single Market Directive, Art. 3 and 4. On the text and data mining exception, see Strowel (n 8) s 3.1.1.

[64] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111/16 ("Software Directive").

[65] Software Directive, Article 1.

[66] Software Directive, recital 7.

2.1.4. Trade secrets

Trade secrets protection is harmonized at EU level by the 'Trade Secret Directive',[67] leaving however significant room for maneuver in for national transposition. The legal protection covers the trade secret defined as "information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret".[68] Industrial and/or "commercial data"[69] could potentially be subject to trade secret protection, subject to national law transposing the Directive,[70] provided reasonable steps have been taken to keep them secret. Trade secrets may be in any form, including digital. The definition of 'trade secret' is particularly broad and does not discuss the semantic content of information. In principle, therefore, any information held by a business could qualify as trade secret, subject to *in concreto* analysis.

The qualification as trade secret depends on the level of openness versus secrecy. When it comes to data, internal data (namely, data not made available to third parties) can be opposed to data produced externally. Stepanov gives the example of connected vehicles, which produce data while driving on open roads.[71] A parallel can be drawn with trains, concerning train traffic data which would only arise from data produced or collected based on the traffic of trains in areas accessible to the public.

Acquiring, using or disclosing trade secrets may qualify as unlawful, depending on the circumstances and the quality of the entity at stake.[72] The disclosure of trade secrets in breach of a confidentiality agreement can qualify as unlawful use or disclosure within the meaning of the Trade Secret Directive.[73] The Directive further prohibits commercial activities (such as the production and placing on the market) of "infringing goods", namely goods "significantly benefit[ing] from unlawful activity regarding trade secrets, when performed with knowledge of the unlawful activity.[74] The Directive provides for extensive remedies to the benefit of the trade secret holder, namely the person "lawfully controlling the trade secret",[75] and enforceable against infringers. Remedies include provisional measures.[76]

Trade secret protection does not amount to property, as the EU lawmaker consciously designed it "in the interest of innovation and to foster competition". The Directive does indeed not create exclusive rights. As a result, "the independent discovery of the same know-how or information should remain possible". Similarly, "reverse engineering of a lawfully acquired product should be considered as a

[67] 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, OJ L 157/1 ('Trade Secret Directive').
[68] Trade Secret Directive, Art. 2(1).
[69] Trade Secret Directive, Rec. 2.
[70] Gintare Surblyte, 'Data as a Digital Resource' (2016) Max Planck Institute for Innovation & Competition Research Paper 16–22 9.
[71] Stepanov (n 8) 72.
[72] Trade Secret Directive, Art. 4.
[73] Trade Secret Directive, Art. 4(3)(b) and (c).
[74] Trade Secret Directive, Art. 2(4) and 4(5).
[75] Trade Secret Directive, Art. 2(2).
[76] Trade Secret Directive, Art. 10.

lawful means of acquiring information […]".[77] Trade secret protection under the Directive is often rather described as a protection of 'possession'.[78]

Finally, the Trade Secret Directive provides for exceptions for reasons pertaining to fundamental rights and freedoms (such as the freedom of expression), subject to a balancing test. It also lays down the conditions under which use, disclosure and acquisition of trade secrets shall be deemed lawful.[79]

Guidance for RNE -

- In the data economy, both data and algorithms could theoretically qualify as trade secrets within the meaning of the Trade Secret Directive, which is agnostic to the form of trade secrets.
- However, there is a broad consensus that 'raw data' are unlikely to qualify as trade secret. While trade secrets are defined, *i.a.*, by the fact that they have commercial value, value is derived from the *aggregation* of data, rather than from individual data.[80]
- In any case, data produced or collected in public areas (*i.e.* general data about train circulations) cannot be considered 'secret' and can therefore not be protected as a trade secret.

2.2. Legal frameworks potentially applicable directly to data

Section 2.1 above deals with general frameworks not initially designed for data. However, the specificities of data are so that the EU legislator increasingly had to adopt data-specific legislation.

This section is divided into two sub-sections: the first one provides an overview of general legal frameworks while the second looks into legal frameworks more specific to the situation of RNE, either because transport-specific or because public sector-specific.

2.2.1. General legal frameworks

2.2.1.1. The Cybercrime Directive

The Cybercrime Directive[81] harmonizes the law of EU Member States concerning "criminal law in the area of attacks against information systems".[82] In particular, the Directive mandates EU Member States to include as criminal offences the following acts:

1. "Access without right to the whole or to any part of an information system […] where committed by infringing a security measure", also known as hacking;[83]

[77] Trade Secret Directive, rec. 16.
[78] As noted by Strowel, the extent and nature of the remedies afforded to trade secret holders are however close to these afforded to owners, in particular concerning the "infringing goods", see Strowel (n 8) 134.
[79] Trade Secret Directive, Art. 3.
[80] Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) 8 JIPITEC; Herbert Zech, 'Data as a Tradeable Commodity' (*European Contract Law and the Digital Single Market: The Implications of the Digital Revolution*, August 2016).
[81] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218/8.
[82] Cybercrime Directive, Rec. 1.
[83] Cybercrime Directive, Art. 3.

2. "Seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right";[84]
3. "Deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right";[85]
4. "Intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right".[86]

The rationale for the creation of *sui generis* criminal offences related to data and information systems lies in their specificities and particularly in the ubiquity of data. For instance, the criminal offence 3 was designed as an alternative to 'data theft'. As a non-rivalrous good, data can logically not be 'thieved', which would, in most (at least civil law) jurisdictions, require a simultaneous deprivation of possession.[87] The fact that specific criminal offences were created so as to find an equivalent to 'theft' that would fit the features of data constitutes one of the arguments invoked to deny the existence of ownership rights on data (on the absence of data ownership, see section 2.2.1.2 below).

Guidance for RNE -

- Subject to national transposition, 'hacking' and/or more serious acts of interference with one' (RNE's) data and computer systems is considered a criminal offence.
- In order to attract the legal protection of the Cybercrime Directive (especially concerning 'mere' hacking), it is necessary – and therefore advisable - to implement security measures.

2.2.1.2. (Intellectual) Property law

The expression 'data ownership' should be understood as "an economic ownership right in data as intangible assets in the form of an exclusive right that enables the right holder to appropriate the economic benefits from the use of these data".[88] 'Who owns [this piece of] data?" is a commonly asked

[84] Cybercrime Directive, Art. 4.
[85] Cybercrime Directive, Art. 5.
[86] Cybercrime Directive, Art. 6.
[87] The question arose for instance in Belgium concerning software. The Court of Appeal of Antwerp had to determine whether software can be the object of a theft. While recognizing that the copy of a software without prior consent of the maker could lead to a decrease in the value of the software, the Court denied the qualification as theft, for lack of a deprivation of possession, Antwerpen, 13 december 1984, R.W., 1985-86, 244-246.
On the contrary, the Highest judiciary court in France (Cour de Cassation) ruled on two occasions that downloading data without the prior consent and will of the data holder constitutes a 'theft', irrespective of – and without even discussion - the absence of deprivation of possession (Cour de Cassation, ch. Crim., 20th May 2015 No 14-81336 and Cour de Cassation, ch. Crim., 28th June 2017 No 16-81113). This case-law is surprising, since theft is defined in French criminal law as the fraudulent deprivation of someone else's property (French Criminal Code, Art. 311-1). These two rulings can be interpreted as recognising implicit ownership rights in data, which was however not discussed head on by the Court.
[88] Josef Drexl, 'The (Lack of) Coherence of Data Ownership with the Intellectual Property System' in Ansgar Ohly and others (eds), *Transition and Coherence in Intellectual Property Law: Essays in Honour of Annette Kur* (Cambridge University Press 2021) s 16.2 Data Ownership as Intellectual Property. The term "ownership" should be preferred over "property rights", which, in common law countries, may encompass more generally "rules governing access to and control of […] resources", Jeremy Waldron, 'Property and Ownership' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Summer 2020, Metaphysics Research Lab, Stanford University 2020) <https://plato.stanford.edu/archives/sum2020/entries/property/> accessed 23 November 2021.

question, in different sectors where valuable data are at the crossroads of many stakeholders. Such question starts from the implicit premise that there is, or should be, a right of ownership on data and all that remains to be done is identify the owner in the network of stakeholders who have somehow played a role in the creation of data. Arguments in favor of recognizing a data ownership right would typically start with the premise that, as valuable resources in the data economy, data *ought to be protected* as property.[89] The absence of ownership rights would amount to a gap in the protection of the patrimony of one.[90] As highlighted by C. Straker, individual property has become so important in our society that it is perceived as "natural or self-evident".[91] Because of their specific features, data however challenge the naturality of individual property.

This section is divided into three sub-sections. The first sub-section identifies the technical and societal changes specific to the data economy which triggered the revival of the 'data ownership' debate in recent years. The second sub-section introduces the 'data producer's right' that the European Commission contemplated to propose in 2016. It was eventually abandoned, following strong opposition by stakeholders' representatives and by scholars. In any case, it constitutes a concrete example of what data ownership could have been. The third sub-section summarizes some of the main legal obstacles that prevent data ownership. It is beyond the ambition of this study to engage into a detailed analysis of all Member States' national law . However, some examples from national laws and national case law are used for illustrative purposes.

Problem statement: From the abstraction to the commodification of data

The debate on whether there is or should be 'data ownership' rights is not entirely new. It has surfaced at every stage of the growth of the digital world and from various entry points. For instance, until specific protection was granted to owners of computer programs (software), courts have been called to decide whether software is protected as property.[92] Similarly, courts have been called to decide whether an unauthorized copy of data can be considered as "theft". Whether personal data are or should be protected as property has also been a recurring debate, mainly in the US but also in Europe.[93] The emergence of online gaming communities with dedicated virtual assets and, then, blockchain assets has again raised the question whether, this time, rival, digital assets can be protected as property.[94]

The 'data ownership' debate was recently revived with the emergence of the data economy. What is new with the data economy is the "abstraction of data", leading in turn to the commodification of data, as identified by Zech. The abstraction of data refers to the process by which information becomes

[89] Ducuing (n 1) 26–29.

[90] For a critical review of the arguments often invoked in favour of a data ownership rights, see *i.a.* Hugenholtz (n 6); Strowel (n 8); Drexl (n 39); Drexl (n 47).

[91] Christian Straker, 'From Data Property to Data Rights: Legal Thoughts on Basic Principles of the European Digital Economy in the Age of Big Data' (2018) 70 Revue du Droit des Technologies de l'Information (RDTI) 63, 63.

[92] See for instance in Belgium, Antwerpen, 13 december 1984, R.W., 1985-86, 244-246.

[93] Václav Janeček, 'Ownership of Personal Data in the Internet of Things' (2018) 34 Computer Law & Security Review 1039;

[94] The debate has spurred not only in Europe but also in the US and, particularly concerning "virtual property" in Asia, see W Erlank, 'Introduction to Virtual Property: Lex Virtualis Ipsa Loquitur' (2015) 18 PER: Potchefstroomse Elektroniese Regsblad 2525; Joshua Fairfield, 'Virtual Property' (2005) 85 Boston University Law Review 1047; Kelvin FK Low and Ernie GS Teo, 'Bitcoins and Other Cryptocurrencies as Property?' (2017) 9 Law, Innovation and Technology 235.

"something 'on its own' and therefore […] an object". This phenomenon results from the separation of information from four elements traditionally associated with them:

- A physical carrier, which is for instance visible with the increasing recourse to cloud computing.
- A human creator: data are often generated by machines (see the notion of "machine-generated data" below) in the Internet of Things ('IoT') environment.
- A specific meaning: in the Big Data paradigm, the meaning of information becomes less important as the quantity of data increases and allows to identify patterns.
- A potential human recipient:[95] this trend has only accelerated with artificial intelligence ('AI'), which requires data as an input.

The abstraction of information translates into the *commodification* of data in the data economy as an economic consequence.[96] The OECD defines commodities as "goods and services normally intended for sale on the market at a price that is designed to cover their cost of production".[97] Zech goes as far as to consider that treating data as a commodity, or as a good, lies at the heart of the data economy.[98] Commodification refers to the evolution (of data in this case) into valuable business assets and commodities, often traded as such between companies.[99] The commodification of data should not be viewed in isolation. This phenomenon takes place as part of a broader trend of commodification of knowledge, where knowledge is perceived and used as a means to create innovation and economic growth.[100] The commodification of data has been mainly visible with personal data traded away (almost willingly and/or consciously) by individuals in 'exchange' for online 'free services' (phenomenon referred to as "personal data as counter-performance").[101]

Both phenomena of abstraction and commodification of data have made prior arrangements on the allocation of data obsolete. For example, the so-called "cyberproperty" approach,[102] present to some extent in many national jurisdictions, considers that the ownership of the physical data carrier extends to the data *stored in it.* Based on the observation that data – as bits and bytes - are physically stored in the data carrier, the cyberproperty approach goes that they constitute a component of the latter.[103] Data are thereby viewed as ancillary to the physical device and data carrier. However, the dissociation

[95] Herbert Zech, 'Information as Property' (2015) 6 Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 192, s 1.1.1.

[96] Jathan Sadowski, 'When Data Is Capital: Datafication, Accumulation, and Extraction' (2019) 6 Big Data & Society 2053951718820549, 2.

[97] The OECD Economic Outlook: Sources and Methods, 'Commodities', available at: http://www.oecd.org/economy/outlook/sources-and-methods.htm (last visited 18th March 2021).

[98] Zech (n 39) 58.

[99] Koen Swinnen, 'Ownership of Data: Four Recommendations for Future Research' (2020) 5 Journal of Law, Property, and Society 139, 143.

[100] Geneviève Azam, 'La connaissance, une marchandise fictive' (2007) n° 29 Revue du MAUSS 110. More generally and with a focus on the role of innovation in the 'knowledge (or 'information') economy', see Marko Ampuja, 'The New Spirit of Capitalism, Innovation Fetishism and New Information and Communication Technologies' (2016) 23 Javnost - The Public 19.

[101] Damian Clifford, Inge Graef and Peggy Valcke, 'Pre-Formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' (2019) 20 German Law Journal 679.

[102] In the parlance of the US scholar Fairfield, see Joshua AT Fairfield, 'BitProperty' (2014) 88 Southern California Law Review 805, 839.

[103] For an analysis of Dutch and Belgian law on this, see Swinnen (n 58) 158. Such approach was for instance endorsed by the Higher Regional Court of Karlsruhe in Germany in 1995, OLG Karlsruhe, Urt. v. 07.11.1995 – 3 U 15/95.

between data and the physical carrier, with the joint effects of the IoT and cloud computing, makes the cyberproperty approach demonstrably obsolete.

The aborted data producer's right

The 2016 communication 'Building a European Data Economy' ,[104] accompanied by the Staff Working Document 'on the Free Flow of data […]',[105] constitutes the first document in which an EU institution lays down comprehensive policy orientations explicitly dedicated to the regulation of data as an economic resource. One of the options envisaged by the European Commission consists in the creation of a "data producer's right", namely, in its further-reaching dimension, a form of ownership right on data.

The EC approaches the regulation of data as an economic resource by deploring the lack of available data for companies to use, to the detriment of the data economy. Data remain too often with the data holder and are therefore used only in silo while they have the potential to generate value when made reusable for other purposes.[106] The fact that some market players, and especially manufacturers and service providers, become "*de facto* owners" of machine-generated data is viewed by the EC as the illustration of a gap in the regulatory framework, namely the absence of legal protection of data and the existence of unequal negotiation positions (especially between businesses and consumers).[107] In other words, the EC considers *de facto* "ownership" of data as an interference with the principle of fairness in business.

The option to introduce a "data producer's right for non-personal or anonymized data" [108] particularly garnered the attention of scholars. Grounded in proprietarianism, the option to create *sui generis* ownership(-like) rights on data was generally opposed by the economic and the legal scholarship and ultimately abandoned by the EC. The remainder of this sub-section introduces the data producer's right option, with a focus on its *ratio legis.*

In terms of scope, personal data are excluded given the protection that are awarded as a fundamental right under the GDPR. The Commission Staff Working Document confirms this as it considers that the GDPR grants natural persons "control of their own personal data".[109] In contrast, the "absence of legal protection in relation to non-personal or anonymized machine-generated data not yet structured in a protected database" is viewed as a gap lacking legal certainty. A data producer's right would protect the syntactic level of data (not the semantic level) as well as the related metadata. The data producer's right would be backed by technical measures to trace the provenance of data and prove the existence of rights (digital watermarks).

The EC envisaged two options. First, an *in rem* right to exploit data and to exclude others from using them. The EC recognized the challenge in identifying a fair right holder while several parties may have contributed in some way in the generation of the data. The Commission SWD identifies "investment in

[104] European Commission, 'Communication Building a European Data Economy' (2017).
[105] Staff Working Document 'On the free flow of data and emerging issues of the European data economy accompanying the Communication 'Building a European data economy' 2017 (SWD/2017/02 final).
[106] European Commission (n 63) 9–10.
[107] ibid 10–11.
[108] European Commission, 'Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy - Accompanying the Document "Communication Building a European Data Economy"' (2017) 33–36.
[109] Such objective of the GDPR could be deduced from recital 7 GDPR, according to which "[…] Natural persons should have control of their own personal data […]", European Commission (n 67) 33.

data collection through a machine, tool or device" as the trigger for the allocation of rights, which may be joint in case of joint investments. Such option would have genuinely consisted in an ownership right.

The second option would consist of "a set of defensive rights" inspired by the Trade Secret Directive,[110] so as to protect the data holder against what is deemed "illicit appropriation of data" (to be determined). The rights would include "a right to seek injunctions preventing further use of data by third parties who have no right to use the data", "a right to have products built on the basis of misappropriated data excluded from market commercialization" and a right to claim damages. Such protection would be afforded to the data holder, thereby protecting "possession" (similar to the Trade Secret Directive). While recognizing that this may result in consolidating unfair allocation of data to the data holder, the Commission SWD highlights elsewhere (seemingly as a positive thing) the fact that such option would "complement technical efforts currently undertaken by data holders to protect their data and the transmission of such data against third parties with whom they do not have contractual relations". The legal protection could even be made *reliant on* such technical efforts. The Commission SWD then elaborates on exceptions, in the sense of related obligations to share data to several actors.

With a data producer's right, the objective was to "enhance the tradability of […] data as an economic good". The EC seemed to follow at least two theories as for the allocation of rights. While not necessarily conflicting, these theories should be identified as they constitute the *ratio legis* of the data producer's right. While the right was eventually not proposed by the EC, the arguments put forward have been continuously discussed concerning the regulation of data as an economic resource. In its Communication, the EC envisaged to grant the right to the data producer, namely the owner or long-term user of the device with two objectives. First, to "clarify[…] the legal situation", which does support the creation of a right, but not necessarily to the data producer *in particular*. And second, to "open[…] up the possibility for users to utilize their data and thereby contribute to unlocking machine-generated data". The second objective is linked to the fact that data producers are allegedly holders of the data or, in other words, are in factual control of them,[111] the idea being that they should be incentivized to share such data rather than keeping them in silo. Such 'incentive theory-based' argument is backed by the Commission SWD, which argues that data producers will get protection for the investment made in data collection. However, the Commission SWD also supports the first objective identified in the Communication, namely the creation of rights *tout court* to "clarify the legal situation" of data, irrespective of (or at least with less consideration for) the initial allocation. The Commission SWD indeed grounds the data producer's right in the law and economics Coase theorem, based on the efficiency of markets.[112] Provided they are "efficient", markets would serve to allocate goods (secondary allocation) to parties who would most benefit from them. Such reasoning reduces the importance of initial allocation of ownership(-like) rights but pleads in favor of the creation of such rights as a building block for an efficient market to operate.

Such belief in the benefit of markets to allocate (in the case, data-related) value may be put forward to explain the following contradiction. On the one hand, the EC states as a problem the fact that data holders are *de facto* 'owners' of data while, on the other hand, proposing as a solution to afford legal protection to the very same data holders. The primary objective of the EC is to encourage exchange

[110] Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157/1.
[111] European Commission (n 63) s 3.5 A future EU framework for data access.
[112] RH Coase, 'The Problem of Social Cost' [1960] The Journal of Law and Economics 44.

and reuse of data in order to feed growth and innovation. From the proprietarian perspective, markets for data constitute a means to achieve this objective and should be back where needed by legal measures – such as a data producer's right – endorsing the commodification of data. Data holders would be incentivized to commercialize more data, based on the expectation of generating revenues. This clarification of the regulatory objective helps understand how the very same policy document simultaneously envisages a seemingly opposite option, namely the imposition of (sectoral) data access regimes. Data access regimes are discussed in this study when applicable to the railways.

No data ownership rights

There is a general agreement that there is no 'data ownership' in most jurisdictions *de lege lata.*[113] The present sub-section summarizes the general reasons why data are not – and can hardly be - an object of ownership rights.

Although very often referred to, the *incorporeality of data* does not constitute the crux of the problem. The law has already accommodated many different immaterial objects of ownership, where needed based on legal fictions, such as intellectual property rights and 'rights to pollute' (emission tradeable permits). Property law has indeed evolved in all jurisdictions so as to allow for new types of "things" aside corporeal (or tangible) ones. Incorporeality (lack of corporeality) is often used implicitly as a proxy for rivalry, which is the condition for the *possession* of a thing. Possession of a thing implies the simultaneous preclusion of use by third parties.[114] However, intangibles can be turned into rivalrous goods (at least to some extent and in a given environment), as recognized for instance by the Court of Leeuwarden in the Netherlands in 2009 on the occasion of a theft of avatars within the closed ecosystem of an online game.[115]

In contrast, (mere) data are essentially ubiquitous, namely easily duplicable and transferable without detrimental effect to the original data.[116] By nature, data are not excludable,[117] although, as technological goods, excludability of data could be arranged by technical and organizational means. Relatedly, data can be described as non-rivalrous goods, in the sense that the consumption of data by one does not negatively affect the potential for consumption by others. That being said, consumption of the same data by many actors may result in some cases in (economic or non-economic) detrimental consequences for the data producer or initial holder. As a result, data are often considered in economic

[113] Doubts have been cast on the legal status of data under property law in France, after the supreme court (Cour de Cassation) ruled on two occasions that downloading data without the prior consent of the data holder constitutes "theft", although the French Criminal Code defines theft as the fraudulent *deprivation* of someone's property (Art. 311-1), see Cour de Cassation, ch. Crim., 20th May 2015 No 14-81336 and Cour de Cassation, ch. Crim., 28th June 2017 No 16-81113.

[114] See the Court of Appeal of England and Wales case *Your Response Ltd*, [2014] EWCA (Civ) 281. As reported and discussed by S. Van Erp, the Court denied that a database could be "possessed" for lack of an simultaneous exclusion of third parties and rather chose the expression "degree of control", namely outside the scope of property law, see Sjef van Erp, 'Ownership of Data and the Numerus Clausus of Legal Objects' (2017) 6 Brigham-Kanner Property Rights Conference Journal 235, 245–246.

[115] LJN: BG0939, Rechtbank Leeuwarden, 17/676123-07 VEV .

[116] OECD, 'Data-Driven Innovation - Big Data for Growth and Well-Being' (OECD 2015) 195 <https://read.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en> accessed 7 April 2019.

[117] Bertin Martens, 'An Economic Perspective on Data and Platform Market Power' (JRC, European Commission 2021) 2020–09 5.

terms as a "public good", namely a good that is both non-rivalrous and non-excludable, in contrast to "private goods" being excludable and rivalrous.[118]

A major question has been whether data can qualify as a 'thing' within the meaning of property law. In addition to their ubiquity, data are characterized by their volatility and dynamicity in the data economy. Such features challenge both the general principle of legal certainty and the principle of transparency in property law. The principle of transparency finds its justification in the *erga omnes* effect of property rights. Because property rights are enforceable against 'everyone', the latter should logically be made aware of the existence and scope of such rights as a precondition. In order to do so, the 'thing' as object of property rights should be clearly delineated (the same holds true for the exclusive rights afforded to the owner). Especially when large amounts of data are processed at a rapid pace in the data economy, the datum as a set of bits and bytes disappears rapidly and therefore does not constitute a suitable object for property. Similarly, it makes it practically difficult to organize publicity, namely, to let third parties know about the attributability of the rights.

Another challenge lies in the allocation of rights. There is often a multitude of stakeholders who have contributed to the creation of data and could therefore legitimately claim ownership. While co- or joint ownership could take place, *systematic* cases of co- or joint ownership as it would likely be the case would increase – rather than decrease – the uncertainty surrounding data as well as the transaction costs of exchanging and commercializing data.

Because data are pervasive, ownership rights in data would inevitably raise consistency issues with other legal frameworks, and especially intellectual property rights and data protection law. Ownership rights on personal data can indeed not be reconciliated with the rights afforded to data subjects, which are typically non-waivable. Consistency issues between legal frameworks are common in the law. However, with data ownership, they would be systematic, and it is not clear how they could be solved. When envisaging a form of data ownership (see sub-section on the 'data producer's right above), the European Commission proposed to limit the scope *rationae materiae* to "non-personal data". Such limitation was aimed at preventing contradictions with data protection law, which would then, theoretically, not stand in the way of ownership rights. However, the qualification as 'personal data' is highly contextual (see Part I) which makes it illusionary to design ownership rights solely for non-personal data.[119] As described in Part I, distinguishing 'data' from 'information' is difficult. In practice, there is a risk that an ownership right on data could lead to the appropriation of information, to the detriment of the freedom of expression and the freedom to conduct a business (which implies a general right to copy, save exceptions).[120] Data ownership would also lead to an inherent inconsistency

[118] Bertin Martens, 'The Impact of Data Access Regimes on Artificial Intelligence and Machine Learning' (2018) JRC Technical Reports 2018–09 11. His work therein follows the work of leading information economists, such as Joseph E Stiglitz, 'The Contributions of the Economics of Information to Twentieth Century Economics' (2000) 115 The Quarterly Journal of Economics 1441; R Hal Varian, 'Markets for Information Goods' (1998) <https://people.ischool.berkeley.edu/~hal/Papers/japan/> accessed 25 March 2021.
Two additional types are sometimes included in this categorisation, namely "club goods", but also "common-pool resources".

[119] Inge Graef, Raphael Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation' (Social Science Research Network 2018) SSRN Scholarly Paper ID 3256189 <https://papers.ssrn.com/abstract=3256189> accessed 29 July 2019.

[120] Hugenholtz (n 6) 13; Serge Gutwirth and Gloria Gonzalez Fuster, 'Titre 5: L'éternel retour de la propriété des données: de l'insistance d'un mot d'ordre', *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés*

to property law, concerning digital assets (such as crypto-assets or avatars in online games, see above) which, although intangibles, are rivalrous.[121]

Finally, the expression 'data ownership' should be handled with care. It suggests a form of consensus on what ownership rights on data would consist of. However, property law is never united and does (increasingly) take into account the specificities of the things (such as movables v immovables). Given the specificities of data as described in this sub-section, ownership rights on data *quod non* would have to be designed *sui generis.*[122]

Guidance for RNE -

- It is generally agreed that there is no 'ownership right' in (mere) data, although the physical environment where data is stored may be the object of property (*i.e*. servers).
- It is very unlikely that ownership rights will be created on data (at both EU and national level) in the near future, because of the specificities of their features in the data economy.
- As discussed in the other sections of the present study, this does not mean that data evolve in a lawless environment, as many legal frameworks can have an impact on the processing of data.
- At EU level but also globally, the 'data ownership' debate has evolved towards a debate on 'data rights' (see section 2.5).

2.2.1.3. Contract law as a fallback

The present analysis demonstrates that a patchwork of EU laws exist which give partial 'entitlements' on data. This fragmented legal landscape applicable to data cannot fully address the need for clarity and stability in legal data transactions. However, despite the legal ambiguities, businesses exchange and use data through contracts daily.

A data transaction (contract) could be defined as any legal exchange or act which has as its subject either the actual use of data and/or the rights permitting or enabling such use. A data contract may contain data of any kind (e.g., raw data, inferred data, or data subject to IP protection) and the envisaged use may range from simple access to a permanent or temporary transfer of data (with or without further rights to modify, aggregate, share or otherwise commercialize data). Depending on the purposes and the type of data use, a data contract may expressly or impliedly contain several other transactions (e.g., consent, specific IP license, or other authorisations) subject to different legal regimes and contractual restrictions. Data transactions can be standalone, or they may constitute a portion of a broader legal contract.

Based on the above, a data transaction consists of five components:

- The data and/or the data source (type, volume etc.).
- The operations to be carried out, types of usage (e.g., transfer access, modify)

dans le cybermonde - Liber Amicorum Yves Poullet (Degrave, Elise ; Terwangne, Cécile de; Dusollier, Séverine ; Queck, Robert, Larcier 2018).

[121] See the work of UNIDROIT on digital assets, https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/#1622753957479-e442fd67-036d

[122] On this, see Swinnen (n 58).

- The purposes for which the recipient will use the data (e.g., text and data mining analysis, service optimisation, aggregation, automation, sales development and so on)
- The legal form(s) through which the transaction will come into existence (license, written consent, terms of use, sectoral data sharing schemers etc)
- The technical tools that will be used to give the recipient the necessary control for the agreed usage of data.

Contract law is generally not specific to data. Yet contracts are the main legal instrument used by businesses that *de facto* regulates data as an asset. Several studies have shown how contracts can be designed so as to imitate property rights in data, for the purpose of the business relationship between the parties (*inter partes* effect, in contrast to the *erga omnes* effect of ownership rights, see section above). In such case, it is often the initial data holder who acts as the 'owner'. As a matter of fact, many B2B contracts refer to 'owner' or 'ownership' of data. While not prohibited as such, the reference to 'data owner' or 'data ownership' is not advisable if not carefully defined and regulated contractually. The absence of ownership rights in data in positive law can indeed only obscure the interpretation of such clauses by a judge.

More commonly, data transactions are based on the notion of *control* over data—irrespective of whether such control rests on legal grounds or simply stems from one's control over physical means enabling exclusion. In other words, a data transaction, aiming to regulate the access and usage of data, equips the recipient with control over the data by way of legal and/or technical means. As such, control over data is a multifaceted concept emerging in different guises in different parts of the data ecosystem. As an umbrella term, it may be understood as the totality of the physical and legal means that enable or facilitate the exploitation of data (e.g., access, license, transfer, modify, combine, edit, and delete).

It should be noted that contractual agreements are not bulletproof. Due to the complex and fragmented regulatory environment (i.e., data protection, copyrights, sui generis right, trade secrets), the legal validity of data transactions/contracts can be subject to controversy. It is usually difficult to know in advance whether any data contract could survive the legal challenges stemming from personal data protection and IP rights. Moreover, dealings on data might also be restricted by domestic laws aiming to protect the weaker party in contracts, e.g., the provisions relating to *standard contract terms* or *unfair contract terms*. Accordingly, the clearance of rights and identifying the stakeholders who might have entitlements on data may turn out to be excessively cumbersome. In a nutshell, data contracts/transactions can be prone to invalidity claims and further enforceability problems.

Even in the case of truly valid and enforceable contracts, this will not prevent the appropriation or the use of data by those who are not bound by the contract. This is due to the principle of "privity of contract", that is, contracts only have a binding effect between the signatories. Therefore, the contractual arrangements are of little or no use for business models which somehow require the publishing or sharing of data with an indeterminate group of persons.

2.2.2. Specific legal frameworks

2.2.2.1. The ITS Directive ecosystem

The Intelligent Transport Systems Directive

The Intelligent Transport Systems ("ITS") Directive sets a legal framework for a coordinated deployment of ITS in the EU, through the adoption of technical, functional and organizational specifications. ITS is defined as "*systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport*".[123]

The Directive sets out four priority areas and, within those, several priority actions. The most relevant priority area of the ITS Directive for the purposes of this report is the "optimal use of road, traffic and travel data"[124], which includes a priority action for the provision of EU-wide multimodal travel information services[125], also covering rail transport. Amongst the specifications set out for this action item, ensuring availability of data and facilitating data sharing holds a prominent position. Indeed, Annex I of the ITS Directive provides the following concrete actions: a) ensuring the availability and accessibility of accurate road and real-time traffic data used for multimodal and real-time travel information to ITS service providers without prejudice to safety and transport management constraints; b) facilitating cross-border electronic data exchange between the relevant public authorities and stakeholders and the relevant ITS service providers; and c) timely updating multimodal travel information by the ITS service providers.

The European Commission is granted the competence to adopt delegated acts to lay down specifications and standards concerning, first, the priority actions and, then, other actions in the priority areas.[126] As a result, the European Commission adopted a large number of such acts.[127] The Commission Delegated Regulation on EU-wide multimodal travel information services (MMTIS)[128] constitutes the most recent Regulation adopted by the European Commission under the ITS framework. It illustrates the willingness of the EU legislator to foster data sharing, particularly in the transport sector. The MMTIS, extends to the railways under certain circumstances and is analyzed below.

The European Commission announced its plan to propose a revision of the ITS Directive by the third quarter of 2021,[129] which should include a revision of delegated regulations "to further contribute to data availability, reuse and interoperability and establish a stronger coordination mechanism to federate the National Access Points established under the ITS Directive through an EU wide CEF

[123] ITS Directive, Art. 4(1).
[124] ITS Directive, Art. 2.
[125] ITS Directive, Art. 3.
[126] ITS Directive, Art. 3.
[127] For a list of delegated acts adopted on the basis of the ITS Directive, see here: https://eur-lex.europa.eu/search.html?DB_DELEGATED=32010L0040&qid=1582188552054&DTS_DOM=ALL&type=advanced&lang=en&SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL.
[128] Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services, OJ L 272/1 ('MMTIS').
[129] European Commission, Communication 'Commission Work Programme 2021, A Union of vitality in a world of fragility', COM/2020/690 final, Annex I, 19 October 2020.

Programme Support Action (2020).[130] The willingness to use the ITS Directive ecosystem as an instrument fostering data sharing was already visible in the most recent delegated acts adopted to the ITS Directive (see above). The revision of the ITS Directive reinforces this pattern.

The European Commission issued a proposal for the revision of the ITS Directive in December 2021.[131]

Commission Regulation on EU-wide multimodal travel information services

The MMTIS Regulation aims to enable the provision of comprehensive travel information services.[132] Such services rely on both static and dynamic travel and traffic data, where "static travel and traffic data is essential for information and planning purposes" (pre-planning phase) while "dynamic travel and traffic data, for example, travel disturbances and delays, can allow end users to make well informed travel decisions and bring time savings".[133] The MMTIS does not lay down obligations to collect or produce data, but applies only *to data already collected and available in "machine readable format"*,[134] both static and dynamic travel and traffic data as listed in the Annex. The Regulation has a broad scope. First, and unlike other ITS delegated acts, it applies geographically to the whole EU (. Second, it applies to all transport modes, including the railways (defined as "schedule based").[135]

Data sharing and exchange via National Access Points

In order to facilitate the exchange and re-use of data, Member States are required to set up National Access Points ("NAPs").[136] Transport authorities, transport operators, (railway) infrastructure managers[137] and transport on demand service providers shall provide 'their' static travel and traffic data as well as historic traffic data, through NAPs.[138] Such data include for instance location searches (origin / destination), trip plans, trip plan computation, etc., as laid down in Annex, point 1. The list is unique for all transport modes and actors, so that it remains unclear who should provide which data, especially when several actors may dispose of the same (e.g. transport operators and infrastructure managers). Anyways, some data are clearly for (railway) infrastructure managers to provide, such as "network topology and routes/lines". As for the railways, data should be provided using the standards and technical specifications laid down in the TAP TSI.[139] Data should be provided with their metadata. The APIs that provide access to such data via the national access point "shall be publicly accessible allowing users and end-users to register to obtain access".[140]

In contrast, the Regulation does not lay down a positive obligation to provide *dynamic* travel and traffic data, such as information disrupted traffic, real-time status information, estimated departure and arrival times of services, etc. (Annex, Point 2). It is up to Member States to decide whether they make the provision of such data mandatory. Should they do so, the duty-bearers – transport authorities,

[130] European Commission, European Data Strategy, 19 February 2020.
[131] Proposal for a Directive amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, 2021/0419 (COD), 14.12.2021.
[132] MMTIS, Rec. 10.
[133] MMTIS, Rec. 12.
[134] MMTIS, Rec. 14.
[135] MMTIS, Art. 1 (2), Rec. 8 and Annex.
[136] MMTIS, Art. 3.
[137] MMTIS, Annex, Point 1.
[138] MMTIS, Art. 3 and 4.
[139] MMTIS, Art. 4(1)(b).
[140] MMTIS, Art. 4(4).

transport operators, infrastructure managers or transport on demand service providers – would have to provide such data in the respective format laid down in the Regulation, namely TAP TSI-based standards , and should more generally follow the conditions laid down in the Regulation. In particular – and same as for static data - APIs that provide access to such data shall also be "publicly accessible allowing users and end-users to register to obtain access".[141]

Beneficiaries – namely the 'users' – can be any public or private entity which uses the NAP, such as transport authorities, transport operators, travel information service providers, digital map producers, transport on demand service providers and infrastructure managers.[142] In other words, beneficiaries can be either the duty-bearers as identified under the MMTIS or any third parties. The NAP shall not merely provide the data but shall also provide "discovery services to users", allowing for searches in the datasets for instance.[143] The role of NAP should not be underestimated. They act as a central national repository and may also play a role in the interoperability of data. The European ITS Platform has recently conducted a comprehensive report on NAPs.[144] The report sets out that real-time traffic information is the most implemented NAPs, whereas the number of NAPs implemented for multimodal travel information services is significantly lower.[145]

Because travel information services shall be based on accurate data, data providers of, respectively, static or dynamic data (see above) also have an obligation to *update* the data that they provide (in case of change) to the NAP and to correct inaccurate data where appropriate "in a timely manner".[146] Data may be provided subject to terms and conditions imposed by the data provider through a license agreement, although the terms are subject to a necessity and proportionality test. The price for the provision of the data ("financial compensation") shall be "reasonable and proportionate to the legitimate costs incurred of providing and disseminating the relevant travel and traffic data".[147]

Although the beneficiaries of the Regulation – namely mostly the travel information service providers – have no obligation to update the data they produce, they do have obligations under the Regulation. First, they shall also provide data based "on the static, and where possible, dynamic information", that they benefited from, to other information service providers, yet only upon request.[148] Such obligation applies with respect to "routing results", namely the "travel itinerary in a machine readable format resulting from an end-users' journey request with reference to the hand-over point(s) used".[149] This provision aims to overcome the (geographical) fragmentation of offers and allow for genuine comprehensive travel information services. Second and more innovative, the travel information service providers also have neutrality obligations with respect to the reuse of the (static and dynamic) data. Travel information service providers shall make their criteria for ranking travel options of different transport modes transparent. They shall not be based on "any factor directly or indirectly

[141] MMTIS, Art. 5.
[142] MMTIS, Art. 2 (11).
[143] MMTIS, Art. 3 (3).
[144] EU ITS report, p.27.
[145] EU ITS report, p.27.
[146] MMTIS, Art. 6.
[147] MMTIS, Art. 8 (4).
[148] MMTIS, , Art. 7 (1).
[149]MMTIS, Art. 2 (22).

relating to the user identity or, if any, the commercial consideration related to the reuse of the data". Such criteria shall be "applied on a non-discriminatory basis to all participating users".[150]

Although the data provision obligations are obviously aimed at supporting the provision of multimodal travel information services,[151] the MMTIS does not *stricto sensu* restrict the reuse of data for other purposes or is, to the least, unclear on this aspect. The definition of the NAP points towards that interpretation. Indeed, a NAP is defined as "a digital interface where at least the static travel and historic traffic data together with the corresponding metadata are made accessible *for reuse* to users, or where the sources and metadata of these data are made accessible *for reuse* to users". The MMTIS allows data providers to condition the making available of the data on the conclusion of a licence agreement, which shall however not "unnecessarily restrict possibilities for reuse […]" and shall "impose as few restrictions on reuse as possible".[152]

Should the Regulation be read so that it restricts the reuse of data only for the purpose of providing multimodal travel information services, it would remain to be seen how to ensure this is the case in practice.

The MMTIS should be revised in 2022 *i.a.* so as to include dynamic datasets.

Guidance for RNE -

- RNE is not directly concerned by the provisions of the ITS Directive and the MMTIS, but IMs are.
- The Regulation applies a step-by-step data availability approach (see Art. 4(3)), in the sense that data had (have) to be provided via the NAP respectively by 1st December 2019, 1st December 2020, 1st December 2021 and 1st December 2023.
- The data covered by the scope of the Regulation should be considered as publicly available, given the fact that any party can claim access to the national access point without restriction of purpose for reuse, subject to national transposition, and potential licensing conditions imposed by the operators making the datasets accessible. If the data are considered as public sector information, the Open Data Directive applies (see section 2.2.2.2 below).
- The MMTIS can have a double-edged sword effect on data commercialization by RNE: on the one hand, data within the MMTIS scope can be considered as reusable without the need of prior clearance of rights. On the other hand, the commercial value of such data may be diminished, given the MMTIS regulation of the (especially, financial) terms under which data are made available for reuse. That being said, data within the MMTIS scope can be commercialized in a bundle with other data to make the offer more appealing.

[150] MMTIS, Art. 8 (2).
[151] MMTIS, Rec. 10 and Art. 8(1).
[152] MMTIS, Art. 8(4).

2.2.2.2. From the PSI to the Open Data Directive

Public undertakings under the Open Data Directive

The PSI Directive[153] was repealed and replaced with the 'Open Data Directive',[154] that was due to be transposed by July 2021. The Open Data Directive fosters the 'PSI regime' and aims to broaden its scope. The EU and particularly the European Commission ('EC') are indeed actively trying to increase data sharing across the Union, in order to foster growth and innovation. Making public sector information available for reuse by third parties is viewed by the EC as core to this strategy. "Re-use" means the use of the data or documents held by (in this case) the public undertakings for purposes *other than* the initial purpose of *providing services in the general interest* for which the documents were produced […]" (emphasis added).[155]

The EC was initially willing to extend the scope of the PSI regime to public undertakings such as utilities (public transport operator, energy operators including water operators, etc.), due to the large amount of valuable data that they produce in the course of their activities.

Public undertakings are however subject to contradictory incentives in that respect: on the one hand, they are tasked with public service obligations, subsidized by public funding and can be subject to more or less direct control by public sector bodies ('PSBs'). But, on the other hand, they pursue an economic activity on a market from which they are expected to (partly) cover their costs. They may also be indirectly exposed to competition (for instance: after a temporary monopoly situation) and are often subject to private company(-like) governance. Because of this particular situation, the Open Data Directive does *not* impose the 'PSI regime' *mutatis mutandis* to public undertakings, which are therefore not mandated to make their data available for reuse. The Directive merely harmonizes the *terms and conditions* for making data available for reuse (i.e. non-discrimination, transparency, fairness, proportionality, etc.), *should* public undertakings make their data available for reuse.[156]

The obligation for non-discrimination

Article 11 of the Open Data Directive provides that "any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use, including for cross-border re-use". The 'non-discrimination' notion may not be as straightforward as it seems at first glance. It implies the prior identification of comparable situations of reuse of data or documents and, therefore, the identification of categories of re-use. Rec. 46 clarifies that the "conditions for re-use should be non-discriminatory for comparable categories of re-use. In that regard, the prohibition of discrimination should not, for example, prevent […] the adoption of a differentiated charging policy for commercial and non-commercial re-use". Public undertakings could therefore charge differently, depending on the commercial or non-commercial re-use. It would also seem logical that public undertakings can distinguish the *technical* conditions for re-use, *i.e.* whether bulk vs single data or whether data stream vs ad hoc data, which could have an impact on the IT systems of the public

[153] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, OJ L 345/90.
[154] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172/56.
[155] Open Data Directive, Art. 2(11).
[156] Open Data Directive, Art. 3(2) and Rec. 26. For a study of the Directive, see
Charlotte Ducuing, 'Data as Infrastructure? A Study of Data Sharing Legal Regimes' [2019] Competition and Regulation in Network Industries <https://doi.org/10.1177/1783591719895390>.

undertakings. It seems however unlikely that public undertakings could differentiate the conditions for re-use depending on the mere *purpose* for re-use. It would indeed imply that the public undertakings would interfere in the (business) decisions of the re-users, while the Open Data Directive is precisely based on the fact that 'the market' will find the best ways to re-use data and documents.

The specific legal regime for public undertakings under the Open Data Directive seems well-balanced. On the one hand, it respects the freedom of public undertakings to conduct a business and more generally the specific situation they are in and prevents data-driven practices which they could have been subjected to by (potential) competitors. On the other, their (temporary) monopoly to conduct public services obligations justifies that they shall be subject to general principles of fairness when making data available for reuse by third parties, just like in public procurement law and in the sectoral regulation of most utilities.

The definition of a 'public undertaking' is based on public procurement law.[157] RNE is not a public undertaking according to Austrian law but (some) RNE members could qualify as public undertakings.

The decision to make data held by public undertakings available for reuse may stem from the public undertakings themselves, *i.e.* in order to commercialize their valuable data. Or else, such making available of data for reuse may be mandated by national law,[158] such as in Belgium, where the federal legislator did however regrettably not take into account the above-mentioned specificities of public undertakings.[159] Additionally, by exception, the Directive maintains an obligation for public undertakings to make *some of their data* available for reuse by third parties, namely in the case where they would qualify as "high-value datasets", as described in the following sub-section.

Guidance for RNE -

- RNE is not *directly* concerned by the Open Data Directive regime. However, it may be *indirectly* affected via the obligations of its members who qualify as public undertakings.
- Public undertakings (such as the IMs) are included in the scope of the Open Data Directive but are not subject to the 'PSI regime' (I.e. the obligation to make data available for re-use) pursuant to the Directive in principle.
- However, there are exceptions. First, the national legislator may choose (or have chosen) to apply those obligations to them *mutatis mutandis* or subject them to specific regulation. Second, public undertakings must comply with high-value datasets-related provisions (see below). Third, public undertakings must comply with the conditions for reuse set forth in the Open Data Directive for documents that they choose to make available for reuse.
- In this respect, the consent given by IMs to RNE for commercializing a given data or document *not yet made available for reuse* would trigger the application of the Open Data Directive regime (subject to national transposition) for such data. The IM would then likely

[157] Open Data Directive, Rec. 29 and Art. 2(3).

[158] The Directive "encourages" Member States to broaden the scope to "documents held by public undertakings, which are related to activities that have been found, pursuant to Article 34 of Directive 2014/25/EU […] to be directly exposed to competition" (Open Data Directive, Rec. 19).

[159] For public undertakings subject to federal law, see the Act of 4th may 2016 ('Loi relative à la réutilisation des informations du secteur public' or 'Wet inzake het hergebruik van overheidsinformatie') and the implementing royal decree of 2nd June 2019 ('Arrêté royal relatif à la réutilisation des informations du secteur public' or 'Koninklijk besluit inzake het hergebruik van overheidsinformatie').

have to make such data or document available for reuse to third parties under the (especially, financial and non-discrimination related) conditions laid down in the Directive.

High-value datasets

The term "high-value datasets" is created by the Open Data Directive. It is broadly defined as "documents the reuse of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and of the number of potential beneficiaries of the value-added services and applications based on those datasets".[160] A list of "thematic categories" of such datasets is included in the Annex I of the Directive which includes "geospatial, earth observation and environment, meteorogical, stastistics, companies and company ownership and mobility". The EC is entitled to add other thematic categories by means of delegated acts.[161]

High-value datasets are subject to a specific legal regime.

a) First, high-value datasets in the thematic categories shall be identified by the EC by means of implementing acts. The identification shall be based on an *assessment of the value* that such data are likely to produce for society, in the prior impact assessment. On the other side, the EC shall also analyze the impact of providing such data on PSBs required to generate revenues and on public undertakings in a competitive economic environment.[162] 'Mobility' is identified as one of the relevant thematic categories.[163]
b) Then, *when held by either PSBs or public undertakings,* high-value datasets shall be made available free of charge in principle, except in a limited set of cases, such as when there is a risk of distortion of competition for public undertakings in the relevant markets or to the benefit of PSBs which need to rely on licensing fees to sustain their activities.[164] The datasets shall be made available for reuse in a machine-readable format, provided via APIs and, "where relevant", as a bulk download.[165]

It remains unclear whether limitations to the scope of the Open Data Directive (i.e. when access or reuse would interfere with intellectual property rights, trade secrets, data protection law or security and defense secrecy) are also applicable to high-value datasets. Concretely, when the high-value datasets are identified by the EC, will PSBs and public undertakings be allowed to invoke such limitations to refuse to make such data available for reuse?

Another question lies in the level of detail in which the data will be identified by the EC.

The most striking aspect is the obvious pride given to data reuse, illustrated by the criteria for identifying high-value datasets, namely according to their value for reuse, while the PSI regime was based on the idea that existing data would be made available for reuse, *and societal actors (and especially market players) would determine whether data have value to their business*. The latter approach was in line with an economic liberal approach, where value is determined subjectively by economic actors in a decentralized manner (rather than by central public authorities). With high-value

[160] Open Data Directive, Art. 2(10).
[161] Open Data Directive, Art. 13(2).
[162] Open Data Directive, Art. 14(2).
[163] Open Data Directive, Annex I, 6.
[164] Open Data Directive, Art. 14(1) and (3).
[165] Open Data Directive, Art. 14(2).

datasets, the legislator takes a noteworthy proactive economic role in determining the value of traded 'goods', which shows once more its willingness to reap benefits expected from data-driven markets.

The EC has not yet adopted an implementing act to identify high-value datasets but committed to "start the procedure" by the first trimester of 2021 (see the European Data Strategy).[166] The European Data Portal, established by the EC, published a study on the identification of the high-value data sets.[167] While the report aims at focusing on the perspective of data providers / data holders, it is surprisingly based on interviews from stakeholders, none of them representing public undertakings. The report underlines that defining the value of data is a very complex task, not least because the value of data "can be perceived and defined very differently by different stakeholders" and depending on local issues,[168] which comes as no surprise. In other words, the value of data is intrinsically *subjective* – it depends on the particular use of a given actor. Data are indeed deemed to be valuable in the data economy *because they can be (re)used for a wide range of purposes* (sometimes unexpectable *ex ante*). The challenge lies in the fact that, in contrast, the EC, as a public institution, shall conduct an *objective* analysis of the value of data, in order to identify high-value datasets without unduly favoring a business (model) over another.

Guidance for RNE -

- . Subject to pending acts to be adopted by the EC, public undertakings (such as the IMs) should be under the obligation to make 'high value datasets' available free of charge, save for some exceptions.
- The commercial value of 'high value datasets' would obviously decrease since RNE members would have to make them available free of charge. However, this prevents neither RNE members nor RNE to commercialize the very same data in an aggregated manner (possibly with other data) and/or data inferred from such data, should there be a business case for doing so.

2.3. Prospective regulation of data

2.3.1. The European Data Strategy: the new EC orientations to regulate data as an economic resource

The Data Strategy of 2020[169] crystalizes the new paradigm of the EC concerning the regulation of data as an economic resource.

In the Data Strategy, the EC reiterates the importance of data for *i.a.* the economy and the objective to make data more broadly accessible for businesses. The EC aims to increase the amount of data available while preserving the EU's fundamental values, "in particular personal data protection,

[166] European Commission, Communication 'A European strategy for data', 19.2.2020, COM(2020) 66 final, Section 5.1.

[167] European Data Portal, Analytical Report 15 - High-value datasets: understanding the perspective of data providers, 2020, accessible online: https://www.europeandataportal.eu/sites/default/files/analytical_report_15_high_value_datasets.pdf (last visited 27th November 2020).

[168] Idem, p.9.

[169] Communication 'A European strategy for data' 2020 (COM/2020/66 final).

consumer protection legislation and competition law".[170] While reiterating the objective to foster data access and reuse, the EC highlights the need for rules for access to and use of data to be "fair, practical and clear" (something already present in the Communication 'Building a European Data Economy' of 2016) but also based on "clear and trustworthy data governance mechanisms".[171] While deploring again the lack of data sharing between businesses, the EC points to a range of potential explanations: "the lack of economic incentives […], lack of trust between economic operators that the data will be used in line with contractual agreements, imbalance in negotiating power […]", especially between online platforms and their users so that online platforms can decide on the conditions for access and (re)use of data, the fear of misappropriation of the data by third parties, and a lack of legal clarity on who can do what with the data (for example for co-created data, in particular IoT data)".[172]

The Data Strategy envisages a two-tiered approach,[173] namely a horizontal (sector-agnostic or cross-sectoral) one accompanied by sector-specific measures with "common European data spaces":

A "cross-sectoral (or horizontal) governance framework for data access and use"

The horizontal governance framework should be subsumed in two main[174] legislative instruments. The first one (resulting in the proposal for a Data Governance Act) should strengthen the governance mechanism for common European data spaces. The second one (*forthcoming* Data Act) should "provide incentives for horizontal data sharing across sectors". In order to support business-to-business data sharing, the future Data Act could in particular "address[…] issues related to usage rights for co-generated data (such as IoT data in industrial settings), typically laid down in private contracts", "address any undue existing hurdles hindering data sharing and […] clarify rules for the responsible use of data (such as legal liability)".[175] While data sharing should be voluntary in principle, data access regimes could be mandated by law "where specific circumstances so dictate" under FRAND conditions (Fair Reasonable and Non-Discriminatory, to which the Data Strategy adds the principle of proportionality). The Data Act could also deal with IPRs, whether to clarify or revise them so as to facilitate data access and use. Finally, data intermediaries for personal data applications and personal data spaces ("brokers") could be regulated in the Data Act so that individuals are "empowered to be in control of their data through tools and means to decide at a granular level about what is done with their data".[176]

The data spaces

Second, the horizontal approach should be complemented by sectoral initiatives, namely the "common European data spaces in strategic sectors and domains of public interest". The common European data spaces are not only economics-driven; both their identification (*i.e*. as domains "of public interest") and their expected impact should be societal as well, based on the enhancement of data availability,

[170] ibid 5.
[171] ibid.
[172] ibid 7.
[173] The Data Strategy includes another pillar, which does however not have legislative dimensions and is therefore not introduced here, see pillar B "Enablers: Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability" (ibid 15–20.).
[174] Other – less significant - legislative instruments are listed in the Data Strategy, i.e. the implementing act on the high-value datasets. However, this should not be considered a political initiative or announcement, since the EC is legally mandated to adopt such Act based on the PSI and Open Data Directive (see section 2.2.2.2).
[175] Communication 'A European strategy for data' 13.
[176] ibid Pillar C-20.

"the technical tools and infrastructures necessary to use and exchange data" and "appropriate governance mechanisms".[177] Where appropriate, sectoral legislation could be enacted to complement horizontal legislation on data access and use. While the governance mechanisms for data spaces should not follow a one-size-fits-all approach, "common governance concepts and models can be replicated in the different sectors".[178] A list of nine data spaces is included in the Data Strategy, with the respective legislative and non-legislative initiatives expected to be adopted,[179] *i.e.* "industrial (manufacturing) data space", "Green Deal data space" or "mobility data space".

As for the mobility data space, the European Commission places the emphasis on intelligent transport system ('ITS') and the automotive, while mentioning "other modes of transport".[180] As for the railways, the EC (merely?) commits to review the "regulatory framework for interoperable data sharing in rail transport" in 2022. Although without clarification of which concrete "regulatory framework" is at stake, the EC seems to target the 'New PRR' provisions on data sharing (see section 3.2.1) as well as the TAP and TAF TSIs (Section 3.2.2). It is worth noting that the EC intends to amend its proposal for a Regulation on the Single European Sky[181] so as to include "new provisions on data availability and market access of data service providers in order to promote the digitalization and automation of air traffic management" by 2020 (further discussion on data sharing in the aviation sector under section 4 below).[182]

Conclusion – from the Communication 'Building the European Data Economy' to the Data Strategy

The Data Strategy constitutes obviously a continuation of the 2016 Communication 'Building the European Data Economy', when it comes to the objective assigned to the regulation of data as an economic resource. That being said, some evolutions can be observed. The question whether and to what extent legislation should be horizontal versus sector-specific, which was asked in the Communication 'Building the European Data Economy', is generally decided by the EC under the Data Strategy. In essence, the EC plans to propose both horizontal and sectoral legislation which should complement one another. Especially data access regimes, where appropriate, should mainly be adopted in sectoral legislation.

On the other hand, substantive rights on data should be adopted, where appropriate, in horizontal legislation. The "sectoral" dimension of the Data Strategy leaves however many open questions. What 'common European data spaces' concretely are remains unclear; whether it is only a concept or squarely a governance mechanism to be set up between relevant actors. Besides, not all data spaces are genuinely 'sectoral' and could therefore easily overlap. While "mobility" generally refers to transportation, the "common European Green Deal data space" (for instance) refers more generally to a horizontal policy of the EU, which should ideally affect many – if not all – sectors.

[177] ibid 21.
[178] ibid.
[179] ibid Appendice.
[180] ibid D and Annex.
[181] Proposal for a Regulation on the implementation of the Single European Sky (recast), /* COM/2013/0410 final - 2013/0186 (COD) */, dating back from 2013. The EC did indeed issue an amended proposal for a Regulation on the implementation of the Single European Sky (recast), COM/2020/579 final, in 2020.
[182] Communication 'A European strategy for data' Annex.

A major evolution can be observed concerning the options to create *substantive rights on data*. From the data producer's right to data usage rights on co-generated data, the EC has visibly abandoned the proprietarian approach - and *especially the exclusivity of one's right on data*.

Finally, a new item enters the field of the regulation of data as an economic asset with the Data Strategy, namely (the regulation of) "data governance" in the sense of "operational, organizational approaches and structures (both public and private) needed [to] enable data-driven innovation on the basis of the existing legal framework".[183] As a likely result of scholarly discussions in this respect, the Data Strategy revealingly refers to many data governance mechanisms, such as "data pool",[184] "data cooperative"[185] and "data trust".[186] The Data Governance Act proposed by the EC is discussed in more details in the following section.

2.3.2. The Data Governance Act

In November 2020, the EC proposed a "Data Governance Act" ('DGA').[187] At the time of writing, the Council of the European Union and the European Parliament have agreed on a compromise text.[188]

The general aim of the DGA proposal is to bring trust to data holders and (re)users so that they are incentivized to share data. This translates into several different tracks: Chapter II complements the Open Data Directive concerning the making available of data / documents 'tainted' by entitlements of third parties; Chapter III regulates three types of 'data sharing service providers'; chapter IV sets up an optional regime for 'data altruism organizations'. In line with the EC's 'digital sovereignty' objective, the DGA also aims to regulate the international aspects related to data sharing.

It is beyond the ambit of the present study to provide an exhaustive presentation of the DGA.[189] The section focuses mainly on the 'data sharing service providers' – a notion new to EU law, and more specifically on the (yet unclear) notion of a provider of intermediation services between businesses. Chapter II of the DGA is briefly introduced, although, in the state of the legislative process at the time of writing, it should not be directly applicable to RNE.

2.3.2.1. Chapter II – Complement to the Open Data Directive

Chapter II of the DGA aims to complement the Open Data Directive concerning the making available for reuse of data / documents (on the distinction between the two notions, see Part I on Definitions) 'tainted with' entitlements of third parties. In the eyes of the EC, such data are outside the scope of the Open Data Directive. With the DGA proposal, the EC aims to foster the reuse of such data despite the existence of entitlements of third parties (such as intellectual property rights, confidentiality obligations or data protection obligations), subject to a specific legal regime.

---

[183] Communication 'A European strategy for data' 8.
[184] Communication 'A European strategy for data' 14.
[185] ibid 10.
[186] ibid.
[187] Proposal for a Regulation on European data governance, 2020/0340(COD), 25.11.2020 ('Data Governance Act' or 'DGA proposal').
[188] Presidency of the Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Analysis of the final compromise text in view to agreement, Interinstitutional File: 2020/0340(COD), 10.12.2021.
[189] For a thorough analysis of the Data Governance Act as proposed by the European Commission, see Julie Baloup and others, 'White Paper on the Data Governance Act' (Social Science Research Network 2021) SSRN Scholarly Paper ID 3872703 <https://papers.ssrn.com/abstract=3872703> accessed 21 November 2021.

The proposal from the EC excludes data held by public undertakings from the scope of Chapter II,[190] the latter being applicable only to 'public sector bodies' (PSB). In the state of the legislative process at the time of writing,[191] data held by private undertakings remain outside the scope of the DGA.

This being, the legal regime laid down in Chapter II of the DGA may inform the data policy of RNE and RNE members. By attempting to foster data sharing and reuse even when they are the object of rights of third parties, Chapter II indeed lays down avenues how to accommodate both the interests of the data economy – and in particular of candidate data reusers – on the one hand, while protecting confidentiality (but also IPRs and data protection) of third parties on the other hand.

In the compromise text agreed upon by the Council of the European Union and the European Parliament in December 2021,[192] Chapter II starts with (well-known to Open Data Directive-based legal regimes) transparency obligations concerning the procedure for allowing reuse of data as well as the conditions of reuse of such data as well as with the non-discrimination principle.[193] In order to "ensure the protected nature of data", PSBs shall adopt the following measures upon making available for reuse, which may include the following ones:

- Anonymisation of data in the case of personal data (or, we could add, in the case where data can point to a given business such as an RU) and/or "method of disclosure control" such as modification and aggregation in the case of confidential information;
- Subject to safeguards ensuring the integrity of the functioning of the technical systems, remote access and re-use within a secure processing environment provided or controlled by the PSB;
- Subject to the same integrity-related safeguards, "access and reuse of data within the physical premises in which the secure processing environment is located in accordance with high security standards, if remote access cannot be allowed without jeopardising the rights and interests of third parties".[194]

The DGA proposal also lays down legal safeguards, such as the adherence of the data reuser to a confidentiality obligation, i.e., that prohibits the further disclosure of "any information that jeopardises the rights and interests of third parties that the reuser may have acquired despite the safeguards put in place" (cf. supra). In this respect, "the reuser shall without undue delay, where appropriate with the assistance of the PSB, inform the legal persons whose rights may be affected in case of an unauthorized reuse of non-personal data" (or, in other words, of a data breach).

Where the reuse of data cannot be granted under the conditions and safeguards listed above, the PSB shall make "best efforts […] to provide assistance to potential reusers in seeking permission from the third party(ies) whose [confidentiality] rights are at stake. Should the third party(ies) *not* grant permission, the PSB shall "ensure" that the confidential information is not disclosed as a result of allowing reuse.

Chapter II also lays down specific safeguards in case of transfer of data to third countries.

[190] DGA proposal, Art. 3(2)(a).
[191] Namely, Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Analysis of the final compromise text in view to agreement, Interinstitutional File: 2020/0340(COD), 10.12.2021.
[192] Ibid.
[193] Ibid, Art. 5(1) (2).
[194] Ibid, Art. 5(3).

Guidance for RNE -

- In the current state of the legislative process, the data held by, respectively, RNE and the IMs are outside the scope of chapter II of the DGA proposal.
- This being, Chapter II of the DGA proposal constitutes an interesting precedent for RNE and RNE members, in attempting to further share data while confidentiality of third parties could simultaneously be at stake. While the legal implications of the existence of confidentiality obligations in the SERA Directive are not clear (see section 3 below), Chapter II of the DGA could constitute an interesting interpretation grid.
- Chapter II of the DGA proposal deals with the question how to alleviate the obstacles to further data sharing by PSBs constituted by the presence of confidential information. It takes both the existence and scope of confidentiality obligations for granted. Chapter II of the DGA can therefore *not* be used to inform on the interpretation of the *scope* of confidentiality obligations in the SERA Directive, but 'merely' of their legal implications.
- First, Chapter II of the DGA proposal is based on the principle that the existence of confidentiality does not imply a total ban on further processing and sharing.
- Second, Chapter II of the DGA proposal envisages an array of both legal and technical mechanisms to protect *i.a.* confidentiality of data while enable further reuse. Such mechanisms could also be used by RNE and RNE members as part of their data policy.

2.3.2.2. Chapter III - Data intermediaries

The EC intends to structure and regulate the market of data intermediaries and thereby bring trust to data holders and data users, with the expectation that they would be incentivized to share their data more. As data have become a commodity in the data economy (see section 2.2.1.2 "Problem statement: From the abstraction to the commodification of data"), the EC aims to expand the trading of data so as to foster data reuse. In order to do so, the DGA proposal lays down a comprehensive and heavy-handed regulation. This sub-section focuses on the identification and scope of "intermediation services between data holders which are legal persons and potential data users".[195]

Such data intermediaries are not clearly defined in the DGA proposal. They consist in "intermediation services between data holders which are legal persons and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users."[196] The very core notion of "intermediation" is not defined. The description of such data intermediaries is so broad that it would basically encompass any type of mere support provided to data holders and users to facilitate the exchange of data.

Recital 22 aims to clarify the scope:

- First, only data intermediaries that have "as a main objective" the establishment of a relation between data holders and users and "the assistance to both parties in a transaction of data

[195] DGA proposal, Art. 9(1)(a).
[196] Ibid.

assets between the two" should be in the scope, which excludes companies or other entities (such as RNE) providing support to data exchange as an ancillary activity.

- Second, only services "aiming at intermediating between an indefinite number of data holders and data users" should be in the scope, thereby excluding the facilitation of data exchange meant to be directed at closed groups of data holders and users.
- Third, cloud services should be excluded.
- Fourth, service providers that "obtain data from data holders, aggregate, enrich or transform the data and licence the use of the resulting data to data users, without establishing a direct relationship between data holders and data users" should be excluded from the scope, such as advertisement or data brokers. However, data intermediaries "should be allowed" to adapt the data exchanged "to the extent that this improves the "usability of the data by the data user where the user desires this, such as to convert it into specific formats". Where to draw the line between "more usable data" and "enriched data" is not clarified.
- Fifth, services that "focus on the intermediation of content, in particular on copyright-protected content" should be out of scope. The need to exclude such services can be associated with the broad definition of "data" in the DGA proposal (see Part I).
- Sixth, "data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms developed in the context of objects and devices connected to the IoT that have as their main objective to ensure functionalities of the connected object or device and allow value added services" are out of scope.
- Seventh, "'consolidated tape providers' in the sense of Article 4 (1) point 53 of Directive 2014/65/EU […] as well as 'account information service providers' in the sense of Article 4 point 19 of Directive (EU) 2015/2366 […]" should be out of scope.
- Eighth and final, data altruism organizations operating on a not-for-profit basis are out of scope.

More than clarifications, recital 22 appears to regulate the scope *rationae personae* of the provisions of Chapter IV of the DGA proposal. Additionally, recital 22 does so by stating what is *not* in the scope without defining what *is* in the scope, which further obscures the interpretation.

The text resulting from the provisional agreement between the Council of the EU and the European Parliament does not fundamentally modify the notion and scope of data intermediaries. Although regrettably not in the body of the provision, the text does provide a definition in recital 22a, namely "services which aim at the establishment of commercial relationships for the purpose of data sharing between an undetermined number of […] data holders on the one hand and data users on the other hand, through technical, legal or other means […]".[197]

Guidance for RNE -

- RNE does not qualify as a "data intermediary" under the DGA proposal in its state as of the time of writing.
- Should RNE engage in further data commercialisation, it could use data intermediaries for supporting its business strategy.

[197] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Analysis of the final compromise text in view to agreement, Interinstitutional File: 2020/0340(COD), 10.12.2021, Rec. 22a and Art. 9.

2.3.3. Data Act

The European Commission issued the Data Act proposal on 23rd February 2022.[198] The Data Act can be pictured as a patchwork of various provisions, which differ quite significantly in terms of policy objectives and scope (both *rationae materiae* and *rationae personae*). The common thread of all chapters is obviously 'data' and the overarching goal of the European Commission to allocate the value arising from data in a fair manner. This overarching objective unfold in a number of specific ones pursued by the various chapters. First, Chapter II (jointly with Chapter X as an enabler) aims to allocate the value of IoT products data and in particular to empower IoT products users with respect to such data, vis-à-vis IoT products manufacturers. Second, Chapter III is aimed at constituting a *lex generalis* for data sharing obligations to be laid down in the future. There is a direct – although implicit – connection with data spaces, for which more specific (and especially, concerning mobility, sector-specific) data sharing obligations could be laid down in the future. Chapter III is thereby complemented by the provisions dealing with interoperability for data spaces in Chapter VIII. Chapter IV aims to mainstream the principle of fairness in B2B commercial data transactions, although only to the benefit of SMEs, which significantly reduces the scope of application. Following the Covid pandemic, Chapter V aims to allow public sector bodies to require access to data held by private entities in order, essentially, to fulfil exceptional needs. The Data Act regulates cloud and edge services in several respects. Chapter VI addresses lock-in vendor issues left unsolved by the Free-Flow of Non-Personal Data Regulation.[199] Similar to the provisions of the Data Governance Act concerning public sector bodies, data altruism organizations and data intermediaries,[200] Chapter VII aims to preserve the European Union 'digital sovereignty' by laying down safeguards applicable when a foreign law would require international transfer of non-personal data from cloud and edge services providers. Art. 29 lays down the essential requirements for interoperability for cloud and edge services, subject to further regulation by the European Commission.

The Data Act is therefore not truly horizontal, in the sense of context-agnostic. Most of its provisions target specific actors and specific range of data. Against this background, to what extent does the Data Act apply to RNE (data)?

Chapter II "Business to consumer and business to business data sharing" – Chapter II applies to the relationship between manufacturers of IoT products ("products" in the Data Act)[201] in their quality as 'data holder'[202] and thus duty-bearer on the one hand, and the IoT product user as beneficiary on the other. The IoT product user benefits from (i.) a right of access to the data generated by the use of such product, enforceable against the data holder and (ii.) a right to port or have data ported to a third party, especially for the purpose of being provided a service by such party. The data holder shall in particular not use non-personal data for a range of purpose detrimental to the user (such as deriving insights about the economic situation, asset and product methods of the user).[203] In any case, the data

[198] Proposal for a Regulation on harmonized rules on fair access to and use of data (Data Act), COM(2022)68 final ('Data Act proposal').
[199] Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303/59 ('Free-Flow of Non-Personal Data Regulation').
[200] On this topic, see Baloup and others (n 149).
[201] Or the service provider of « related services" within the meaning of Art. 2(3).
[202] See the definition of data holder in Art. 2(6). The data holder may be another party, such as the seller, renter or lessor of the IoT product or yet another party, see Art. 3(2).
[203] Data Act proposal, Art. 4(6).

holder can use the data only subject to a contractual agreement with the user.[204] Trains (but also possibly track beacons) could to some extent arguably qualify as IoT products under the Data Act proposal, although they have manifestly not be considered specifically.[205] However, RNE is neither an IoT product user nor an IoT product manufacturer - and therefore data holder *vis-à-vis* the user. RNE is therefore not concerned with Chapter II concerning its data. While not applicable to RNE (data), Chapter II appears to confirm the shift (identified in section 2.5 below) from 'data ownership' to 'data rights', possibly allocated to a plurality of actors.

Chapter III "Obligation for data holders legally obliged to make data available" – Chapter III does not directly lay down obligations to make data available to third parties. It provides a *lex generalis* applicable in case of such obligations laid down either in another chapter of the Data Act or in another EU (or national law when implementing EU) legal framework entering into force after the entry into force of the Data Act.[206] Data shall in particular be made available under fair, reasonable, non-discriminatory terms ('FRAND' terms) and in a transparent manner.[207] In sum, Chapter III is expected to apply to situations of data sharing obligations deriving from Data Spaces-specific legislation. With respect to the railways, the European Commission committed to revise TAP and TAF TSIs (see 3.2.2) as part of the Mobility Data Space. Should TAP and TAF TSIs be revised in the sense of laying down new obligations to make data available (with the reservation identified in the same section), the conditions laid down in Chapter III would then become applicable *ipso facto.*

Chapter IV – Unfair terms related to data access and use between enterprises – Chapter IV consists in data-specific regulation of B2B unfair commercial practices. The scope of application is however limited to (i.) contractual conditions imposed on (in the sense of not negotiated with) SMEs and (ii.) to contractual terms related to "the access to and use of data or the liability and remedies for the breach or the termination of data-related obligations". [208]

Chapter V - Making data available to public sector bodies and union institutions, agencies or bodies based on exceptional need – Chapter V lays down the legal framework applicable to what is commonly referred to as 'B2G' (business to government') data sharing obligations. RNE could be concerned by Chapter V in its quality as private body to whom public sector bodies and/or Union agencies or bodies could turn to case of "exceptional need to use data". Exceptional need to use data can be found to exist in the situations described in Art. 15. Any situation could possibly exist in the future, and in particular under Art. 15(c)(2). The application of the procedure provided by Chapter V Data Act, *i.e.,* via a request addressed to RNE as a central repository of railway data from all Member States (*i.e.,* on marshaling yards) could indeed "substantively reduce the administrative burden for data holders or other enterprises" compared to, for instance, requests addressed to every and all individual IMs. In

[204] Data Act proposal, Art. 4(6).
[205] IoT product ("product")is defined as "a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data". Whether the data exchanged between tracks and trains are communicated via a public or private electronic communication service remains to be analyzed. Another question arises, namely whether data should be generated automatically. Indeed, some of the data produced by the operation of train circulations are generated automatically while others are generated by human interactions, which may depend upon the safety system in place.
[206] Data Act proposal, Art. 12.
[207] Data Act proposal, Art. 8(1).
[208] Data Act proposal, Art. 13(1).

such case, the public sector body, union institution, agency or body in question should comply with the conditions laid down in Chapter V.

The remainder of the Data Act is of little relevance for the question of access, further sharing and right of use to RNE data. This being, Art. 34 ("Model contractual terms") mandates the European Commission to "develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations". Such model contractual terms would of course not be binding *per se.* They could however (i.) provide inspiration to private entities engaging in related contracts and (ii.) they could provide a yardstick for what is fair with respect to data access and use between parties. Whether and, if so to what extent, the European Commission could take inspiration from the ELI-ALI Principles, and especially concerning third parties rights, remains an open question.

Guidance for RNE –

- The Data Act proposal is not as horizontal in scope as one could have expected. Its most innovative provisions (Chapter II) are eventually sector-specific in the sense that they deal only with IoT products. More specifically, the provisions of Chapter II are targeted only at the relationship between the manufacturer and the user of IoT products and not at all situations where valuable data arise from the interaction between many stakeholders. As a result, they do not apply to RNE data.
- RNE could get inspiration from the model contractual clauses that the European Commission shall be mandated to draft, and which shall serve as recommendations for businesses (willing to) exchange(ing) data. However, RNE does not have to wait for such clauses which do not have a legal binding value and which have their own timeline (publication can probably not take place before roughly two years), misaligned with RNE's.

2.4. Scholarly proposal: the ALI-ELI Principles for the data economy[209]

EU law does not (yet?) contain a general framework for the regulation of data as an economic resource. In turn, the European Law Institute ('ELI') and the American Law Institute ('ALI') have designed comprehensive 'Principles for the Data Economy' for that very purpose. Albeit they have no direct legal binding value, the Principles can serve as a source of inspiration for one's data-related contracts and internal data policy. More than that, the Principles are likely to gain some legal value in the near-future, either as an interpretation grid for data-related disputes before Courts and/or competent administrative bodies (such as 'regulatory bodies' in the railways) or, more directly, as a source of inspiration for statutory law.

[209] https://principlesforadataeconomy.org/. This section is based on the last draft of the Principles available at the time of writing, namely the 'ELI final Council Draft', although not yet approved by ELI membership. The text is available here: https://principlesforadataeconomy.org/fileadmin/user_upload/p_principlesforadataeconomy/Files/Principles_for_a_Data_Economy_ELI_Final_Council_Draft.pdf (last visited 17th December 2021).

Part I – General provisions - Purpose and scope	
Purpose (Pl. 1)	The Principles are intended to be used primarily in both the EU and the USA. They could be used, partly or in whole, at different levels of the legal systems. They can govern contracts, they can serve to guide courts when dealing with data-related issues, such as data-related contracts and data-related unfair commercial practices. They can inform (sectoral) codes of conduct. They can also inform the law-maker when designing data-specific regulation. **Comments**: The European Commission endorsed the notion of (if not also the whole principles about) 'co-generated data' in the Data Strategy. **Application to RNE**: The expected added-value of the Principles for RNE could be the following ones: - The Principles could be used to inform RNE data policy, with the aim to play a role in the data economy while preserving the legitimate interests of stakeholders (and especially IMs and RUs); - The general obligation for IMs to protect confidentiality of RUs is subject to diverging interpretations by the various IMs. There is no clear framework, which results in incentivizing the IMs to be conservative. The ALI-ELI Principles could serve to provide an interpretation for such general confidentiality obligation and thereby secure RNE and the IMs.
Scope (Pl. 2)	The Principles are expected to apply to data in the sense of "records of large quantities of *information as an asset*, resource or tradeable commodity" (emphasis added). Not in the scope: - "functional data" ("data the main purpose of which is to deliver particular functionalities, i.e. computer program) - "representative data" ("data the main purpose of which is to represent other assets or value, i.e. crypto-assets") **Comments** Only digital data are in the loop: the aim is to regulate the data economy. The intention is to tackle data traded "for itself" as a good. They adopt a functional (rather than essentialist) approach, i.e. depending on the function that data play in a given transaction / situation. The same data could serve as both a tradeable commodity and representative data, depending on the context. The Principles are intended to apply to data transactions / data contracts on the one hand and data rights on the other: - Data transactions / data contracts: the Principles constitute by default rules, which could serve as source of inspiration for parties, judges and the law-maker.

	- Data rights are not necessarily meant to apply in a contractual context (see below). They are intended to serve as source of inspiration for statutory law.
Part I – General provisions **-** **Founding notions (Pl. 3)**	
The controller & Control of data'	"The person that, alone or jointly with other persons, has control of data" & "Being in a position to access the data and determine the purposes and means of its processing" **Comment**: *de facto* control of data. The definition is inspired by data protection law, with the difference that the controller shall have access to data, while the ECJ ruled in several occasions[210] that one does not have to have access to data to qualify as a controller within the meaning of the GDPR. Just like in the GDPR, the data controller is the main duty-bearer.
Co-generated data	"Data to the generation of which a person has contributed, such as by being the subject of the information or the owner or operator of that subject, by pursuing a data-generating activity or owning or operating a data-generating device, or by producing or developing a data-generating product or service". **Comment**: The co-generation of data is the trigger for the application of the 'data rights'. Co-generator(s) of data have enforceable rights against the data controller. There are several ways by which one can co-generate data, as a result of the cumulative use of both property law and personality rights rationales. The proposed data rights for co-generators of data aims to account for the roles of the various stakeholders in the coming into existence of data. The term "co-generated data" was coined by ALI-ELI and constitutes the main innovation of the Principles.
Derived data	"Data generated by processing other data; includes *aggregated* data and data inferred from other data with the help of external decision rules" (emphasis added). The term reflects the dynamic character of data in the data economy and the fact that data are often generated on the basis of other data.
Data right	"Right against a controller of data that is specific to the nature of data and that arises from the way the data is generated or from the law for reasons of public interest". The Principles foresee two sources of data rights: - Private law-style rights arising from the co-generation of data;

[210] CJEU 5 June 2018, C-210:16, ECLI:EU:C:2018:388 ('Wirtschaftsakademie case'), CJEU 10 July 2018, C-25/17, ECLI:EU:C:2018:551 ('*Jehovan todistajat* case'); CJEU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 ('*Fashion ID* case'). On this, see Ducuing, Charlotte; Schroers, Jessica; 2020. The recent case law of the CJEU on (joint) controllership: have we lost the purpose of 'purpose'?. Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht; 2020; Vol. 2020; iss. 6; pp. 424 – 429

Different types of data 'supply': - **Transfer v access** - **Porting of data (data portability)**	- Public law-style rights arising from public law rule, typically access rights aimed at ensuring the competitive order. The term "data rights" is (as of yet) unknow to the EU legislation but already in use in the literature to describe "rights that do not clearly qualify as personality rights or property rights but lie somewhere in between". Access means "being in a position to read the data and utilize it, in unspecified or specified ways, and with or without having control of that data." In contrast, transfer means that "the supplier puts the recipient in control of the data supplied. This normally implies that data is to be physically stored on a medium within the recipient's sphere of control. Transfer does not imply that copies of the data are subsequently erased by the supplier". **Comment**: the notion of "transfer" aims to adapt this of "sale" in property law to the specificities of data in the data economy. However, because data are non-rivalrous goods, no erasure of the original data is required and the supplier does not commit to exclusive transfer. "Requesting or otherwise initiating the transfer of data controller by another party to oneself or to a particular third party". The notion is taken from the GDPR (Art. 20 GDPR).
Part II – Data contracts (*short overview*)	
Data transfer contract (Pl. 7) **Contract for simple access to data (Pl. 8)**	The data contracts principles aim to provide guidance as for the various types of data contracts, by analogy with existing taxonomy of contracts in general contract law. A single contractual relationship may well contain a combination of several types of data contracts. (for further details, see Part II). As close as possible to 'sales contract', adapted to the specificities of data: i.e. in principle, no limitation to the (purpose of) use of data; the supplier shall 'clear' data from third parties' rights (e.g. IPRs). Data transfer contracts amounts to placing the recipient in a position of control of data. With such contract, the supplier remains fully in control of the data (as opposed to data transfer contract). There is generally no distinction being made in the law between data transfer contract v contract for simple access to data. **Comment**: Because of the specificities of data, the relationship between data transfer contract and contract for simple access to data is a continuum rather than a clear-cut distinction, because of the specificities of data. Besides, the Principles offer archetypes, which can and should be adapted to the needs of the parties.

Contract for exploitation of a data source (Pl. 9)	The focus of the transaction is the data source (i.e. device) rather than the data. It implies *i.a.* the supply of *all* data from the data source in real time (in the IoT environment). Such a contract implies no data quality or quantity requirement for the supplier. Contracts for exploitation of a data source cannot easily be analogized with other contracts, but the most similar could be contracts for the lease of a device of facility.
Contract for authorization to access (Pl. 10)	The contract for authorization to access resembles the contract for exploitation of a data source, but the supplier ('authorizing party') has a passive role. His obligations are therefore less stringent. *i.e.* there is no obligation to facilitate the access of data incumbent on the authorizing party to the benefit of the recipient. Similarly, duties with respect to third parties(rights) are incumbent on the recipient. This model contract can typically serve for transactions between online businesses and consumers, who 'pay' a 'free service' by allowing for the use of 'their' personal data.
Contract for data pooling (Pl. 11)	This contract is not about a supplier v recipient of data, but rather about joint sharing – and sometimes exploitation – of data between 'data partners', while different (technical, legal, organizational) means can be used. The contract is based on a 'license' rather than 'sales' approach, in the sense that data are shared within the pool only for a given purpose. The contract includes clauses concerning the creation of IPRs on the derived data. The contract also anticipates the situation where a data partner leaves the data pool.
Contract for the processing of data (Pl. 12)	This contract is about the transaction where a processor undertakes to process data on behalf of the controller (such as cloud computing, data scratching, data analytics services, …). The clauses are inspired by the GDPR, *i.e.* the fact that the processor shall not process data for his own purposes.
Data trust contract (Pl. 13)	"A data trust contract is a contract among one or more controllers of data (the 'entrusters') and a third party under which the entrusters empower the third party (the 'data trustee') to make certain decisions about use or onward supply of data (the 'entrusted data') on their behalf, in the furtherance of stated purposes that may benefit the entrusters or a wider group of stakeholders (the 'beneficiaries')." The term "trust" does not necessarily refer to the Common Law "trust"; a distinction should be made between the data trust contract and the legal structure as a trust. PIMS (personal data management services) are typical 'data trusts'. **Application to RNE**: With respect to data processing, RNE appears to play the role of a data trustee for the benefit of IMs as data entrusters. Such role is however not based on a specific and dedicated data trust contract. RNE data activities on behalf of the IMs are rather subject to ad hoc decisions (within the meaning of RNE governance). ***A suggestion for RNE to move on with data exploitation is therefore to formalize its data policy in a dedicated document, subject to approval within the conditions of RNE governance***.
Data escrow contract (Pl. 14)	"Data escrow contract is a contract among one or more parties planning to use data (the 'contracting parties') and a third party (the 'escrowee') under which the escrowee undertakes to make sure the

	powers and abilities of some or all of the contracting parties with respect to the data are restricted (the 'restricted parties') so as to avoid conflict with legal requirements, such as those imposed by antitrust law or data privacy/data protection law." With this contract, the 'restricted parties' voluntarily surrender control in the hands of the escrowee, most often so as to ensure compliance with legal obligations.
Data marketplace contract (Pl. 15)	"A data marketplace contract is a contract between a party seeking to enter into a data transaction (the 'client') and a data marketplace provider, under which the data marketplace provider undertakes to enable or facilitate 'matchmaking' between the client and other potential parties to data transactions and, in some cases, provide further services facilitating the transaction."
<u>Application to RNE</u>: The data contracts under the ALI-ELI Principles provide a taxonomy of data transactions types as well as templates for data-relevant clauses. This could help RNE update its data contracts templates. Instead of differentiating between B2B v B2G data contracts, RNE could for instance differentiate the data contract types following ALI-ELI taxonomy. In this respect, it should be born in mind that data transactions types under ALI-ELI Principles can be combined in one single contractual relationship (*i.e.* the 'data escrow contract' would typically back another type of data supply contract).	
Part III Data rights - **General presentation**	
<u>See below:</u> - **Part B – Co-generated data;** - **Part C – Data rights for the public interest**	With the concept of 'data right', the ALI-ELI Principles aim to create new rights, which arise from the specific features of data as an economic asset, i.a. (i.) the fact that it is a non-rivalrous asset (ii.) often created by the various contributions of many stakeholders in the data economy. Data rights are not (necessarily) contractual. Data rights can arise from either the co-generation of data (private law) to the benefit of the co-generator(s) of data or from statutory rules of a public law nature (such as access rights to prevent anticompetitive behaviors). Data rights are to be enforced against the data controller(s). In the former case, the data rights "fulfil functions similar to those fulfilled by ownership with regard to traditional rivalrous assets", by unbundling the bundle of property rights and granting them to the various stakeholders. Data rights are flexible in nature, in the sense that the granting of data rights depends very much on the context, i.e. on the involvement of the co-generators of data, on the legitimate interests at stake, etc. **<u>Comments</u>**: the proposed data rights are intended to serve as inspiration for statutory rights to be implemented by law, *i.e.* in the future Data Act proposal from the European Commission or as part of the regulation of unfair commercial practices. Data rights can also be used as founding principles for one's own data management and marketing policy, especially when one is the data controller and there are many co-generators of data. They can indeed serve to find a balance between the legitimate interests of the many stakeholders and overcome the "open access" v "closed data" dichotomy. The ALI-ELI Principles foresee 4 non-exhaustive data rights enforceable against the data controller: 1. Right to access;

	2. Right to desistance from certain data activities or, to the extreme, the right to erasure; 3. Right to correct data; 4. Right to an economic share in profits derived from the use of data. As for EU law, data rights are expressly inspired by legal mechanisms already in force, such as - Concerning 1/ right to access: data access regimes in various sector-specific legislations and data portability right in the GDPR; - Concerning the right to desistance: the right to require a controller to restraint from processing personal data (GDPR and, before it, the Data Protection Directive). Such right "fulfills a similar function as the right to reclaim physical goods". Other data rights could be foreseen, and especially rights ancillary and instrumental to the 4 data rights proposed by ALI-ELI, such as a right to be informed about the processing of data, instrumental to the exercise of all the other rights. **<u>Comments</u>**: The right to desistance can also by related to the purpose limitation principle in data protection law, by which personal data can be processed only for and insofar as required for a specific and legitimate purpose. The right to desistance amounts to prohibiting processing of data for some purposes and can therefore be viewed as a nuanced form of purpose limitation, the principle remaining freedom to process data.
Part III Data rights **-** **Part B – Data rights arising from co-generation of data**	
Co-generated data (Pl. 18)	To determine whether and to what extent one should be considered as co-generator of data, the following factors ought to be taken into account, in the following order of priority: 1. The "extent to which a party is the subject of the information coded in the data or is the owner or operator of an asset that is the subject of that information"; 2. "The extent to which the data was produced by an activity of that party, or by use of a product or service owned or operated by that party"; 3. "The extent to which the data was collected or assembled by that party in a way that creates something of a new quality"; 4. "The extent to which the data was generated by use of a computer program or other relevant element of a product or service, which that party has produced or developed". In order to grant data rights, the ALI-ELI Principles take into account the magnitude and investment of a party in the co-generation of data, both objectively and subjectively (in comparison to the contribution of the other parties). Data rights are mainly foreseen to consist in individual rights but they could also consist in collective rights (i.e. resulting from the generation of data by the citizens of a country, as represented by the State of other constituency). The term "generation" of data should not be understood technically but rather generally as the coming into existence of data.

General factors determining rights in co-generated data (Pl. 19)	The factors based on which one is to qualify as "co-generator" of data relate to, respectively, the theory of personality rights (such as personal data under the GDPR), the "labour theory of property" and the theory according to which the product of a thing should belong to the owner of the thing. **Comments**: Interestingly, the theory of personality rights is applied here (1st factor) not only to individuals (personal data being data relating to individuals, based on which individuals do have rights) but also to legal entities. They could be interested in two ways: first, when data relate to them as legal entities in a way similar to personal data; second, when data relates to an asset that is the subject of the information, such as a train or a piece of railway infrastructure. The factors for being recognized as a co-generator of data relate to either the syntactic level (such as 4th factor) or the semantic level (such as 1st factor) of data, namely the information encapsulated in the data. **Application to RNE data**: Considering TIS data, RNE would qualify as 'data controller' while the RUs and IMs would likely qualify as co-generator of data, for the respective data feeding the TIS ecosystem.
Access or porting with regard to co-generated data (Pl. 20)	Data rights are based on the notion of fairness. The recognition of a party as co-generator of data does not automatically lead to the granting of a data right, which depends also on - the circumstances and especially on the "share which a party had in the generation of the relevant data"; - the legitimate interest that the party can put forward to claim a certain data right (duty to state reasons); - the (counterbalancing) legitimate interests of the controller or of a third party in denying the data right; - the imbalance of bargaining power between the parties; - any public interest, such as fair and effective competition. The public interest factor, and especially fair and effective competition, may play a role both in favor of *granting* data rights (such as data access) and in *denying* data rights. Data rights shall be waivable unless stated otherwise in applicable law (such as in the GDPR). Data access rights are considered the most important data rights. Principle 20 provides further details as for the various types of legitimate interests that a party can put forward to claim a data access right. Principle 20 provides further details as for the restrictions which could/should be applied when granting a right of access, such as disclosure to a trusted third party, disaggregation, anonymization or blurring of data. Such restrictions can be a means for the data controller to accommodate both the right of access of a party on the one hand and the rights of third parties on the other (such as IPRs of privacy rights).
Desistance from data activities with regard to co-generated data (Pl. 21)	Similarly to Pl. 20 for data access rights, Pl. 21 lays down the conditions in which a right to desistance can be claimed. The right to desistance shall be justified by the risk that the data activity cause significant harm (whether of economic or non-economic nature) *and* the inconsistency between the purpose of the data activities and the way the party contributed to the generation of data. I.e. the party could not reasonably expect data to be then (re-)used for such a purpose.

	At the extreme, the right to desistance can amount to a right to erasure of data (see also in the GDPR, Art. 17). The right to desistance also shares similarities with other GDPR rights, and especially the notion of consent (based on the processing of data for a given purpose). However, the right to desistance departs from the spirit of the GDPR in that the processing of data is, by default, not subject to prior authorization and conditions. **Comments**: The right to desistance resembles a "weak" purpose limitation principle in the GDPR. It is weak in the sense that, by default, data processing is allowed, unless the processing of data by the controller for a given purpose proves to cause significant harm in the conditions laid down by Pl. 21. **Application to RNE data**: The right to desistance could help RNE commercialize data while taking into account IMs' legitimate interests. The principle being that RNE can freely commercialise data, IMs could claim a right to desistance against RNE concerning *certain* data processing activities. Following Pl. 21: - IMs could *i.e.* claim desistance for security reasons (non-economic ground) or for RU confidentiality reasons (economic ground). In the latter case however, IMs would stand for the interest of third parties (RUs), based on the contract that they have. It could be claimed, however, that IMs stand for their own interests, namely to not be sued by RUs or RBs for breach of confidentiality obligations. - It is clear that IMs did not produce and contribute 'their' data to the RNE pool for the purpose of commercializing them, but (only) for the purpose of planning / running international trains. This rule of reason is based on the principle that the processing of data should be free. Only in case of proved harm (or proved likelihood of harm) would data be considered confidential and therefore not further disclosed, or further processed for specific purposes and with specific safeguards in place. This reasoning is expected to accommodate the legitimate interests of all parties and serve the general interest of the data economy, namely to share and reuse data broadly, while preventing abuses (such as unjustified ban on any further processing). To make it workable and because the environment is a closed one where RNE and the IMs have a close and continued relationship, ***it is recommended to set up a joint data policy (see above).***
Correction of co-generated data (Pl. 22)	Co-generators of data can require from the data controller(s) the correction of data, based on (likelihood of) harm. Such data right serves the objective of data quality, in the interest of the co-generator(s) of data but also of the general interest that data be of high quality in the data economy. In principle, the data controller has an interest in having high data quality, but this is not always the case.
Economic share in profits derived from co-generated data (Pl. 23)	The right to an economic share in profits is viewed as exceptional, the by default rule being that co-generators of data are not entitled for feasibility reasons. The claim for such an economic share in profits shall be based on the exceptional nature of the contribution of the party, on the exceptional nature of the derived profit and on the unbalance of bargaining power between the co-generator of data and the data controller.
Part III - Data rights	

– **Part C – Data rights for the general interest**	
Justification for data rights and obligation (Pl. 24)	Data rights – most often, data access rights - can be justified by the public interest, irrespective of the contribution of one to the generation of the data. In such case, the data right shall be subject to a necessity and proportionality test as it interferes with the legitimate interests of the data controller (i.e. its freedom to conduct a business). The necessity and proportionality test shall apply both to the granting of the right and, where applicable, to the (*i.a.* technical, financial, …) conditions of application of such right. There is however an exception for data access rights enforceable against public entities ('open data' policies), which do not conduct economic activities and can therefore not claim a freedom to conduct a business. This being said, rights of third parties should be protected (such as IPRs or data protection). The public interest may *i.e.* consist in addressing a market failure (see Type-Approval Regulation, Art. 61), protecting the environment and preventing unnecessary harm to animals (REACH, Rec. 40 and Art. 27), preventing anticompetitive behavior
Granting of data access by the controller (Pl. 25)	Pl. 25 lays the conditions when the law grants access to data of a data controller: - The controller shall apply FRAND (Fair, Reasonable and Non-Discriminatory) conditions; - "Appropriate restrictions" should be designed so as to protect the legitimate interests of third parties or the public interest, *i.e.* "disclosure to a trusted third party, disaggregation, anonymization or blurring of data" where possible; - The controller shall pass on to the recipient (beneficiary of the data access right).
Data activities by recipient (Pl. 26) **& Reciprocity (Pl. 27)**	While Pl. 25 is about the conditions that the data controller shall comply with when providing access to data, Pl. 26 and 27 are about the conditions under which the recipient (beneficiary of the data access right) shall use the data. In principle, data can be used for any lawful purpose, provided not in a manner inconsistent with the purpose for which the data access right was granted and not harming the legitimate interests of the data controller beyond the intended purpose of the data access right. In principle, and depending on the context, the recipient (beneficiary) shall be bound by a reciprocal obligation to give access to 'their own' similar data. The principle is therefore freedom of use, given the expectation that broad reuse of data will deliver innovation and growth. Such a 'sales contract' approach is therefore favoured instead of a 'licence contract' one. However, data rights for the general interest being provided by the law, restrictions as for the purpose and conditions of use of data could also be decided.
Part IV Third Party Aspects of Data Activities **-** **Chapter A Protection of others against data activities**	
Wrongfulness of data activities vis-à-	These Principles provide for the protection of third parties rights, which shall be complied with by parties engaging in data activities (especially based on data contracts and data rights within the meaning of the Principles), failing what data activities are wrongful. Such third parties rights may *i.a.*

vis another party (Pl. 28) **& Rights that have third-party effect *per se* (Pl. 29)** **& Contractual limitations (Pl. 30)** **& Unauthorized access (Pl. 31)**	consist of data protection rights and IPRs (or 'data ownership', should such a right be applicable in a given jurisdiction) but also, in more limited conditions, contractual rights agreed upon. Data activities may also be wrongful when data were obtained by unauthorized means. Wrongfulness implies also to look at the conditions in which data activities are conducted, i.e. concerning data security measures. These principles are especially inspired by the GDPR (concerning data security as a safeguard) and by the Trade Secrets Directive (concerning third parties effect). It is of course for *applicable law to determine* the conditions in which rights of others should prevail over data activities and especially the exercise of data rights. In this respect, the European Commission announced that IPRs could be modified so as to facilitate the data economy. **Comments**: as many IP scholars have already discussed at length, the prevalence of IPRs (including the *sui generis* protection of databases) could endanger the data economy as a whole. It is not even sure that data rights could be exercised at all, should they not interfere with IPRs of third parties. The same goes for rights of third parties detracting from limitations granted contractually (*i.e.* downstream third party effects of contractual clauses in NDAs), which often substitute the absence of a general legal status of data. These principles are therefore vague and need to be substantiated with statutory rules to determine in how far existing rights of others can make data activities 'wronful'.
Part IV Third Party Aspects of Data Activities **-** **Chapter B: Effects of Onward Supply on the Protection of Others**	
Duties of a supplier in the context of onward supply (Pl. 32)	Upon supply of data, the supplier shall pass on to the recipient the duties and restrictions attached to the data (mainly IPR, privacy obligations and contractual limitations, see Part IV, Chapter A). The supplier shall also engage in proactive measures to ensure compliance by the recipient (and possible further downstream recipients). Essentially, the supplier shall engage in risk-based due diligence assessment of the recipient, which may at the extreme lead to renunciation to deal. After the deal, the supplier shall monitor compliance by the recipient to some extent and, upon knowledge of wrongdoings, take reasonable steps to stop them. The supplier is liable only for his own (due diligence) obligations and *not* for the activities of the recipient of further downstream recipient. The justification given by ALI-ELI rapporteurs for such far-reaching obligations relates to the large number of data transactions in the data economy, so that rights of one could easily get infringed along the data value chain. The extent of the obligations shall depend upon the context, and especially the relationship between the supplier and recipient (*i.e.* whether the recipient is another controller or a processor). These obligations resemble Standard Contract Clauses for the international transfer of personal data under the GDPR. **Application to RNE**: When sharing data with third parties, safeguards based on Pl. 32 could be designed by RNE in order to preserve the rights and legitimate interests of, *i.a.,* the IMs. Which

	concrete safeguards could / should be implemented could *i.e.* be integrated in the data policy of RNE and subject to prior discussion with the IMs.
Direct action against downstream recipient (Pl. 33)	Pl. 33 grants the initial supplier of data ('A') a direct action against downstream recipient ('C') who received data from the immediate recipient ('B'), in case C breaches terms imposed by B on behalf of A. **Comments**: Such direct action is inspired by legal mechanisms already in place in many jurisdictions for various types of contractual relationships. While data are volatile and the data economy implies many data transactions, data holders are often scared to share 'their' data for lack of the ability to control whether the terms and conditions they imposed have indeed been fulfilled in downstream contracts. A question remains however as to how the initial supplier can be made aware of an infringement by a downstream recipient. While the immediate recipient would (as a supplier himself) have due diligence and monitoring obligations (under Pl. 32), he may not be aware himself of all infringements by the downstream recipient. To solve this problem, a solution could be to contractually impose a marking of the data throughout the value chain, where possible.
Wrongfulness taking effect vis-à-vis downstream recipient (Pl. 34)	Pl. 34 deals with the situation of 'data thieves', in plain words the situation where data activities by a downstream data recipient shall be considered wrongful, following wrongful supplied by the immediate recipient to the detriment of protected parties (third parties or the initial supplier). Wrongdoing by the immediate recipient may consist in wrongful *control* of data, wrongful transfer of data or failure by the immediate supplier to pass on restrictions which would have prohibited the data activities of the data recipient. The downstream recipient is liable for data activities subsequent to such wrongdoing in the case where he had knowledge or should have had knowledge of it, while the extent of his duty of care depends on the circumstances. Pl. 34 includes exceptions which can be raised by the downstream recipient, *i.a.* the absence of "material harm" or the fact that data was generally accessible. In such case, data activities of the downstream recipient shall be deemed to not be wrongful. This is viewed by the rapporteurs as a means to protect not only the downstream data recipient confronted with complex 'tainted datasets', but also the data economy as a whole. Pl. 34 is deliberately inspired by trade secret protection and by the inducement of non-performance of a contractual obligation theory. It thereby resembles a weak 'droit de suite' for tangible assets protected as property (in which case the behavior of, including knowledge of the facts by, the downstream recipient would be irrelevant in principle).
Part IV Third Party Aspects of Data Activities **-** **Chapter C: Effects of Other Data Activities on the Protection of Third Parties**	
Duties of a controller with regard to data	Pl. 35 deals with the responsibility of the data controller. When deciding upon the purposes and means of data processing, the data controller shall notably take into account the duties and restrictions which weigh on the data. When dealing with derived data, the data controller shall decide

processing and derived data (Pl. 35)	whether and to what extent duties and restrictions applicable to the original data are also applicable to derived data, taking into account (i.) the level of similarity between original and derived data (*i.e.* the level of aggregation of individual data) and (ii.) the level of risk following the processing of derived data in comparison with original data. Pl. 35 aims to take into account the *dynamicity* of data. Data are indeed never the same in the data economy: they are constantly processed, which results in new data. Pl. 35 aims to find a balance between the following: - The legitimate interests of protected parties (under *i.a.* IPR regimes, data protection law, contractual restrictions decided by upstream suppliers, …) on the one hand, and - Feasibility considerations and the objective to foster – rather than prevent – data transactions in the data economy. Pl. 35 does not expressly deal with sanctions and remedies, since they should logically consist in the duties and restrictions weighing on the data.
Wrongful processing (Pl. 36)	Pl. 36 deals with remedies in case of wrongful processing (irrespective of the ground for wrongfulness). In principle, the controller shall undue wrongful processing (i.e. by disaggregating or deleting derived data). If not feasible or disproportionate, the controller shall pay monetary compensation to the damaged protected party(ies) instead. This should especially be the case when the contribution of the original data at stake is only minor to the derived data. The same may be applicable to downstream data-based products and services, subject to the necessary adjustments. Pl. 26 applies as a fallback principle, when duties and restrictions weighing on original data do not apply to the derived data.
Effect of non-material non-compliance (Pl. 37)	Pl. 37 consists in a recommendation that the law includes the rules that "wrongfulness with respect to some items in a dataset should not necessarily result in treating data activities with respect to the entire set as wrongful" and provides for criteria when this should, or respectively, should not be the case. This being said, the controller shall remove the data at stake from the data set for the purpose of future data activities upon notice of the non-compliance. The purpose of Pl. 37 is to prevent over-deterrence of parties in the data economy to share data for fear of disproportionate sanctions and liability for minor non-compliance.
Part V – Multi-State issues ***(not covered here)***	

2.5. Opening: from ownership to 'data rights'?

It is generally agreed that there is neither such thing as 'data ownership' nor should there be (see 2.2.1.2). Following the abandonment of the 'data producer's right' option once contemplated by the European Commission, the debate on 'how to allocate the value arising from data' has shifted, first, to data access rights and, second, to data governance regulation (see the new orientations of the EC under the Data Strategy, section 2.3.1).

Following the PSI Directive, data access (or 'sharing') rights have been imposed in various sectors, such as in the energy and in the banking sectors. Data access rights are often found to pursue either (1) competition or (2) innovation purposes (while the two rationales may be cumulative),[211] by making data accessible (1) to actors active in the same value chain who could suffer from anticompetitive foreclosure of data and /or (2) to a broader range of actors so as to incentivize data-based innovations, possibly beyond the original sector. Following the data portability right granted to data subjects by the GDPR concerning personal data that they 'provide' to service providers,[212] data portability has also been contemplated more generally as an interesting legal instrument supporting switching between data-related service providers and thereby conducive to more competitive markets.

The Data Governance Act proposed by the EC in 2020 followed a heated scholarly debate on the need to foster various types of data governance mechanisms, from data markets to data cooperatives or data commons. Data governance mechanisms are expected to enable both individuals and companies to enter the data economy and share 'their' data without losing being unfairly treated (*i.e.* by the Big Tech companies). The variety of data governance mechanisms is expected to adapt to the various context and expectations of stakeholders concerning data. By providing them with a legal framework, the Data Governance Act proposed by the European Commission recognizes the long-standing need for laws to support (data) resource exchange, and especially to support markets.

In sum, the abandonment of the data producer's right option did also amount, more generally, to the abandonment of the idea to create horizontal (in the sense of sector-agnostic) substantial rights so as to allocate the value arising from data.

The ambition to create horizontal rights on data so as to allocate the value arising from them may however revive with the bourgeoning notion of 'data right'. The notion of 'data right' was coined by the Chinese scholar Lian Yuming in 2019.[213] He observes, first, that data are at the crossroads of many legal branches, such as property law, personality rights, intellectual property rights or trade secrets. Second, the features of data make it a poor fit for the traditional "one ownership for one object" principle of property law. Against this background and inspired by the GDPR rights of data subjects, Lian Yuming proposes the creation of a combination of different data rights, to be afforded to various stakeholders and inspired by both personality rights and property law. While ownership is based on exclusive possession as a principle, data rights shall be based on a sharing principles, given the non-rivalry and ubiquity of data. Inspired by Lian Yuming, the ELI-ALI Principles for the Data Economy provide for a suggested framework for the allocation of value arising from data based on the creation of 'data rights' (see section 2.4). The data rights under the Principles for the Data Economy display significant differences from the Lian Yuming proposal, and especially the fact that they shall be enforceable against the data controller. This being said, three main principles remain. First, data rights constitute a specific range of data-specific rights so as to take into account the specific features of data. Second, data rights shall be allocated to various stakeholders simultaneously *on the same data*, thereby doing away with the exclusivity as core feature of ownership rights. Third and relatedly, data rights are based on data sharing or access. The same notion of 'data right' with the exact same meaning as the ELI-ALI Principles for the Data Economy's is used in the Opinion of the German Data Ethic Commission, which endorses the ELI-ALI Principles related to data rights.[214] The Data Act proposal, and

[211] Ducuing (n 116).
[212] GDPR, Art. 20.
[213] Lian Yuming, *Data Rights Law 1.0 - The Theoretical Basis* (Peter Lang Ltd 2019).
[214] 'Opinion of the Data Ethics Commission' 238.

especially its Chapter 2 on the regulation of IoT product data seems to be (implicitly) based on a similar notion of 'data rights', inspired by GDPR rights granted to data subjects.

3. The confidentiality obligations in the Single European Railway Area Directive

The present section is based on a combination of both (i.) desk research and (ii.) empirical research. The latter is based on data gathered through a semi-quantitative semi-qualitative survey. As a first step, a questionnaire was designed by RNE and circulated to all RNE members (see Annex 1). As a second step, one-to-one meetings took place with 4 RNE members based on a set of guiding open questions. The 4 RNE members were chosen so as to represent the diversity of legal situations across RNE members, with (i.) Bane NOR (Norway) and Trafikverket (Sweden) having a policy of minimum confidentiality, (ii.) ADIF (Spain) having a high degree of confidentiality policy, and (iii.) ProRail whose confidentiality policy has evolved from high to a lesser degree.

The section is divided in three sub-sections. We will first present the confidentiality obligations that IMs shall abide by under the Single European Railway Area Directive, based on concrete examples. They are of general nature, with little guidance, which makes it difficult to interpret them and even more so to have a harmonized interpretation throughout the EU. The second sub-section looks into the impact of other EU railway legal frameworks on confidentiality obligations. Then, the third and last sub-section focuses on the impact of the liberalization process and fair competition as objectives of railway law, on confidentiality obligations.

3.1. Outline of the confidentiality obligations

3.1.1. The applicable legal framework

IMs have confidentiality obligations to the benefit of their customers – RUs – pursuant to EU railway law and especially the Single European Railway Area Directive ('SERA Directive') as consolidated, which are reproduced plainly here.[215]

Charges - Pursuant to Art. 29 of the SERA Directive concerning the establishment, determination and collection of charges, "an IM shall respect the commercial confidentiality of information provided to it by applicants" (Art. 29(4)). Art. 32 related to exceptions to charging principles further states that, in the case of exceptional charging levied by the IM, information shall be provided by the IM in the network statement to prevent discrimination, namely to ensure that "any given infrastructure manager's average and marginal charges for equivalent use of its infrastructure are comparable and that comparable services in the same market segment are subject to the same charges". However, the IM shall provide such information only "in so far as this can be done without disclosing confidential business information" (Art. 32(5)).

Capacity allocation – The IM is in charge of the capacity-allocation processes. In particular, the IM shall ensure that infrastructure capacity is allocated "in a fair and non-discriminatory manner and in accordance with Union law" (Art. 39(1)). When doing so, the IM shall "respect the commercial confidentiality of information provided to [it]" (Art. 39(2)).

[215] Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area Text with EEA relevance, OJ L 343/32 ('SERA Directive'). Confidentiality is also a condition for the outsourcing of infrastructure management functions, pursuant to the SERA Directive, Art. 7(c). Such confidentiality clause is however not discussed here as it is deemed to lie beyond the scope of the present analysis.

In the context of capacity allocation, the IM may conclude a framework agreement with an applicant pursuant to the conditions laid down in the Directive (Art. 42(1)). In order to prevent discrimination, the Directive further requires the IM to make the "general nature of each framework agreement […] to any interested party" while however "respecting commercial confidentiality" (Art. 42(7)).

The Directive regulates the situation where, confronted with conflicting requests for infrastructure capacity, the IM shall conduct a coordination of requests in order to "ensure the best possible matching of all requirements" (Art. 46(1)). Coordination is based on the disclosure of information, namely "train paths requested by all other applicants on the same routes", "train paths allocated on a preliminary basis to all other applicants on the same routes", "alternative train paths proposed on the relevant routes […]", "full details of the criteria being used in the capacity-allocation process". Such information shall however be provided "without disclosing the identity of other applicants, unless applicants concerned have agreed to such disclosure", with a reference being made to the confidentiality obligation stated in Art. 39(2) (Art. 46(3)).

3.1.2. Problem statement

Confidentiality obligations incumbent on the IM appear to mainly consist of principle-based obligations, in the sense that they "emphasize general and abstract guiding principles for desired regulatory outcomes". This can be contrasted with rule-based regulation which "prescribes or prohibits *specific* behaviors" (emphasis added).[216] In particular, confidentiality obligations incumbent on the IM provide little guidance on the following items, which are however required for the obligation to be applicable in a specific case:

- Concretely, which information should be deemed confidential and in which circumstances;
- The process for determining that information is confidential;
- The consequences of labelling information as confidential.

There is however one exception with Art. 46(1) dealing with confidentiality in the coordination process, which presents itself as a specific application of the general principle of confidentiality laid down in Art. 39(2). Pursuant to Art. 46(1), the confidentiality obligation consists in removing the link between information on train paths allocated to an applicant and the name of the applicant. In other words, it consists in anonymizing train path-related information in the context of the coordination phase so that direct competitors cannot access such information. This, however, does not answer all the questions. First, and depending on the market at stake, the anonymization process may be in vain, *i.e.*, in case where competition is limited to a few RUs on a given route, which raises the question of what the IM should do in such case. Second, because Art. 46(1) constitutes only an application of the general principle of confidentiality, it does not provide guidance on how the latter should be interpreted in general.

This being, in the case of Art. 46, the confidentiality obligation incumbent on the IM is quite obviously related – and instrumental – to the competition between RUs. It is indeed the competitive offer of train paths between RUs which triggers the need for confidentiality obligations. In the case of Art. 46, confidentiality obligations relate directly to the object of the transaction, namely the train path. The liberalization of railway carriage being the overall objective of the SERA Directive, there is little doubt

[216] Mark Fenwick, Wulf A Kaal and Erik PM Vermeulen, 'Regulation Tomorrow: Strategies for Regulating New Technologies' in Toshiyuki Kono, Mary Hiscock and Arie Reich (eds), *Transnational Commercial and Consumer Law: Current Trends in International Business Law* (Springer Singapore 2018) Section 5.2.

that confidentiality obligations should be understood as part of parcel of the legal apparatus regulating the newly created market for train paths and, more generally, the activities of IMs to the benefit of RUs and applicants more in general. However, how and to what extent the liberalization process should drive the interpretation of confidentiality obligations requires further analyses.

Both charging- and capacity allocation-related provisions are under the supervision of the railways regulatory body[217] (Art. 55). It is therefore up to the regulatory body, subject to judicial review, to interpret confidentiality obligations. However, at the time of writing, no clarification of the scope of confidentiality obligations in the SERA Directive has been provided by any regulatory body across the EU (see Annex 2/Question 7).

With the exception of the confidentiality obligation of Art. 46(3) which was included with the adoption of the SERA Directive, all confidentiality obligations stem from the earlier Directive 2001/14[218] (namely, Art. 4(6), 8(3) and 17(6)). Apart from Art. 8(3), the confidentiality obligations incumbent on the IM were already present in the Proposal from the European Commission.[219] Such obligations were not discussed in the preparatory works. In any case, the confidentiality provisions of the SERA Directive are subject to national transposition. They can be – and as a matter of fact, they are often – further substantiated by contractual (such as the 'contract of use') or otherwise legal terms (such as the network statement) regulating the relationship between the IM and the RUs. Finally, confidentiality obligations pursuant to the SERA Directive are without prejudice to other confidentiality or secrecy obligations, *i.e.*, for security purposes.

Some aspects remain unclear at this point. In particular, what "confidentiality" exactly means and what concrete interests it protects, remains an open question. Concretely, the Directive does not clarify whether the mere existence of a link between information and a RU or applicant would suffice to label it as confidential. Alternatively, the confidentiality obligations could be aimed at protecting certain (commercial) vested interests. It can be contrasted with the Trade Secret Directive, which clarifies, in the definition of "trade secret", what a trade secret is and why it should be protected (namely, because there is commercial value in the very secrecy of a given information) (see section 2.1.4). In contrast to trade secret protection, confidentiality obligations are aimed at protecting the interests of a party who does not hold the information (in this case, the RU while the IM holds the information). This questions, therefore, what process should be in place for labelling certain information as confidential *i.e.*, whether the IM could or should apply a harm-based screening of confidentiality claims from RUs. This, however, is also not tackled by the Directive.

Similarly, the lack of clarity of the scope of confidentiality obligations *rationae materiae* does not relate only to which *specific* information should be considered confidential, which could be related to the state of the market (see above). It also relates to the area covered by confidentiality. Does confidentiality apply *strictu sensu* to charging and infrastructure capacity allocation, as the location of confidentiality obligations in the body of the Directive would suggest? Or does confidentiality apply generally to all information, irrespective of the area at stake, which would include *i.e.*, traffic management-related information? Another way of phrasing the question is to look at the

[217] SERA Directive, Art. 55.

[218] Directive 2001/14/EC of the Council of 26 February 2001 on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification, OJ L 75/29.

[219] Proposal from the European Commission for a Council Directive relating to the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification, /* COM/98/0480 final - SYN 98/0267 */, OJ C 321/10.

confidentiality obligations from a phased-based approach. Does the IM have confidentiality obligations when conducting charging- or capacity allocation-related tasks *only* or does the obligation to protect confidentiality extend also to traffic management as a function of railway infrastructure management?

Another question relates to whether confidentiality obligations apply 'only' to information "provided to" the IM (see Art. 29(4), 32(5) and 39(2)), implicitly "by the applicant" (whether RU or not) or do confidentiality obligations apply to, potentially, any information, including information that could be *produced by the IM* (see Art. 42(7) does not refer to information 'provided to' the IM by the RU)? The latter would evidently considerably broaden the scope of confidentiality obligations *rationae materiae.* It would seem only logical to have differences between freight vs passenger traffic, where passenger traffic is open to the general public while freight traffic operates based on B2B over-the-counter contracts. However, to what extent distinctions should be made between them remains also unclarified in the Directive.

The legal consequences of labelling information as 'confidential' is not dealt with explicitly in the Directive. Theoretically, the labelling of information as 'confidential' could, for instance, prohibit the disclosure of such information, it could require the anonymization of information prior to disclosure (as regulated, by exception, in Art. 46(3)), it could otherwise require information to be aggregated or disclosed only to certain third parties or for a limited range of purposes, etc. The Directive does not clarify this point.

Finally, it should be noted that RNE is not an IM and is therefore not directly subject to confidentiality obligations pursuant to the SERA Directive. When (deemed) confidential information is shared by IMs with RNE (*i.e.,* for the purpose of making international train path or in relation to the traffic management of international circulations), IMs disclose them to RNE subject to contractual confidentiality obligations.

3.1.3. Going concrete: data and information in the railways

The following table gives a taste of the diversity of data and information types which could respectively be tackled by the confidentiality obligations, based on the results of the empirical research. The table is notably based on the contentious items identified in the sub-section above, namely the type and nature of information or data, how they are generated and by whom (*i.e.*, whether the RU, the IM or both), the phase(s) in the lifecycle of the train that they refer to and/or are generated from. Finally, the table summarizes the status of information or data as confidential or not and, where so, the rationale for labelling information as confidential. The table is not aimed at providing exhaustive information on the topic but only to show the diversity of cases.

Type of information	**Nature of information or data (static vs real-time, specific vs aggregated vs anonymized, etc.)**	**How the information is generated (*i.e.*, whether 'provided by' the RU)**	**Phase in the lifecycle of the train (capacity allocation phase, train circulation phase, post-circulation phase)**	**Whether labelled as confidential or not and rationale for labelling as confidential where appropriate**
Train path information	The train path is the object of the transaction between the RU and the IM. Train path information constitutes rather static information. In principle,	Depending on whether related to a train path request or to an allocated train path, information is produced either by the RU or by the IM.	Train path information, whether related to a train path request or to an allocated train path are produced during the capacity allocation	Train path information undoubtedly qualify as confidential information, which detracts directly from the Directive (see above).

	it can be directly related to an RU. Train path information could relate to requests for train path (by the RU) or to train path as allocated (by the IM). Train path information can theoretically be anonymized (*i.e.*, for the purpose of conducting coordination in case of conflicting requests), however depending on the state of the given market and, therefore, on the competitiveness of the market.	In the first case, information related to a train path request is actively provided by the RU. In the second case, information related to an allocated train path is actively provided by the IM, based on information provided by the RU. The nature of information to be provided by, respectively, the RU and the IM in the train path allocation process is further regulated in the TAP and TAF TSIs.	phase, namely prior to the train circulation.	This view should however be nuanced, following the rationale. Train path allocation information is confidential because it informs on business opportunities of the respective RU. As a result, train path information qualifies as confidential. However, whether the rationale for labelling such information as confidential after the capacity allocation phase remains valid, and, if so, why, is often un(der)discussed.
Train traffic information	Train traffic information can be related *i.e.*, to "train running information" in the TAP TSI (Point 4.2.15). It relates *i.a.* to "details of the current status of the train at agreed points". Train running information can be the same as train running forecast or in can deviate from it (*i.e.*, in case of delays, rerouting, ..). As visible from Point 4.2.14 TAP TSI, train traffic information starts with data captured at certain points of the network (most of the time, data are automatically generated upon circulation of the train). It is based on such 'raw' data that the IM can elaborate train traffic information (including new forecast).	Data is co-generated by the circulation of the train on the railway infrastructure, as captured by sensors on the infrastructure. Then, train traffic information is created based on the IM train traffic management IT systems. Information is therefore not actively 'provided by' RUs. This being, information is generated from the operation of the RU train on the IM network.	Train traffic information is created during the train circulation phase. Then train traffic information can be aggregated and further processed so as to create derived data and information, i.e. information on delays (see below).	Train traffic information is often considered confidential. Most often, it means that only the RU in question can access such information. The rationale for this is often, generally, that information relates to the RU and to the RU business. Confidentiality can be driven by security considerations, *i.e.*, the disclosure could inform on the location of trains parked at marshaling yards and therefore lead to thefts. Whether the status of such information as confidential remains in time (namely, after the train circulation phase), and if so why, remains un(der)discussed.

				The question what concrete harm could be caused to the RU by the disclosure of such information in given circumstances is not often discussed.
Delays	It depends. Delays information can be provided either in real-time (see TAP TSI, Point 4.2.16) or ex post (after the train circulation), either train-specific, RU-specific or aggregated. Aggregation of information can be monthly, yearly, etc. Information on delays can also be linked to the cause of delays (whether caused by the IM, by the RU or by external agents or circumstances), *i.e.*, for the purpose of the performance regime. As a result, information on delays can consist in a large array, from 'raw' data to elaborate forms of information.	See 'Train Traffic Information'. Aggregation of data is made at the IM. Similarly, the attribution of cause for delays is made by the IM, possibly under the supervision of the regulatory body and possibly with a right for the RU to challenge the information. In short, both delay-related data and more elaborate information are produced by equipment and staff of the IM, not of the RU. There is no definition of what 'provided by' means, whether it requires active provision (by the RU) or not. Should it not require active provision by the RU, whether the fact that IM equipment capture data from RU train to produce data could amount to passive 'provision' by the RU remains to be seen.	Delay-related data and information can arise at two phases, depending on the nature of such data or information: - Either from train circulation in real-time, namely during the traffic management phase; - Or post-circulation.	It depends. Real-time train-specific delay information for passenger trains is generally not considered confidential. Such information is often displayed to the general public, *i.e.*, in stations. On the other side of the spectrum, freight RU-specific monthly or yearly aggregated delay information linked with the cause of delays is often considered confidential. It would seem that information on (comparatively) poor performance by RUs could lower their commercial attractivity (vis-à-vis their customers).
Information related to passengers at train stations	Many information can relate to passenger at train stations, *i.e.*, camera footage or (more or less aggregated information on) number of passengers in trains and/or in the stations.	Information on passenger at train stations is at the crossroads of RUs, IM and train station operator (when different from RU and IM). Information on passengers at train stations can be elaborated based on various sources, *i.e.*, directly captured by camera belonging to an IM or a station manager, on RU	/	Many pieces of information related to passengers at train stations are often deemed confidential, because such information relates to the business (model) of passenger RUs. The sharing of information related to passengers at train stations to the train station operator when the train station operator is also

		information on passenger traffic, etc.		an (the incumbent) RU could constitute an advantage for the latter when competing with other RUs.

The table shows, first, that for every general type of information (*i.e.*, "train traffic information") a great array of data and/or information can be concerned, from *i.e.*, raw data stemming from network-based sensors to train- or RU-specific information, through aggregated information (and aggregation can be made in different ways). Every type of data or information raises distinctive questions, under the confidentiality obligations legal regime. With the exception of train path request information which is actively "provided by" RUs (or applicants more generally), data and information seem to be mainly generated at the IM, namely either manually or based on network-based sensors. Information can relate to different phases in the lifecycle of the train. Whether data or information generated at a given phase should remain confidential during the subsequent phases, and if so why, is however not often documented. The rationale for labelling information as confidential is often based, generally, on the link with the RU or the RU business but it is not justified based on objective and concrete (potential) harm.

The label of information as confidential would often have far-reaching consequences, such as ban of any disclosure beyond the strict necessity of executing the IM obligations under the contract of use. Overall, it seems like, in the light of the uncertainty created by the Single European Railway Directive, most IMs often have an extensive interpretation of confidentiality obligations incumbent on them to the benefit of their customers, with few exceptions though.

Finally, it should be reminded that the information and data outlined in the table can serve as raw material for data processing activities (*i.e.*, at RNE), in turn leading to new data and information. Such new data and information ('derived data') can be more or less similar to the original data or information (as outlined in this table), such as (*i.e.*, route-based or weekday-based, etc.) statistics. The legal regime of such derived data under confidentiality obligations laid down in the Single European Railway Directive is not discussed here. It can however be assumed that the less similarity with the original data, the less harmful for RUs, and therefore the less likely such data and information should be deemed as confidential.

3.2. Impact of other legislation on confidentiality obligations

While the SERA Directive provides little guidance on the interpretation of confidentiality obligations, the latter are influenced by other legal frameworks. They are analyzed now in turn, based on question (in) how (far) they influence the interpretation of confidentiality obligations under the Single European Railway Directive.

3.2.1. The PRR: impact on the status of real time passenger train traffic data

The Railway Passenger Rights Regulation of 2007 ('PRR')[220] lays down the obligation for passenger RUs to provide passengers with information, in particular during their journey.[221] This includes information on connecting trains and delays. In the *Westbahn* case,[222] the question was raised to the CJEU whether

[220] Regulation No 1371/2007 of 23 October 2007 on rail passengers' rights and obligations, OJ L 315/14 ('PRR').
[221] PRR, Art. 8(2) and Annex II, Part II.
[222] CJEU, 22 November 2012, *Westbahn* case, C-136/11, ECLI:EU:C:2012:740.

the RU should provide passengers with information concerning its own trains only or, also, information concerning the trains of other – potentially competitive – RUs. The Court answered that the RUs should provide not only information concerning their own train services but also these of the other RUs or else passengers would be prevented from switching to another RU and would therefore be tempted to stay with the largest RU (namely the incumbent ÖBB RU in the case). The obligation to provide information on all trains is thereby viewed by the Court not only as beneficial to passengers but also as instrumental to the establishment of a level playing field. In other words, the obligation to provide such information is conducive to guaranteeing the competitiveness of markets.[223] This, however, requires logically that the RUs have acquired such information upstream from either the IM or the station manager. In other words, it requires a real-time flow of information on delays.

This pattern is reinforced by the New PRR[224] adopted in 2021 and which will enter into force in 2023. The New PRR introduces a new provision in Art. 10 "Access to traffic and travel information". IMs shall "distribute real-time data relating to the arrival and the departure of trains to RUs, ticket vendors, tour operators and station managers",[225] under regulated conditions.[226] In particular, data shall be provided via an API. Then, RUs have an obligation to provide other RUs, ticket vendors and tour operators that sell their services with access to certain information, and in particular information on "disruptions and delays (planned and in real-time)" that should be provided during the journey.[227] In other words, the New PRR codifies the case law of the Court and clarifies its logical consequence, namely that, for the RU to provide comprehensive information to passengers, such information should be provided to them upstream, *i.e.*, by the IM. This being, the expression "real-time data relating to the arrival and the departure of trains" (that IMs shall provide to RUs) is not further defined in the New PRR. In particular, the level of details that IMs should provide to RUs is not clarified. The scope of data can logically be interpreted to follow this of RU obligations. In this respect, real-time data relating to the arrival and the departure of trains should cover in particular regular train schedules and real-time adjustments to the schedule, such as delays, cancellations or rerouting. Against this background and following the *Westbahn* case, the scope of data should logically extend to train data not only of the beneficiary RU but also of other RUs.

The New PRR also regulates the conditions under which such data and information shall be provided, namely "in a non-discriminatory manner and without undue delay. A one-off request shall be sufficient to have continuous access to information". Both the IMs and the RUs may subject the provision of such data and information to the conclusion of a contract "or other arrangement" as a legal basis.[228] Both IMs and RUs bound to provide access to, respectively, real-time data relating to the arrival and departure of trains (pursuant to Art. 10(1)) and "minimum travel information" (pursuant to Art. 10(2)) may require a financial "compensation" from the data and/or information beneficiary (Art. 10(3)). RUs may require a "fair, reasonable and proportionate financial compensation for the costs incurred in providing the access" while IMs may require "compensation in accordance with the applicable rules".

[223] On this, see Charlotte Ducuing, 'Transport ferroviaire et protection des consommateurs' (2016) 3 Revue du Droit des Industries de Réseau (RDIR) 275, 281.
[224] Regulation (EU) 2021/782 of the European Parliament and of the Council of 29 April 2021 on rail passengers' rights and obligations, OJ L 172/1 ('New PRR').
[225] New PRR, Art. 10(1).
[226] New PRR, Art. 10(3).
[227] New PRR, Art. 10(2) and Annex II, Parts I and II.
[228] New PRR, Art. 10(3).

This calls for several comments. First, the 'compensation' is demonstrably not aimed as constituting a price for the data or information itself but rather a compensation for the effort exposed by the making available of such data or information, as visible for the compensation that RUs may request. Second, the mention that IMs and RUs may request the prior conclusion of a contract or other "arrangement" may misleadingly give the impression that all types of data or information provisions would be on equal footing. However, this may not be the case in view of the contractual ecosystem in the railways. For instance, IM-to-RU provision of information would in all likelihood qualify as an execution of the contract of use. In contrast, RU-to-RU provision of information consists concretely in the exchange of information between competitors.[229] Third and relatedly, the question consequently arises what it means for the compensation for the data provided by the IM to be "in accordance with the applicable rules". When it comes to data provided to RUs (as customers of IMs), the question arises how Art. 10(1) and (3) connects with the SERA Directive, and especially whether the provision of such data qualify as "all other information required to implement the service for which capacity has been granted"[230] as part of the minimum access package to be provided to RUs.[231] Alternatively, and with different consequences when it comes to charging, the provision of such data would qualify as an ancillary service ("provision of supplementary information").[232] Neither the New PRR nor the SERA Directive do clarify this question, which may be further regulated as part of national law. Given (i.) the fact that the provision of such data by the IM is mandated by law and (ii.) the justification of the Court in the *Westbahn* case that the provision of real-time data to RUs (including concerning the trains of other RUs) is a prerequisite for fair competition, it would rather seem that such data are "necessary" or RUs and would make part of the minimum access package. This being, the question remains open whether and how IMs may charge the provision of such data to other entities, such as the station managers, ticket vendors and tour operators. Fourth, this charging provision raises a consistency question, with reference to all the other data and information provisions (in particular by the IMs to other actors in the railway ecosystem) with respect to charging conditions.

Under Art. 9, RUs (and, where appropriate, station managers) have the obligation to provide the same information to passengers, "where possible based on real-time travel information, including by using appropriate communication technologies" (and a reference is made to the TAP TSI in this respect).

Finally, passenger RUs are under the obligation to set themselves service quality standards, to monitor their own performance and to publish a yearly report on their service quality performance. Service quality standards shall in particular relate to the punctuality of services.[233] This obligation can be viewed as a means for passengers to spur performance-based competition between the RUs.[234]

Practical guidance for RNE –

- To the extent that data are shared to the entire rail passenger transport ecosystem, including passengers, they can logically not be considered confidential.

[229] On the role of the PRR on the contractual ecosystem in the railways, see Ducuing (n 9).
[230] SERA Directive, Annex II, Point 1.
[231] SERA Directive, Art. 13(1).
[232] SERA Directive, Annex II, Point 4.
[233] PRR, Art. 28 and Annex III.
[234] Ducuing (n 9) 276.

- Real-time data relating to the arrival and the departure of passenger trains can therefore not be considered confidential. Travel information provided to passengers can also and obviously not be considered confidential either.
- Transparency obligations under the PRR to the benefit of passengers should, also, be understood as market regulation, given the overarching liberalization objective of railway law.
- More generally, the objective to set a level playing field between RUs appears to have consequences on the exchange (or conversely the confidentiality) of information.
- The information on punctuality of passenger services shall be made available by RUs to the general public. It shall therefore not be considered as confidential information.
- The provision of real-time data relating to the arrival and the departure of passenger trains by the IM to RUs and to a range of actors in the railway ecosystem (station manager, ticket vendors and tour operators) may be subject to charging, although the New PRR is unclear on the extent and ground on which IMs are allowed to charge. In this respect, whether the charging policy may differ depending on the beneficiary (*i.e.*, RUs as customers on the one hand vs other entities in the railway ecosystem on the other) is also an open question. In the case of provision of data from the IM to the RU, the question arises how such data qualify under the SERA Directive, whether as part of the minimum access package or an ancillary service, with different charging principles being applicable.
- Art. 10(3) New PRR invites to clarify the three situations in which the IMs (and RNE) may find themselves with respect to data provision:
    - First, the provision of data or information for *operational purposes* pursuant to a contractual agreement (such as the contract of use with the RUs) or to similar arrangements;
    - Second, the provision of data or information for *operational purposes* (possibly mandated by law) to other entities in the railway ecosystem, without the existence of a prior contractual relationship (or other arrangement). Such provision may be mandated by law, and in particular by the (New) PRR, which tends to mandate cooperation with the railway ecosystem for the sake of passenger rights and interests.
    - Third, the provision of data or information for non-operational purposes, and especially for commercial purposes ("data monetization"), to entities who may or may not be in the railway ecosystem and in all likelihood without the existence of a prior contractual relationship (or other arrangement).

3.2.2. Impact of TAP & TAF TSIs

The Technical Specification for Interoperability relating to the subsystem Telematics Applications for Passengers of the trans-European rail system ('TAP TSI')[235] and the Technical Specification for Interoperability relating to the Telematics Applications for freight subsystem of the rail system ('TAF

[235] Commission Regulation (EU) No 454/2011 of 5 May 2011 on the technical specification for interoperability relating to the subsystem telematics applications for passenger services of the trans-European rail system (consolidated), OJ L 123/11 ('TAP TSI').

TSI')[236] are based on the 'Interoperability Directive'.[237] According to the Interoperability Directive, telematics applications include applications for passenger services on the one hand, "including systems which provide passengers with information before and during the journey, reservation and payment systems, luggage management and management of connections between trains and with other modes of transports". On the other hand, applications for freight services include "information systems (real-time monitoring of freight and trains), marshalling and allocation systems, reservation, payment and invoicing systems, management of connections with other modes of transport and product of electronic accompanying documents".[238] TAP and TAF TSIs are aimed at meeting the essential requirements and ensuring the interoperability of the rail systems with respect to such telematics applications.[239] More concretely, TAP and TAF TSIs define "procedures and interfaces between all types of actors to provide information [in the scope of the respective TSIs].[240] The execution of the TAP and TAF TSIs relies on the joint efforts of railway actors (starting with IMs and RUs) to create specifications defining "the data exchange system based on common components and on the interconnection of the information and communication systems of the relevant actors". The TSIs also include "a description of the governance for the development, deployment and operation of this system".[241] TAP and TAF TSIs are indeed based on an iterative process where railway actors (starting with IMs and RUs) contribute actively to the system, as a result of which the TSIs are respectively revised.

TAP and TAF TSIs relate directly neither to data sharing obligations in the data economy nor to confidentiality obligations as per the SERA Directive. When it comes to information and data potentially protected as confidential under the Single European Railway Area Directive, the TAP and TAF TSIs are mainly about the standardization of exchange of messages between the IMs and the RUs concerning the allocation of train paths and train traffic management. Symptomatically, the main subject-matter of the TSIs is indeed the "message", between the IM and the RU. Concerning technical compatibility as an essential requirement served by the TAP and TAF TSIs, the Interoperability Directive requires that "steps must be taken to ensure that the databases, software and data communication protocols are developed in a manner allowing maximum data interchange between different applications and operators, *excluding confidential commercial data* […]" (emphasis added).[242] Such provision does neither lay down additional confidentiality obligations nor does it clarify the scope and consequences of confidentiality. It should be understood as a reminder that messages exchanged

[236] Commission Regulation No 1305/2014 of 11 December 2014 on the technical specification for interoperability relating to the telematics applications for freight subsystem of the rail system in the European Union […] (consolidated), OJ L 356/438 ('TAF TSI').

[237] Directive 2008/57/EC of 17 June 2008 on the interoperability of the rail system within the Community (Recast), OJ L 191/1, as revised by Directive 2016/797 of 11 May 2016 on the interoperability of the rail system within the European Union, OJ L 138/44 ('Interoperability Directive').

[238] Interoperability Directive, Annex II, Point 2.6.

[239] TAP TSI, Rec. 3.

[240] TAP TSI, Rec. 5.

[241] TAP TSI, Rec. 8.

[242] Interoperability Directive, Annex III, Point 2.7.1.

A similar reminder of the existence of confidentiality obligations was included in the TAF TSI as in force before the entry into force of the Commission implementing Regulation 2021/541 of 26 March 2021. As part of the governance structure for the execution of the TAF TSI, Point 7.1.4 of the Annex laid down the obligation for "stakeholders" (namely, IMs, RUs and wagon keepers) to, *i.a.*, "protect the confidentiality of customer relationships". In our view, such reference to confidentiality should be understood as a reminder of the existence of confidentiality obligations as a boundary condition. Such provision was not kept in the last version of the TAF TSI.

between IMs and RUs may contain confidential information, which the TAP and TAF TSIs should therefore not attempt to maximize the exchange. Indeed, the TAP and TAF TSIs are technical enablers for the performance of exchange of information as regulated under other legal frameworks, such as the SERA Directive[243] and the PRR (with respect to the TAP TSI).

When it comes to data sharing, the TAF and TAP TSIs do not lay down data sharing obligations. Both are however aimed at facilitating the exchange of information within railway stakeholders, which includes not only the IMs, RUs and applicants, but also the broader ecosystem. This is especially the case of the TAP TSI which, similarly to the PRR, includes also *i.a.* the ticket distribution value chain actors at large.[244] Similarly, the TAP and TAF TSIs are not concerned with who has entitlements on data ("ownership"). They are aimed at the sound execution of the exchange of messages with respect to the respective purposes of such messages. For this reason, a significant emphasis is placed on data quality and accuracy, evaluated with respect to the purpose of use. This is based on such considerations that *i.e.*, the TAF TSI lays down the principles that (i.) data should be recorded "economically", namely "on one single occasion for the whole transport"; (ii.) data should be "introduced into the system as close as possible to its source […]"; and (iii.) the originator a TSI message is "responsible for the correctness of the data content of the message […]".[245]

This being, the recent revision of the TAF TSI of 2021 introduces a new provision according to which a sender may charge for the sending of certain messages, namely Path Details message, Train Running Forecast message, Train Running Information message and Train Delay Cause Message, Train Running Interruption message, Wagon ETI/ETA message and Alert message. Such messages may be exchanged with "other stakeholders involved in the same freight service, under the condition that the stakeholders are identifiable".[246] The question arises whether such provision should be read as a first step of the TAF TSI towards the direction of the data economy, and in particular towards the commercialization of data. The preparatory works of the TAF TSIs are not openly accessible, so the rationale for the introduction of such provision is not known to the general public. In any case, such provision cannot be understood as a general allowance granted by EU law for IM to commercialize data in the railways. It is indeed bound to the scope of the TAF TSI, namely to the exchange of the said messages to the stakeholders and for the purposes set in the TAF TSI.

The new charging provision in the TAF TSI can be brought together with the Art. 10(3) New PRR concerning the charging of data and information. Both raise the question whether such provisions, adopted both in 2021, could be viewed as a legal recognition of the economic value of such data. In neither of the two cases is the 'authorization' to charge attached directly to the (intrinsic value of the) data itself, in the sense that there would be a market for 'data as a good'. In the case of Art. 10(3) New PRR, the charging principles (applicable to information provided *by RUs)* shall be linked to the costs incurred by the *provision* of access. In the case of TAF TSI, a literal reading of the provision suggests that it is the act of sending of the message – rather that the data sent – which may be charged. This being, it cannot be denied that both provisions reckon, at least, that the *provision* of data or information incurs costs, which may be accounted for. It remains however unclear and paradoxical that only a few of the data and information exchanges (should one compare them to the overall flux of information pursuant to both TAP and TAF TSIs) are subject to an authorization to charge. Similar to

[243] See for instance, TAF TSI, Annex, Point 2.3.1.
[244] See TAP TSI, Annex, Point 8 "stakeholder".
[245] TAF TSI, Annex, Point 4.1. See also TAP TSI, Annex, Point 4.2.18.
[246] TAF TSI, Annex, Point 4.2.

the New PRR provision in Art. 10(3), how the charging 'authorization' in TAF TSI interacts with the strict charging regulation of services provided by IMs to RUs remains unclear.

The Commission Delegated Decision 2017/1474[247] sets the objectives with respect to future changes of TSIs, and in particular TAP and TAF TSIs. It gives a taste of the future direction of both TAP and TAF TSIs, beyond changes already made in the last revision process since the adoption of the Commission Delegated Decision. Both TAP and TAF TSIs are expected to expand to new stakeholders so that the community of stakeholders exchanging messages regulated under TAP and TAF TSIs increases in size. Concerning the TAF TSI, the Commission Delegated Decision notes that the requirement for a "contractual agreement for lead RUs to provide information to stakeholders could constitute a barrier for the digitalization of railways".[248] As a result, the Commission Delegated Decision states that the TAF TSI "shall not impose requirements on RUs which could constitute a barrier for the digitization of railways".[249] Besides, the TAF TSI shall, in the future, "include data which shall be exchanged with safety related applications".[250] As for the TAP TSI, the Commission Delegated Decision states that, in the future, the TAP TSI shall "aim to facilitate the emergence of through-ticketing, integrated ticketing and multi-modal travel information and reservation systems".[251] This should be done "through the access to and exchange of relevant railway travel data with stakeholders along the multimodal value chain".[252]

Practical guidance for RNE –

- TAP and TAF TSIs are instrumental to the objectives of, *inter alia*, the Single European Railway Area Directive.
- TAP and TAF TSIs do lay down neither new data sharing obligations nor new confidentiality obligations, incumbent on the IMs.
- TAP and TAF TSIs are expected to be assigned new objectives in the near future (*i.e.*, through-ticketing for the TAP TSI and link to safety-related messages concerning TAF TSI), which could result in an opening of the IT community to new actors and/or new functionalities.
- This being, TAP and TAF TSIs cannot be seen as legal instruments designed to serve the data economy, namely the exchange of data in their quality as an economic resource. Indeed, data (and more precisely "messages") remain bound to their original purpose.
- The mentions in the recently revised PRR and TAF TSI that the sending of some messages (*i.a.*, by the IMs) may be subject to charges should not be interpreted as a general authorization for the IM to monetize data 'sold' to third parties for purposes other than those pursued under the TAF TSI. They can be viewed as a recognition that the provision of data and information incurs costs (*i.e.*, incumbent on the IMs) or in other words that

[247] Commission Delegated Decision (EU) 2017/1474 of 8 June 2017 supplementing Directive (EU) 2016/797 of the European Parliament and of the Council with regard to specific objectives for the drafting, adoption and review of technical specifications for interoperability, OJ L 210/5.
[248] Commission Delegated Decision, Rec. 35.
[249] Commission Delegated Decision, Art. 13(7).
[250] Art. 13(4).
[251] Commission Delegated Decision, Art. 14(6).
[252] Commission Delegated Decision, Rect. 36.

providing data and information constitutes a service on its own, namely a service which is becoming increasingly important, if not necessary for RUs (and other actors in the railway ecosystem) to operate.

- This being, freedom remains the legal principle and does not require a legal authorization. Data monetization by the IMs (*i.e.*, via RNE) to third parties should be considered as allowed by default, except where prohibited.
- Following a (somehow cryptic)[253] announcement in the European Data Strategy, the European Commission confirms its willingness to revise TAP and TAF TSIs in 2022, under the Commission Staff Working Document on Common Data Spaces.[254] The Commission does however not further specify whether (and, if so, to what extent) the revision will mandate or facilitate the sharing of data for purposes other than the exchange of message for the operation of trains. In any case, and save a revision of the Interoperability Directive, the Commission shall thereby comply with its mandate under this Directive, which is likely to limit the reach of data sharing provisions.

3.2.3. The IM as both an economic agent and a (semi)-State body

IMs are in a particular situation, although their legal status depends on the respective national law provisions. On the one hand, they are economic agents who commercialize train paths and execute the subsequent contract of use of the railway infrastructure ('contract of use'). On the other hand, they are heavily subsidized by the State and are often under its (loose or strict) supervision. This may result in a complex network of obligations and incentives, sometimes contradictory one with the others, especially concerning data sharing. This dichotomy has a number of implications concerning data sharing and the interpretation of confidentiality obligations by the IM, which, in turn, has implications for RNE data.

We first focus on the impact that data sharing, data access or transparency obligations potentially applicable to the IMs have on the interpretation of confidentiality obligations. Then, we briefly point to the legal nature of the 'contract of use', which often regulates confidentiality obligations. Especially, we highlight the impact that its qualification and regulation under public or, conversely, private law may have on the leeway for the IM to revise clauses unilaterally.

3.2.3.1. Effects of data sharing, data access or transparency obligations

The Open Data Directive was presented in section 2.2.2.2. The point of the present section is not to replicate it but to point to the effects of the application of such data sharing or other data access or transparency obligations on the interpretation of the confidentiality obligations under the SERA Directive by the IMs. Aside from the Open Data Directive, national law may encompass transparency obligations, such as access regimes to information held by IMs, *i.e.*, in their quality as (semi-)State bodies, while the exact legal form depends upon national legislation.

It is both logical and confirmed by the empirical studies that data sharing or transparency obligations have an impact on the interpretation and application of confidentiality obligations by the IM. When not confronted with data sharing or transparency obligations and when no incentives for sharing data

[253] The European Data Strategy merely refers to a "Review [of] the regulatory framework for interoperable data-sharing in rail transport in 2022", Communication 'A European strategy for data' 2020 (COM/2020/66 final) 29.
[254] Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 20.

are in place, the IM is logically incentivized to interpret confidentiality broadly, in order to satisfy its customers (RUs). This serves to keep good relationships with them, given the fact that business relationships in such markets are of a medium-term to long-term nature. This also serves to avoid complaints before the regulatory body or before a court and therefore sanctions. Conversely, when the IM is confronted with both confidentiality obligations on the one hand and data sharing or transparency obligations on the other, confidentiality of information is not the by default regime, but an exception to the principle of data sharing and/or access to information. In such case, the IM has to conduct *in concreto* analysis when protecting certain information as confidential. For the IM, this implies (i.) to state (harm-based) reasons for labelling information as confidential. (ii.) Logically, this implies that the IM would shift the burden to prove (likelihood of) harm onto the RUs. (iii.) When certain information is eventually labelled as confidential, the effects of confidentiality on data sharing and/or transparency have to be minimized. For instance, information would be anonymized and/or aggregated before further sharing to third parties.

The decision whether to share information should not be pictured as a black or white one, between sharing information and not sharing information out of confidentiality concerns. Especially because of data sharing and/or transparency obligations, it should rather be pictured as a triangle between the three following possible behaviors: (i.) not sharing information, (ii.) sharing information for free or with limited compensation and (iii.) sharing information as a commercial service, *i.e.*, subject to an economic price.

The data sharing and/or transparency obligations may regulate the price possibly levied by the IM upon sharing of information. It is beyond the ambit of these studies to look into the various national legislation on access to information. When it comes to the Open Data Directive and as outlined in section […], the question whether the regulated entities can charge a price is a contentious one. Two logics can be identified: on the one hand, the Open Data Directive (and the PSI Directive before it) is based on the view that data produced throughout the completion of activities for the general interest and subsidized with public funding are thereby already paid by the general public. Additionally, and relatedly, the logic goes that data is produced incidentally, as a by-product of the activities of regulated entities. Against this background, data should be made available for reuse in principle free of charge, or subject to low charges (*i.e.*, limited to the marginal cost of making data available, which excludes systematically the cost of *producing* data in the first place). The purpose is to enable a large number of economic players to leverage such data for the development of data-driven innovative products and services, including SMEs who may be sensitive to price.[255] This logic is visibly at work in the Open Data Directive concerning public sector bodies on the one hand,[256] and both public sector bodies and public undertakings in case of high-value datasets on the other.[257]

On the other hand, another logic is (increasingly) at work, that sees entities regulated under the Open Data Directive as active data providers in the data economy, or in other words as economic agents commercializing data. This logic is fed by the following factors. The rationale for mandating data sharing is partly based on competition law considerations, in the sense that the regulated entities are viewed as exclusive holders of data produced throughout the activities that they pursue based on a

[255] See Open Data Directive, Rec. 36.
[256] Open Data Directive, Art. 6(1).
[257] Open Data Directive, Art. 6(6)(a), subject to the (limited) exceptions laid down in Art. 14.

legal monopoly.[258] For instance, the Directive clarifies that competition law applies to the establishment of the principles for data reuse. In this respect, particular attention should be paid to exclusive agreements (deemed in principle anticompetitive).[259] Entities regulated under the Open Data Directive are thereby viewed as *economic actors* in the data economy, which is striking, especially for public sector bodies (such as a local authority or a municipal library) whose activities are traditionally viewed as out of the scope of the economic sphere.[260] The extension of the scope *rationae personae* to public undertakings with the Open Data Directive (under the *lex specialis* regime as clarified in section […]) also urged the EU law-maker to take into account their specific position, and especially the fact that, contrary to public sector bodies, they are economic agents active on markets (although the market for train path *i.e.*, is a non-competitive one, in the sense that every national IM has a legal monopoly). This is why the 'no charging principle' does not apply to public undertakings,[261] who are therefore free to charge a commercial price. Finally, regulated entities are increasingly expected to be active providers of data for the data economy, thereby departing from the original 'making available data as they are' motto of the PSI Directive. Visible in the Open Data Directive and more recently in the Data Governance Act (Chapter II),[262] this phenomenon is related to the willingness of the EU lawmaker to make as many data as possible available for reuse. In order to do this, however, public sector bodies need to play an active role in 'curating' data to enable their reuse, especially when such data are the object of entitlements of third parties (namely based on IPRs, data protection or confidentiality obligations) (see section 2.3.2). As a result of such logic, regulated entities should be able to levy a commercial price, although under regulated conditions.[263]

Practical guidance for RNE –

- IMs are in a particular situation, scattered between their role as an economic agent commercializing and executing train path on the one hand and (often) their status as a (semi-)public body under the supervision and funding of the State on the other hand.
- Such situation results in various obligations and incentives with respect to information and data sharing and/or transparency obligations, which has implications on the interpretation of confidentiality obligations and on the role that IMs can play in the data economy as data providers.
- First, a major distinction can be seen in the interpretation of confidentiality obligations under the SERA Directive, based on whether IMs are subject to data sharing and/or

[258] Björn Lundqvist, 'Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data' in Mor Bakhoum and others (eds), Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? (Springer Berlin Heidelberg 2018) https://doi.org/10.1007/978-3-662-57646-5_8; Charlotte Ducuing, 'Data as Infrastructure? A Study of Data Sharing Legal Regimes' [2019] Competition and Regulation in Network Industries https://doi.org/10.1177/1783591719895390.

[259] Open Data Directive, Rec. 47 and 48 and Art. 12.

[260] On the competition law aspects of the PSI regime, see Josef Drexl, 'The Competition Dimension of the European Regulation of Public Sector Information and the Concept of an Undertaking' (Social Science Research Network 2014) SSRN Scholarly Paper ID 2397018 <https://papers.ssrn.com/abstract=2397018> accessed 10 January 2018.

[261] Open Data Directive, Art. 6(2)(c).

[262] On this, see Julie Baloup and others, 'White Paper on the Data Governance Act' (Social Science Research Network 2021) SSRN Scholarly Paper ID 3872703 s 3.3 <https://papers.ssrn.com/abstract=3872703> accessed 21 November 2021.

[263] See for example DGA proposal, Art. 6.

transparency obligations. When this is indeed the case, IMs have to balance confidentiality obligations against data sharing and/or transparency. This results in confidentiality obligations being interpreted more strictly, both in terms of scope and of legal effects. This, in turn, has consequences for RNE data marketing strategies.

- The application of data sharing and/or transparency obligations to the IM may result in obligations and/or incentives to share or make available either for free or at a fair and economic price. Whether the IM is allowed to make a profit or at least recover the full price of the provision of data or information has an impact on RNE data marketing strategies.
- The fragmentation of the legal framework concerning data sharing and/or transparency obligations is related to the variety of legal status of IMs across the EU. This constitutes an obvious obstacle to RNE data marketing strategies.
- Whether IMs may, respectively, engage in proactive data processing and data commercialization – *i.e.*, by proxy through RNE – depends on national law, the analysis of which lies beyond the ambit of the present study.
- This being and as a reminder, when IMs would be under the scope of the Open Data Directive as public undertakings, they would remain free to charge an economic price (Open Data Directive, Art. 6), except where regulated more strictly under national law. In other words, the Open Data Directive endorses the view that public undertakings are economic agents and can be active data providers in the data economy, free to engage in data marketing and commercialization activities.

3.2.3.2. The legal status of acts governing confidentiality

As outlined in section 3.1, the SERA Directive confidentiality obligations are of a general nature ('principle-based') and they raise a number of interpretation issues. As a result, confidentiality is often regulated either in the Network Statement of IMs or (most of the time) in the contract of use of the infrastructure between the IM and the respective RUs. When it comes to RNE data, this raises several issues.

In contrast to the network statement,[264] the "contract of use" is not regulated under EU law. As a result, both the substantive contractual clauses and the process for adopting and revising them are subject to national differences. In particular, whether the IM may unilaterally change the contractual provisions (*i.e.*, subject to a more or less regulated consultation of the RUs and/or prior notice) or whether explicit agreement of RUs is required, may differ. The national differences are inevitably mirrored in differences as per the way confidentiality is contractually regulated. But also, where the contract of use has a broad interpretation of confidentiality and the IM has little leeway to revise it, the legacy of the past may weigh heavy on the present willingness of the IM to adapt the confidentiality obligations, *i.e.*, in light of the new data economy environment.

The legal nature of the contract of use and, more generally, the extent to which the IM may unilaterally modify the conditions applicable to the RUs may in particular depend on its legal status, whether as body governed by public law (to some extent) or by private law. In particular, whether the network statement and, above all, the 'contract of use' are regulated as contracts or as legal acts of public law may have an impact on the possibility for the IM to revise them unilaterally, namely without the prior consent of RUs.

[264] SERA Directive, Art. 27.

Practical guidance for RNE –

- The confidentiality obligations are often further substantiated in the contract of use between the IM and the respective RUs.
- The contract of use of the respective IMs is the product of national law but also of the state of the markets (and especially of the power that the RUs may exert on the revision process), which differ from an IM and a country to the others. This results in a fragmentation of the regulation of confidentiality across the EU.
- Subject to national law, and especially of the legal qualification of the contract of use (governed under private or public law), revising confidentiality-related contractual clauses may be difficult (*i.a.*, depending on the level of consent required from the RUs, who are the beneficiaries of the confidentiality protection).

3.3. The liberalization process as an interpretation grid?

The confidentiality obligations should be viewed as part and parcel of railway market regulation and instrumental to the liberalization objective. While the lawmaker does not provide much guidance on how to interpret the confidentiality obligations, this section summarizes whether and how the liberalization as an overarching legal objective for the SERA Directive helps to interpret such obligations.

There is no doubt that, in the railways like in other utilities, access to information and data plays a crucial role in the liberalization process. It is indeed commonplace that mere access to tracks is not sufficient for a new entrant to genuinely compete with an incumbent RU. Some data and information can be considered as assets, the access to which is necessary for new entrants to genuinely compete or in other words (quasi-) essential facilities.[265] Data and information necessary for new entrants may happen to be held by several entities, and especially by the IM and/or by the station manager (possibly the same undertaking as the IM or as the incumbent RU, in the latter case subject to unbundling requirements under the SERA Directive) or by other RUs. As illustrated by the *Westbahn* case under the PRR and by the New PRR provisions related to real-time data relating to the arrival and the departure of passenger trains, it is sometimes only based on the cooperation between such actors that RUs – and especially new entrants – can access the appropriate data. In the case of real-time data relating to the arrival and the departure of passenger trains, RUs are genuinely in the position to inform passengers only based on the provision of data by the IM, the station manager and possibly the other RUs.

This implies a certain level of information flow between the railway entities. In this respect, the "minimum access package" to be supplied by the IM to the RUs[266] includes "all other information required to implement or operate the service for which capacity has been granted". It also implies that the IM shall abide by the principles of non-discrimination[267] between the RUs in the provision of information and data to RUs. Especially when sharing data and information to the incumbent RU – whether in their quality as RU or also possibly in other quality, such as station management or marshaling yards management -, the IM shall beware that the information or data cannot constitute an advantage vis-à-vis other RUs. This is all the more necessary that data, unlike other assets, may

[265] Patrice Bougette, Axel Gautier and Frédéric Marty, 'Which Access to Which Assets for an Effective Liberalization of the Railway Sector?' (2021) 22 Competition and Regulation in Network Industries 87.
[266] SERA Directive, Art. 13(1) and Annex II, Point 1, subject to the charging principles as laid down in Art. 31(3).
[267] SERA Directive, Art. 10(1) and Art. 13(1).

easily serve several purposes. The same data could therefore genuinely serve station management or marshaling yards management purposes while *also* constituting an advantage over competing RU in the carriage market (including indirectly concerning distribution channels). For instance, and as reported by ProRail, information on passengers (*i.e.*, of other RUs) in stations could well be used not only for station management purposes but also for the purpose of its activities as an RU. In the case where the competing RUs would not dispose of the same information, this would constitute an advantage. Depending on the case at hand and especially on the nature and sensitivity of the information, there could in such case be two types of solutions for the IM, namely either to *not* share such information with the RU or to share such information with all RUs (and make it a 'club good').

Turning to confidentiality obligations more specifically, the impact of liberalization is neither straightforward nor necessarily unequivocal. First, it is obviously the existence of markets for train paths which gives value to business-related information, and which therefore justifies the existence of confidentiality obligations to the benefit of RUs. Typically, and to the extreme, freight RU 'B' could try and parasite freight RU 'A', based on the access to information on the planned activities of RU 'A' for a given customer at a given price. This is why train path information, namely information on future activities, shall be deemed confidential in all circumstances, according to the Directive. Aside from the case of train path information, both the scope and the legal effects of confidentiality obligations should not be determined in the abstract but rather *in concreto, i.e.*, subject to the state of the respective markets.

In this respect, the less competitive a market is, the more difficult it is to anonymize data related to an RU (trains), for example in the case of coordination of train paths requests pursuant to Art. 46 of the SERA Directive. This may seem to suggest at first glance that the less competitive a market for train paths is, the more (train path) information should be deemed confidential. Said more precisely, the level of competitiveness of the market has an impact on the legal *means* how to protect confidentiality. Concretely, the less competitive a market for train paths is, the more the confidentiality obligation may lead to *i.e.*, non-disclosure or aggregation of information, based on the observation that anonymization (namely, the deletion of the connection between information and, in this case, an RU) is practically impossible and may therefore be dismissed in this particular case as a means to protect confidentiality. Conversely, protecting the confidentiality of information may prove easier in the case where many competitors are active in the same market. Against the background that confidentiality aims to protect the competitive process, the absence of competition in a market segment in present times and in the near future could be argued to decrease (or even abolish) the need for related data and information.

The account paid to fair competition, to the liberalization process and, more generally, to the markets when interpreting confidentiality obligations leads one to distinguish passenger vs freight railway services. Passenger services are addressed to the general public, which requires information on train circulations (but also, although it is outside of the scope of this study, ticketing and distribution more generally) to be made available broadly, as confirmed by the revision of the PRR. In contrast, freight services are provided to business customers, based on bilateral negotiations.

Finally, the question whether the delays of an RU (and the cause for such delays) constitute confidential information remains debated, mainly because the Directive does not clarify the rationale for protecting information as confidential. On the one hand, such information could be deemed confidential based on the fact that it relates to the business activities of an RU, and possibly because the disclosure of such information could have detrimental effects on the RU. By showing bad

performance, it would lower the reputation of the RU, possibly vis-à-vis its customers and therefore lower its chances to get future contracts. On the other hand, liberalization as an objective of the Directive could point to another conclusion. One could argue that information on (the cause of) delays should be broadly available so that customers of RUs can spur performance-based competition. This is already the case by law to some extent for passenger RUs (see section 3.2.1). Whether it should similarly be the case concerning freight RUs remains an open question. One could however object that freight vs passenger railway services are different, especially in that passenger services are offered to the general public while freight services are offered based on B2B bilateral negotiations.

Practical guidance for RNE –

- The liberalization process constitutes one of the objectives of the SERA Directive. It shall necessarily play a role in the interpretation and application of confidentiality obligations.
- However, the role of the liberalization process in the interpretation of the confidentiality obligations is not unequivocal. It depends on the nature of information and on the context.
- The account being paid to fair competition and to the liberalization process implies that information may have to be shared, where appropriate, in a non-discriminatory manner to the relevant RUs.
- A general distinction shall be made between passenger vs freight railway services, because of the different nature of such markets. Information on passenger train circulation cannot be considered confidential, including in real-time, based on the New PRR.
- Such a finding is, however, without prejudice to the legal regime of information on freight train circulations (and especially, whether confidential or not, and what it legally entails).
- While information on (the causation of) passenger train delays is not confidential, whether the same applies to freight train delays information remains an open question. The liberalization process as a regulatory objective could suggest that such information is *not* confidential, so that customers can spur performance-based competition, as fostered by the SERA Directive (see for instance Art. 35 on the performance scheme aimed to incentivize good performance by the IM and the RUs).

3.4. Conclusion

The confidentiality obligations under the SERA Directive are notoriously vaguely phrased, which raises a number of interpretation questions in terms of the:

- Scope of confidentiality obligations, whether they refer only to the train path allocation or whether they extend also, *i.e.*, to train circulation, both in terms of scope *rationae materiae* (which information shall be deemed confidential, whether 'only' train path-related information or also train circulation-related information) and in terms of duration of confidentiality obligations (whether the obligation to keep confidentiality holds true 'only' during the train path allocation phase or whether it remains in place after that phase);
- Trigger for confidentiality obligations, or in other words which concrete interests or values are protected by confidentiality, *i.e.*, whether the 'mere' link between information and the RU (trains) suffices to trigger confidentiality or whether potential (specific type of?) harm shall be proved, whether information shall be (actively?) "provided by" the RU or not;
- Process for determining that information is confidential;

- Legal effects of confidentiality, *i.e.*, whether it shall call for non-disclosure save prior agreement of the concerned RU, or disclosure subject to prior anonymization or aggregation, or subject to contractual conditions (for (purpose of) reuse), etc.

Guidance can neither be found in the SERA Directive nor in the preparatory works. According to the survey conducted by RNE with its members, there is also no case law and no cases before any national regulatory body.

As a result, confidentiality is regulated mainly in national law and arranged contractually in the 'contract of use of the infrastructure' between the IM and the respective RUs. The extent to which the IM can modify the contractual clauses (potentially subject to prior consultation or agreement of all RUs and to prior notice) depends on national law and on the state of markets (including, on the bargaining powers of the IM and the RUs (representatives) respectively). The contract of use is not regulated under EU law, which results in a fragmentation of the interpretation of confidentiality obligations throughout the EU. The fragmentation is accentuated by the fact that not all IMs have the same legal status (whether 'public' or 'private' entities). Yet, the legal status has consequences on the legal regime of confidentiality and/or the ability or even obligation to share information, either for free or upon an economic price.

Confidentiality obligations are interpreted more or less restrictively, depending on whether the IM is simultaneously subject to data sharing and/or transparency obligations. In such case, confidentiality is an exception to the principle of sharing (or transparency) and must be interpreted strictly, *i.e.*, in terms of scope, of process for determining which information shall be deemed confidential and or impact of confidentiality.

The interpretation and application of confidentiality obligations under the SERA Directive are affected by other legal frameworks. The PRR has just been revised and includes obligations for the IM to share real-time data relating to the arrival and departure of (all) passenger trains to RUs, which shall therefore not be considered confidential. The PRR exemplifies the close connection between fair competition and the liberalization process on the one hand and the regulation of information (including confidentiality) on the other. The TAP and TAF TSIs do not lay down additional data sharing or confidentiality obligations but are rather instrumental to, *i.a.*, the PRR and the SERA Directive. IMs do not necessitate a legal authorization for monetizing data (possibly through RNE) and commercial freedom should be considered as the by default regime, unless where prohibited.

The PRR and the TAF TSI provisions stating that the sending of some messages/information (*i.a.*, by the IMs) may be subject to charges/financial compensation should not be interpreted as a general authorization for the IM to monetize data 'sold' to third parties for purposes other than those pursued under the TAF TSI and, especially, within the scope of the TAF TSI. However, they can be viewed as a recognition of the costs incurred by the provision of data and information and of the growing role of data and information for the operation of railway services. How such provisions interact with charging principles applicable to the services provided by the IMs to the RUs remains however unclear on many aspects. The fact that the EU legislator singles out certain messages (in TAP and TAF TSIs parlance) in this respect, amongst the many data and information exchange occurrences in the sector, is also a source of confusion.

Finally, it is obvious that confidentiality obligations under the SERA Directive are closely connected to the objectives of the Directive to advance the liberalization process and to establish fair markets in the railways. The effect of such objectives on confidentiality obligations may not be unequivocal. In any

case, account should be paid to these objectives when discussing the confidentiality nature of information *in concreto.*

In conclusion, EU railway law offers little guidance on the interpretation and application of confidentiality obligations under the SERA Directive. Then, lessons could be learned from confidentiality regime outside the field of the railways. While having harmonized the legal protection of trade secrets with the adoption of the Trade Secret Directive, the EU has not adopted a unified approach to confidentiality. There is therefore no general confidentiality regime in EU law. That being said, the question of confidentiality has naturally gained specific significance in the field of competition law, which will therefore be analyzed in the following section. Besides, an avenue for interpreting confidentiality obligations under the SERA Directive is to turn to other sectors sharing similarities with the railways. The third section provides an outlook of the aviation sector concerning how data are exchanged and regulated.

3.5. Inspiration from competition law

The present section examines whether competition law could offer some clarity on what constitutes 'confidential information' by looking at both Articles 101 and Article 102 TFEU procedures[268], but also at mergers concerning railway companies. We decided to draw inspiration from competition law given the role that competition policy played during the liberalization process of railway markets; and the role it continues to play, by ensuring that such markets remain open and competitive.

3.5.1. EC Guidance on the notions of "business secrets" and "other confidential information"

The European Commission has provided some guidance on what constitutes confidential information and business secrets in the context of competition law proceedings. This concerns the "access to file" procedure which takes place after the European Commission has issued the so-called Statement of Objections (setting out the alleged competition law infringement(s) of the undertakings under investigation/addressees). Such undertakings are then granted access to, inter alia, any documents received by DG Competition from other undertakings, except if those documents contain business secrets or other confidential information, that those undertakings have declared as such.[269]

In its guidance on confidentiality claims during Commission antitrust procedures,[270] the European Commission sets out the legal precedent on what may constitute business secrets and other confidential information:

- **Business secrets**: Business secrets are confidential information about an undertaking's business activity of which not only disclosure to the public but also mere transmission to a person other than the one that provided the information may seriously harm the latter's interests.
- **Other confidential information**: Other confidential information is information other than business secrets, insofar as its disclosure would significantly harm a person or undertaking. Depending on the specific circumstances of each case, this may apply to information provided by third parties about undertakings which are able to place very considerable economic or

[268] For example, cartels and discriminatory behavior respectively.
[269] Information on the access to file procedure can be found here: https://ec.europa.eu/competition-policy/antitrust/procedures/access-file_en.
[270] https://ec.europa.eu/competition/antitrust/business_secrets_en.pdf.

commercial pressure on their competitors or on their trading partners, customers or suppliers (e.g. customer data when there is risk of retaliation).

The Commission provides further clarifications on confidentiality in its Communication on the protection of confidential information by national courts in proceedings for the private enforcement of EU competition law. According to the case law, for information to be regarded as confidential, all the following conditions must be met: i) such information must be known only to a limited number of persons; ii) its disclosure must be liable to cause serious harm to the person who has provided it or to third parties; and iii) the interests liable to be harmed by the disclosure must be objectively worthy of protection.[271]

To assess the fulfillment of the second criterion, the nature of the information plays a key role. Disclosure of information that has commercial, financial or strategic value is usually considered capable of causing serious harm.[272] Also, the more current information is, the more harm it may cause. Commercially sensitive information concerning an ongoing or future business relationship, internal business plans and other forward-looking commercial information could often qualify (at least partially) as confidential information.

Trade secrets, as defined in the Trade Secrets Directive, are also to be considered confidential information.[273]

The Commission notes that the assessment of what information is business secrets or confidential information needs to be performed on a case-by-case basis. However, it also provides guidance on what does not constitute confidential information.[274] This concerns in particular:

a. information about an undertaking that is already known outside the undertaking (in case of a group, outside the group), or outside the association to which it has been communicated by that undertaking, will usually not be considered as confidential. For information to lose its confidential nature, it is sufficient for it to be available to specialist circles or capable of being inferred from publicly available information.
b. Information that has lost its commercial importance, for instance due to the passing of time. The CJEU has confirmed a period of five years in itself to be sufficient for information to lose its qualification as business secrets or other confidential information.

3.5.2. Obligatory data sharing as a commitment in merger control proceedings

Giving access to data has been the subject of commitments provided in railway-related mergers. In 2010, SNCF and UK's London Continental Railways (LCR) decided to set up a joint venture integrating the Eurostar business that would become a standalone business controlled by SNCF and LCR, operating the Eurostar service throughout France, the UK and Belgium.[275] The Commission raised concerns that the proposed transaction would be problematic as it would render market entry by competitors on the

[271] European Commission guidance on confidentiality claims, para. 11.
[272] European Commission, 'Communication on the protection of confidential information by national courts in proceedings for the private enforcement of EU competition law', OJ C 242, 22.7.2020, para 22.
[273] European Commission Communication, para. 24.
[274] European Commission guidance, paras 14-15.
[275] See Case No COMP/M.5655 - SNCF/ LCR/ EUROSTAR, https://ec.europa.eu/competition/mergers/cases/decisions/m5655_1034_2.pdf. Up until then Eurostar ran by a cooperation between SNCF, EUKL and the Belgian national railways SNCB. Each railway company owned its assets and has responsibility for the operation of the service on its respective national territory.

routes London-Brussels and London-Paris more difficult and might enhance Eurostar's dominant position. The Commission put forward a liberalization rationale, suggesting that competition should be safeguarded and ensuring third party access to the infrastructure was crucial.[276]

The merging parties provided concessions that would remedy the Commission's concerns, including fair and non-discriminatory access for new entrants to passenger services. SNCF committed to providing passenger information services to RUs in the passenger stations covered by the Eurostar service. This consists of written (signposting, display of train times and platforms) and/or oral information, including safety information as well as static and/or dynamic information (real-time information, info flashes). Station marking must be based on signposting and dynamic information systems which must be located all along the routes channelling passengers between town, station and platforms.[277] A similar obligation is foreseen for the Transmanche Zone (static information, systems via signs of displays, dynamic, visible or audible information systems). [278] LCR provided comparable commitments for London St Pancras.[279] The Commission found that the proposed remedies "*lower barriers to entry for new providers and thereby contribute to securing the benefits of the liberalisation of international passenger rail services for consumers*".[280]

Based on the above case, one could argue that information on train circulation for passengers in stations (as described above) cannot constitute confidential information as there was an obligation to make them open. However, the context within which such obligation of openness/access was imposed needs to be taken into consideration. In the Eurostar case, the aim was to preserve the liberalization process and allow third-parties (*i.e.* competitors) to be able to enter the market in the London-Brussels and London-Paris routes. It is unclear if the same argument on the possible non-confidential status of such data (or other train data in the traffic management process) could hold true when the aim of the 'openness' or access to such data would be commercializing them.

The Eurostar case appears to have anticipated on the revision of the PRR (see section 3.2.1), which requires both IMs and RUs to share more data to passengers and throughout the transport and distribution value chain. The Eurostar case also confirms the finding (same section) that there is a close connection between the objective of fair competition between RUs and passenger rights to information.

3.5.3. Procedural aspects concerning confidentiality claims

In the context of the access to file procedure mentioned above, the European Commission follows a specific procedure that allows documents to be shared amongst undertakings (who are likely also competitors) without jeopardizing the confidentiality of information claimed by them. According to the relevant guidance by the Commission,[281] undertakings need to submit a non-confidential version for each submission/document on which they claim confidentiality. They provide the Commission with all relevant details to enable it to assess the confidentiality of a piece of information:

a. **Explanations on the confidentiality claim(s):** undertakings need to explain the reasons why the information in question constitutes a business secret or other confidential information, in

[276] https://ec.europa.eu/commission/presscorner/detail/en/IP_10_755.
[277] See Case No COMP/M.5655 - SNCF/ LCR/ EUROSTAR, p.24.
[278] See Case No COMP/M.5655 - SNCF/ LCR/ EUROSTAR, p.25.
[279] See Case No COMP/M.5655 - SNCF/ LCR/ EUROSTAR, p.32.
[280] https://ec.europa.eu/commission/presscorner/detail/en/IP_10_755.
[281] https://ec.europa.eu/competition/antitrust/business_secrets_en.pdf.

particular, how the disclosure of this information would cause serious harm or would significantly harm them;

b. **Provide a summary:** undertakings need to provide a concise but meaningful non-confidential summary of each piece of information claimed to be confidential.

Standard justifications such as 'business secret' or 'information not known to other party' without any justification are not deemed sufficient. The Commission stresses that the non-confidential versions of the submissions/documents and the summaries of the redacted information must be drafted in an accurate and meaningful way as the purpose is to enable other parties that are entitled to access the non-confidential versions to determine whether the information deleted is likely to be relevant for their defense. If it is, they can ask the Commission to provide them with access to information that has been claimed to be confidential.

Practical guidance for RNE

- The EC guidance on confidentiality in the context of competition law could be used as a standard to be applied across RNE members towards RU confidentiality claims.
- RNE and/or IMs could adopt an internal procedure concerning data confidentiality similar to the one applied by the Commission in the access to file procedure. The Commission guidance provides several examples of confidentiality claims, *i.e*. how to provide reasons and non-confidential summaries. This way the deadlock of not sharing any data can be avoided as IMs and/or RUs could provide non-confidential versions and/or a justification of why the said information is confidential and what is covered by it.

4. Lessons learned from the aviation sector

This section relies on desk-based research, namely identifying and assessing relevant legislation as well as studies and articles that have been written on the topic. This section will explore how the aviation sector deals with the issues of data sharing and/or data confidentiality obligations. In a first sub-section, the study will introduce the aviation sector as a highly safety critical and regulated domain (3.1). In a second sub section, the study will look at the different data sources as important drivers for the aviation sector (3.2). In a third sub section, the study will look at the data paradox, which refers to the situation according to which data are seen as important enablers but where data holders are reluctant to share such data (3.3). In a fourth sub section, the study will identify the data sharing obligations in the field of Air Traffic Management (ATM) where there are some legally mandated obligations (3.4). In the fifth sub section, the study will look at other data or information sharing obligations and practices outside the field of ATM (3.5). Finally, the study will look at emerging mobility technologies and paradigms such as automated ATM/flying and the development of the U-Space framework as potential enablers of further data sharing between stakeholders (3.6). Mention will also be made to the proposal for a recast of the Single European Sky regulation.

4.1. Prolegomena - A safety - security critical and liberalized domain

As with any safety critical sector, aviation is a highly regulated field across Europe. A very dense patchwork of legislation, mainly European but also international, covers a vast array of topics, including operator licensing, aircraft certification, air operations, crew licensing, air traffic control and air traffic management, etc. Aviation, as an activity, is therefore subject to stringent safety and security related rules.

In Europe, commercial air transport operations used to be the monopoly of state managed air carriers (so called 'legacy carriers'). However, the aviation sector, like the railway sector, underwent a liberalization process which was initiated in 1987 and further implemented in 1993. This process was gradual in nature and three successive packages of measures were adopted in EU law. These covered air carrier licensing, market access and fares.[282]

However, despite this liberalization process, the aviation field (specifically in commercial air transportation) is still highly managed for purposes of safety, security and traffic management. Data plays an important role in aviation.

4.2. Plural data sources in aviation: important drivers for safety and efficiency

4.2.1. A 'data driven' domain

Aviation is extremely dependent on data and information. Indeed, data plays a crucial and strategic role in aviation. Namely, data is important for operational, safety, security and commercial purposes. For instance, aircrafts constantly generate huge amounts of (operational) data which are transmitted from the aircraft to the airline and or in some instances to the manufacturer (pending certain commercial agreements between the airline and the manufacturer). Such data is transmitted through specific communication mediums such as data links and ACARS.[283] This allows the carrier to improve its overall operational efficiency as well as optimize the levels of safety.

4.2.2. A plural set of data sources

It is important to highlight the multiplicity and diversity of data sources in the aviation sector. It is, however, difficult to provide an exhaustive typology of data sources used in aviation. But one could differentiate between non-commercial data (safety/security, technical related for instance) from commercial data (passenger reservations, passenger traffic numbers, etc). But in some instances, data may have a mixed nature. As noted in a report, "airports, air transport companies and aviation service providers in Europe all rely on accurate and timely data for delivering their services and they are also forced to exchange some of these data in order to function".[284] Data can be found throughout the complex aviation eco-system of actors which are more often interdependent with each other. Many different types of data are generated and diffused. Some are purely technical in nature, others are more operational, whereas some are strictly commercial. Moreover, personal data can be exchanged as well. Indeed, the communication of passenger related data between carriers and authorities also plays an important role in the overall security of the air transport eco-system. This has been mandated by EU law.[285] Data also plays an important role within airlines statistical tools for the programming of

[282] I.H.Ph. Diederiks-Verschoor, revised by Pablo Mendes de Leon, *An Introduction to Air Law*, 9th revised éd., Wolters Kluwer, 2012, p. 85

[283] ACARS stands for Aircraft Communications Addressing and Reporting System. It is a "digital data link system for the transmission of messages between aircraft and ground stations" (Sybrary article, "Aircraft Communications, Addressing and Reporting System", retrieved on 01/03/2022: https://skybrary.aero/articles/aircraft-communications-addressing-and-reporting-system).

[284] Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability conducted prepared for the European Commission, DG Communications Networks, Content & Technology by Deloitte (2018), p. 262.

[285] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

flights throughout the seasons. Data can also originate from computer reservation systems and global distribution systems (also known as GDS).

4.3. The data paradox: the reluctance of sharing data in aviation

Despite the importance of data in the aviation field, its sharing is not seen as straightforward. The reluctance of aviation actors to share data can be explained by many factors such as legal, privacy and operational reasons. As has been regularly noted, aviation actors tend to harvest data for their own utilization and do not necessarily see the added value of sharing it on a wider basis. More importantly, the sharing of data to third parties is seen as a potential risk to their competitive advantage. This concerns many aviation actors, from air carriers to airports. As has been noted in various sources, so called 'data ownership' and trust issues have persisted over the years and remain alleged obstacles for aviation actors to share data. This has resulted in the creation of data silos where certain entities harvest and keep data without the intention of exchanging it. The absence of data sharing is particularly prevalent in B2B relationships. There is a clear friction between aviation actors to share commercial data (airlines and airports usually do not share customer information with each other. However, data exchanges could provide a more integrated travel experience for passengers).[286] As has been noted, aeronautics stakeholders aggressively invest "in harnessing their data as critical corporate assets to drive strategic insights, improve operations, and support faster aircraft turnaround and predictive maintenance timing".[287]

However, in B2G relationships, there is much more sharing of data, as it may be legally mandated.

4.4. ATM as an example of (partial) network (operational) data sharing

4.4.1. A complex aviation and Air traffic management eco-system

The technical, regulatory, and institutional setting for the aviation air traffic management ecosystem is extremely complex.[288] It blends a mix of both international, pan European and European Union derived requirements and frameworks. The Air Traffic Management (ATM)[289] setting involves many actors such as the Air Navigation Service Providers (ANSPs) (who provide air traffic service provision within their jurisdiction, and may be publicly or privately managed), airports, national regulatory authorities, aircraft operators and the network manager (NM). This latter has a management role in air traffic and coordinates with the ANSPs and the overall air traffic system. Though not completely centralized under the current Single European Sky regime, the EU is pushing for a more integrated approach to air traffic management (through SES 2+ package).[290]

Airport slot allocation

---

[286] Wolfgang Bublitz, "The key stakeholder benefits of data sharing in the aviation industry", The Passenger Terminal Today, 22 October 2020, retrieved on the 18 February 2022: https://www.passengerterminaltoday.com/opinion/the-key-stakeholder-benefits-of-data-sharing-in-the-aviation-industry.html.

[287] Fenareti Lampathaki, Michele Sesana and Dimitrios Alexandrou, « Digital Transformation in Aeronautics through
the ICARUS Aviation Data and Intelligence Marketplace », MATEC Web of Conferences 304, 04002 (2019), p.1: https://www.matec-conferences.org/articles/matecconf/pdf/2019/53/matecconf_easn2019_04002.pdf.

[288] For an overview of the regulatory setting, see: https://learningzone.eurocontrol.int/doc/seslex.htm

[289] On the definition of Air Traffic Management, see: https://skybrary.aero/articles/air-traffic-management-atm

[290] Sean Goulding Carroll, " EU's air traffic reform plan draws fire from airlines", Euractiv website, 10 June 2021, retrieved on 28 February 2022: https://www.euractiv.com/section/aviation/news/eus-air-traffic-reform-plan-draws-fire-from-airlines/

Though often confused, one must differentiate between airport slot management and air traffic slot management, though both are related. Airport slot management concerns the management of airport capacity at so-called coordinated airports.[291] A coordinated airport refers to any airport "where, in order to land or take off, it is necessary for an air carrier or any other aircraft operator to have been allocated a slot by a coordinator, with the exception of State flights, emergency landings and humanitarian flights".[292] In essence, when an airport is congested (level 3 airport or 'coordinated airport'), that is when demand for airport slots exceeds the capacity supply, an airport slot coordinator is designated. The coordinator is an independent body whose mission is to allocate slots in an "transparent and efficient manner".[293] As defined in the EU regulation, a slot is "the scheduled time of arrival or departure available or allocated to an aircraft movement on a specific date at an airport coordinated".[294] In France, the airport slot coordinator is an association named CAHOR. It is composed of different members (both airlines and airports' representatives). Its website provides references to rules on sharing what data and with whom.[295] At an airport where slot allocation is required, the authorities determine the available capacity for slot allocation, *inter alia*, in cooperation with representatives of ATC,[296] air carriers using the airport and/or their representative organizations and the airport coordinator. The slot allocation process involves three different phases: primary allocation, slot returns and slot exchanges and transfers. Initially, each airport must specify a declared capacity.[297]

Information and data exchanged between the slot coordinator and the interested parties[298]

According to the Slot Regulation, where slots are allocated, the *coordinator* shall, on request and within a reasonable time, *make available for review to all interested parties the following information* (art. 4 (8) Slot regulation): (a) historical slots by airline, chronologically, *for all air carriers at the airport*, (b) requested slots (initial submissions), *by air carriers and chronologically, for all air carriers,* (c) all allocated slots, and outstanding slot requests, listed individually in chronological order, *by air carriers, for all air carriers*, (d) remaining available slots, (e) full details on the criteria being used in the allocation. According to article 7 (1) of the Slot Regulation, "air carriers operating or intending to operate at a schedule facilitated or coordinated airport shall submit to the schedules facilitator or

[291] Council Regulation (EEC) No 95/93 of 18 January 1993 on common rules for the allocation of slots at Community airports. For a consolidated version, see: https://www.cohor.org/wp-content/uploads/2021/03/CELEX_01993R0095-20210220_EN_TXT.pdf.

[292] Article 2 (g) of the Council Regulation (EEC) No 95/93 of 18 January 1993 on common rules for the allocation of slots at Community airports as amended.

[293] Matthias Finger, Juan J. Montero-Pascual, and Teodora Serafimova, « Navigating towards a more efficient airport slots allocation regime in Europe", Policy Briefs, 2019/17, Florence School of Regulation, Transport, Energy Retrieved from Cadmus, European University Institute Research Repository, at: http://hdl.handle.net/1814/64612.

[294] Article 2 (a) of Council Regulation (EEC) No 95/93 of 18 January 1993 on common rules for the allocation of slots at Community airports.

[295] Referring to the guidelines of the European Airport Coordinators Association, see: https://www.cohor.org/wp-content/uploads/2018/03/eusg_nr_3_-_transparency_and_interested_parties_eff20150916-1.pdf.

[296] ATC: air traffic control.

[297] Andrea Ranieri, Nuria Alsina, Lorenzo Castelli & Tatjana Bolic, "Airport slot allocation: Performance of the current system and options for reform: Towards a comprehensive performance framework", *The SESAR Innovation Days 2013 Conference*, November 2013, p. 1.

[298] This information is based on the EUACA Slot guidelines as published on the French coordinator's (Cohor) website (see footnote 13).

coordinator respectively *all relevant information requested by them*. *All relevant information shall be provided in the format and within the time-limit specified by the schedules facilitator or coordinator.* In particular, an air carrier shall inform the coordinator, at the time of the request for allocation, whether it would benefit from the status of new entrant, in accordance with Article 2(b) or (ba), in respect of requested slots".

However, there is no information on how the slot information itself must be (or not be) disseminated. One must refer to the EU Airport Coordinator Association guidelines (EUACA) for guidance on the sharing of slot data or information. For instance, these guidelines state that general coordination parameters are made public, as well as local rules and any national legislation. The coordination data is by itself not public. The allocated slots data is only communicated to interested parties.[299] This holds true also for waitlist and slot availability data. According to these guidelines, such interested parties include the "airport managing body with respect to data for the coordinated or schedules facilitated airport for which it is responsible (the airport has to prepare for the operation of the coordinated or schedules facilitated flights)"; "the appropriate ATC/ATS office and Eurocontrol for the same reasons"; "air carriers and other operators (including general aviation) using the airport regularly"; "European, national or regional authorities, the latter for their respective airports, having a genuine interest in receiving the schedule information according to article 4.8 of the EU Slot Regulation"; "Other members and regular observers of the coordination committee in charge of the airport concerned in order to assist them with their duties at the coordination committee"; "air carrier associations, provided they are members of the coordination committee of the airport concerned".[300]

4.4.2. Air traffic management (ATM) and data sharing

Eurocontrol: From air navigation service provider to EU's Network Manager

Eurocontrol is a pan European inter-governmental institution gathering 41 Member States. The European Union is also part of this organization. It has multiple functions ranging from technical expertise, research and operations, etc. It works closely with the European Union as it provides regulatory support and technical expertise to the Commission and its specialized aviation agency (EASA). Eurocontrol also has an operational role in the ATM field by providing air navigation services for the Maastricht Upper Area Control region (MUAC). It also collects en-route charges on behalf of Eurocontrol Member States. Most importantly, within the context of the Single European Sky framework, Eurocontrol was appointed by the Commission as the European Union's Network Manager.[301] Eurocontrol, acting as "Network Manager has extended the role of the former Central Flow Management Unit and now proactively manages the entire European ATM Network (with nearly ten million flights every year), in close liaison with the air navigation service providers, airspace users,

[299] EUACA Slot Guidelines, EUSG 3, 16 September 2015: https://www.euaca.org/up/files/DocsEUACA/EU%20SLOT%20GUIDELINES/EUSG%20Nr%20%203%20-%20Transparency%20and%20Interested%20Parties_eff20150916.pdf.

[300] EUACA Slot Guidelines, EUSG 3, 16 September 2015, p.3 : https://www.euaca.org/up/files/DocsEUACA/EU%20SLOT%20GUIDELINES/EUSG%20Nr%20%203%20-%20Transparency%20and%20Interested%20Parties_eff20150916.pdf.

[301] Commission implementing decision (EU) 2019/709 of 6 May 2019 on the appointment of the network manager for air traffic management (ATM) network functions of the single European sky (notified under document C(2019) 3228). The tasks of the network manager are detailed at Article 7 of the Commission implementing regulation (EU) 2019/123of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.

the military and airports".[302] As such, it is there to "align air traffic demand with available airspace and airport capacity".[303] The network manager therefore has a coordinating role where it manages "ATM network functions (airspace design, flow management) as well as scarce resources (transponder code allocations, radio frequencies), as defined in Regulation 677/2011 and Regulation 2019/123".[304]

Current Data sharing obligations in the ATM field: legal and regulatory mandated sharing of (some) operational data

In order to assure adequate levels of efficiency and safety, there are some data sharing obligations in the field of ATM.[305] In particular, the ATM stakeholders are required to share some data with the network manager. This is therefore mostly a vertical sharing of data between operational stakeholders and the ATM network manager. However, there are some data sharing obligations of operational data between stakeholders.

Article 7 (3) (a) of Commission Implementing Regulation (EU) 2019/123 of 24 January 2019 states that the Network Manager to fulfill its tasks must "ensure that tools, processes and *consistent data are available to support the cooperative decision-making process at network level and that such data are shared.* Such data shall include, in particular, flight plan processing, European data management systems and aeronautical information relevant to the execution of network functions as well as an electronic integrated briefing portal with access to interested stakeholders subject to Article 3a of Regulation (EC) No 551/2004".[306] The Regulation further adds that there should be exchange of "*operational data with operational stakeholders* in accordance with Article 13 of Regulation (EC) No 550/ 2004".[307] This latter regulation provides conditions of access to data and protection of such data. *Inter alia*, it states that "in so far as general air traffic is concerned, *relevant operational data shall be exchanged in real-time between all air navigation service providers, airspace users and airports, to facilitate their operational needs*. The data shall be used only for operational purposes".[308] This regulation further adds that "*access to relevant operational data shall be granted to appropriate authorities, certified air navigation service providers, airspace users and airports on a non-*

[302] Skybrary Article, "Eurocontrol", retrieved on the 18 February 2022: https://skybrary.aero/articles/eurocontrol.

[303] Nikola Ivanov, Fedja Netjasov, Radosav RadosavJovanović, Stefano Starita & Arne Strauss, "Air Traffic Flow Management slot allocation to minimize propagated delay and improve airport slot adherence", Transportation Research Part A: Policy and Practice, vol. 95, 2017, p. 183-197.

[304] Skybrary Article, "Network Manager", retrieved on 28 February 2022: https://skybrary.aero/articles/network-manager.

[305] ATM or air traffic management is defined by EASA as "the aggregation of the airborne and ground-based functions (air traffic services, airspace management and air traffic flow management) required to ensure the safe and efficient movement of aircraft during all phases of operations", EASA website, "What is the difference between ATM and ATC?", retrieved on 22/02/2022: https://www.easa.europa.eu/the-agency/faqs/air-traffic-management-atm#category-atm-basics.

[306] Article 7 (3) (a) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.

[307] Article 7 (3) (j) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.

[308] Article 13 (1) of the consolidated Regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation).

discriminatory basis".[309] Finally, it adds that "certified service providers, airspace users and airports shall establish *standard conditions of access to their relevant operational data* other than those referred to in paragraph 1. National supervisory authorities shall approve such standard conditions. Detailed rules relating to such conditions shall be established, where appropriate, in accordance with the procedure referred to in Article 5(3) of the framework Regulation".[310] Coming back to the Commission implementing regulation (EU) 2019/123 of 24 January 2019, it requires that "*operational stakeholders shall provide the Network Manager with the relevant data* listed in Annexes I to VI, complying with time periods and requirements determined through cooperative decision-making".[311] Such operational stakeholders refer to "the civil and military airspace users, civil and military air navigation service providers and airport operators which operate in the airspace referred to in Article 1(4)".[312] Annex I refers to the European Route Network Design Function, Annex II refers to the Air Traffic Flow Management Function, Annex III refers to the radio frequency function and Annex IV refers to the radar transponder codes functions.

Part B of Annex II, states that the ATS (Air Traffic Services)[313] units shall "provide the Network Manager and the local ATFM[314] units with the following data and subsequent updates, as technically feasible, in a timely manner and ensuring its quality: (i) airspace and route structures; (ii) airspace and route availability including availability through application of flexible use of airspace in accordance with Regulation (EC) No 2150/2005; (iii) ATS unit sector configurations and activations; (iv) aerodrome taxi times and runway configurations; (v) air traffic control sector, and aerodrome capacities including runways; (vi) updated flight positions; (vii) deviations from flight plans; (viii) actual flight take-off times; (ix) information on the operational availability of the Communication Navigation Surveillance (CNS)/ATM infrastructure".[315] It further adds that "the data referred to in paragraph 7(d) shall be made available to and from the Network Manager and the operational stakeholders".[316] The network manager must also "*collect, consolidate and analyse all data identified in Annexes I to VI and provide*

[309] Article 13 (2) of the consolidated Regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation).
[310] Article 13 (3) of the consolidated Regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation).
[311] Article 11 (4) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[312] Article 2 (5) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[313] Air traffic services is "a generic term meaning variously, flight information service, alerting service, air traffic advisory service, air traffic control service (area control service, approach control service or aerodrome control service)" (ICAO Doc 4444 Procedures for Air Navigation Services –Air Traffic Management – 16th Edition – 2016, p. I-4.
[314] ATFM: air traffic flow management.
[315] Annex II, part B, (7) (d) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[316] Annex II, part B (8) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.

this data to the Commission, the Agency and the Performance Review Body as requested".[317] Annex II further states that ATFM unites shall "provide the Network Manager providing central ATFM with all the required local data for the execution of the ATFM function".[318] It also adds that "when implementing arrival and departure planning information (DPI), airport local operational stakeholders shall ensure full coordination with the Network Manager in the establishment and operation of that functionality and the associated data exchange".[319] Annex II to the Regulation also states that "the Network Manager shall ensure that an archive of ATFM data listed in this Annex, flight plans, operational logs and relevant contextual data is created and maintained. That data shall be retained for two years from their submission and made available to the Commission, Member States, ATS units and aircraft operators, as required. That data shall be also made available to airport slot coordinators and airport operators to assist them in their regular assessment of the declared capacity".[320] Annex III refers to a central data register for radio frequencies.[321] Part C of Annex IV details Requirements for the provision and sharing of data related to radar transponder codes.[322]

Moreover, another regulation states that "air navigation service providers may avail themselves of the services of other service providers that have been certified in the Community".[323] It adds that "air navigation service providers shall formalise their working relationships by means of written agreements or equivalent legal arrangements, setting out the specific duties and functions assumed by each provider *and allowing for the exchange of operational data between all service providers* in so far as general air traffic is concerned. Those arrangements shall be notified to the national supervisory authority or authorities concerned".[324]

Confidentiality requirements imposed on the network manager and some regulatory authorities

Existing regulation does provide for some confidentiality requirements in the sharing of some air traffic data. For instance, Regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the Single European Sky (the so-called service provision Regulation) states that "*neither the national supervisory authorities, acting in accordance*

[317] Article 7 (3) (k) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[318] Annex II part B (10) (c) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[319] Annex II part B (15) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[320] Annex II part C (8) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[321] Annex IV part B (17) of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[322] Annex IV part C of the Commission implementing regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011.
[323] Article 10 (1) of Regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation).
[324] Article 10 (2) of Regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation).

with their national legislation, nor the Commission shall disclose information of a confidential nature, in particular information about air navigation service providers, their business relations or their cost components".[325] This confidentiality requirement therefore falls upon the (regulatory) authorities. An exception to this principal is the right of disclosure "by national supervisory authorities or the Commission where this is essential for the fulfilment of their duties, in which case such disclosure shall be proportionate and shall have regard to the legitimate interests of air navigation service providers, airspace users, airports or other relevant stakeholders in the protection of their business secrets".[326] Annex I to this regulation provides further confidentiality requirements on the behalf of the so-called qualified entities.[327] Indeed, it states that the qualified entities must be managed and administered in such a way as to "*ensure the confidentiality of information required by the administration*".[328]

However, ATM regulations are set to be amended. For instance, the amended proposal for a Regulation of the European Parliament and of the Council on the implementation of the Single European Sky (recast) defines rules for the sharing of data costs and confidentiality obligations. Indeed, it states that "the determined costs, actual costs and revenues deriving from air navigation services shall be broken down into staff costs, operating costs other than staff costs, depreciation costs, cost of capital, costs incurred for fees and charges paid to Agency acting as PRB, and exceptional costs and *they shall be made publicly available, subject to the protection of confidential information*".[329] This proposal adds that "*neither* the national supervisory authorities, acting in accordance with their national legislation, nor the Commission, nor the Agency, whether or not it is acting as PRB, nor the Network Manager *shall disclose information of a confidential nature, in particular information about air navigation service providers, their business relations or their cost components*".[330]

The limited sharing of Network Manager data to third parties

This brief overview of regulatory provisions relating to data in aviation therefore covers mostly technical and operational data. There are data sharing obligations between stakeholders, but this mostly concerns operational data in a vertical manner, that is between operational stakeholders (such as airlines, airports, ANSPs) and the network manager or other ATM/ATS related parties. There are however some (operational) data sharing obligations among aviation stakeholders. As noted in a study, such data concerns routes, radio frequencies, special service request codes, position reports and other operational data. Such data is then processed by Eurocontrol and made available to airline operators

[325] Article 18 (1) regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation).
[326] Article 18 (2) regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation).
[327] Under the Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, qualified entities in the air traffic management eco-system are entities which have been delegated certification or oversight tasks of service providers by the competent authority (ATM/ANS.AR.B.005 Allocation of tasks to qualified entities, Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011, p. 18).
[328] Annex 1 to Regulation (EC) n° 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation).
[329] Point 62 of the Amended proposal for a Regulation of the European Parliament and of the Council on the implementation of the Single European Sky (recast) - COM/2020/579 final.
[330] Point 92 of the Amended proposal for a Regulation of the European Parliament and of the Council on the implementation of the Single European Sky (recast) - COM/2020/579 final.

through what they call Data Distribution to Aircraft Operators. Such a service is only provided to aircraft operators.[331] Eurocontrol has indeed developed IT tools and services known as Data Collection and Distribution Services (DCS and DDS) that allows it to collect "all of the real-time data generated by the network and share it with all operational partners".[332] The general public did not have access to such data until recently. However, this may have evolved slightly due to EU obligations with regards to transparency and access to documents held by administrations for citizens. But this has not fundamentally changed the situation. Data has not been 'opened' and the data providers seemingly put strict data confidentiality requirements on Eurocontrol.[333] Access and re-use of data is therefore largely based on what is set in contractual agreements. Bilateral contractual relationship in place "for obtaining the data also has implications in terms of sharing the data with third parties".[334]

Practical guidance for RNE -

- Though airspace air traffic management (ATM) is a three-dimensional dynamic process, a parallel can be made with railway traffic management. Much like railway traffic management, ATM indeed plays a crucial safety and operational role in the smooth provision of flight services.
- Both the railways and the aviation sectors are characterized by their systematic nature and, therefore, the numerous (operational) interfaces between actors. The existence of such interfaces results in the creation of numerous data related to the interactions between them.[335]
- This being, the aviation sector is more complex than the railway one in terms of ecosystem. First, and though closely related, one may differentiate between airport slots and air traffic management slots which obey different processes.
- Second, ATM involves many different types of actors, such as air navigation service providers (ANSPs), airports, aircraft operators and regulatory authorities. The network manager (Eurocontrol), appointed by the EC, acts as a coordinator and facilitator. It plays an active role in air traffic flow management (ATFM).
- In terms of data exchange, some operational data in the ATM sector is shared between actors, specifically between the stakeholders (ANSPs, airspace users and airports) and network manager, for operational purposes, pursuant to data sharing obligations (specifically vertically between the network manager and the 'operational stakeholders').
- In the absence of specific statutory law, which data and/or information shall be deemed confidential remains unclear.

[331] Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability conducted prepared for the European Commission, DG Communications Networks, Content & Technology by Deloitte (2018), p. 263: https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en.

[332] On the Network Manager's B2B services, see Eurocontrol website: https://www.eurocontrol.int/service/network-manager-business-business-b2b-web-services.

[333] Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability conducted prepared for the European Commission, DG Communications Networks, Content & Technology by Deloitte (2018), p. 264.

[334] *Ibid*., p. 264.

[335] On this, and especially on the role that the liberalization process has been playing on the creation of data in the mobility sector, see Juan J Montero and Matthias Finger, 'Platformed! Network Industries and the New Digital Paradigm' (2017) 18 Competition and Regulation in Network Industries 217.

- The sharing of ATM operational data with 'third parties' for non-operational (*i.e.*, commercial) purposes is limited and dependent on the contractual agreements between the network manager and the operational stakeholders such as airline/aircraft operators.
- Apart from ATM operational data, safety related data and information may also be shared (such as for incident/accident event reporting).
- But data silos are in place in the aviation sector, with each stakeholder harnessing its data with very little intent(s) of exchanging it.

4.5. The absence of explicit ad hoc data sharing obligations outside ATM?

4.5.1. Some data and information sharing obligations in the field of safety

Some safety related data sharing has been promoted at the international level by regulatory authorities (ICAO).[336] Indeed, aviation service providers have reporting obligations of safety or security related events.[337] But this concerns mostly information (structured data) than data itself. At the European level, regulation mandates a centralized and standardized manner of collecting, sharing and analyzing safety investigations and the resulting safety recommendations.[338] Moreover, incident and accident reporting are mandated. The sharing of information or data is therefore of a vertical nature between the airline operators and the regulators.

4.5.2. The absence of widespread data sharing in aviation

Outside the ATM field, there is little sharing of data between actors. From a legal perspective, there a few data sharing obligations and conversely, there are few data confidentiality obligations. More simply put, there are currently no regulations preventing companies from sharing data but also no regulations enabling them to do so.

Instead, as has been noted in an EC commissioned study, confidentiality is mainly enforced on a contractual basis.[339] This same study differentiates the types of data. First, operational data, which stems from the aircraft itself, can in some instances be shared from the operator to the manufacturer. Such data can be used to increase the operational efficiency and safety of flight operations. This sharing of data is however based on a contractual agreement(s) which may contain non-disclosure provisions. The amount of data shared is however limited according to this study which mentions that aircraft manufacturers and airlines do not approach the data angle through the concept of 'data ownership' but rather that of 'data sovereignty'.[340] The study also notes that airlines usually have a big advantage in negotiating contractual provisions in their favor. Access to data is therefore only granted in a rather

[336] See for instance: Annex 13 Aircraft accident and incident investigation to the 1944 Chicago Convention and ICAO Doc 9859 - Safety Management Manual.
[337] See: Skybrary Article, "Safety occurrence reporting", https://skybrary.aero/articles/safety-occurrence-reporting.
[338] Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC.
[339] Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability conducted prepared for the European Commission, DG Communications Networks, Content & Technology by Deloitte (2018), p. 266 and following: https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en.
[340] *Ibid,* p. 266-267.

limited way, for instance only to support service provision. The re-use of data exchanged is determined and restricted by the contractual provisions which vary greatly from one to another.[341] The aforementioned study states that manufacturers "do not advocate for a hard policy measure forcing operators to open up access to data, which may be business sensitive"; "it could also expose the aircraft to serious security and safety vulnerabilities".[342] Second, so called technical data, which refers to product information, is usually exchanged "in a very extensive but controlled way".[343] Such data is also subject to IP rules, legislation and contractual requirements. Finally, commercial data, which refers to sensitive data, is usually kept by actors who hold it and protect it through trade secret and IP law.

4.5.3. Flight tracking data and aggregating platforms: some open data in practice?

It must however be noted that some flight data can be accessed by third parties (and the public at large).

Many websites (such as flighradar24, FlightAware, OpenSky Network) provide a tracking platform service where users can have access to a flight's ID, altitude, GPS position, transponder code etc. Such platforms seem to rely on both terrestrial ADS-B receivers as well as satellite-based ADS-B receivers (where no terrestrial coverage exists). For instance, Flightradar24 explains the process as follows: the "1) aircraft gets its location from a GPS navigation source (satellite); 2) The ADS-B transponder on aircraft transmits signal containing the location (and much more); 3) ADS-B signal is picked up by a receiver connected to Flightradar24; 4) Receiver feeds data to Flightradar24".[344]

ADS-B[345] and mode S[346] are communication technologies which are widely used in (commercial) aviation. As noted by this article, "Mode S/ADS-B data updates rapidly, is very accurate and provides pilots and air traffic controllers with common air situational awareness for enhanced safety, capacity and efficiency. Further, it can provide a cost-effective solution for surveillance coverage in non-radar airspace".[347]

But flight tracking platforms seem to aggregate data from a wider spectrum of sources which includes data from satellites, airports, airlines, ANSPs, etc. Presumably, most of these are publicly available data.

---

[341] *Ibid,* p. 266.
[342] *Ibid*, p. 268.
[343] *Ibid*, p. 266.
[344] Flightradar24 website, retrieved on 4 March 2022: https://www.flightradar24.com/how-it-works
[345] ADS-B stands for Automatic Dependant Surveillance – Broadcast. The dedicated SESAR website in Europe desribes ADS-B as such: "ADS-B involves the aircraft using a certified position source to determine own position and broadcasting it in short intervals by means of a data link in radio frequency spectrum. This functionality is usually referred to as ADS-B Out. Conversely, an aircraft can be fitted with an ADS-B receiver – processor to display the detected ADS-B transmissions from other aircraft to the pilot. This is then referred to as ADS-B In. With ADS-B, realtime visiblity is provided to air traffic control and to other equipped ADS-B aircraft with position and velocity data transmitted periodically. ADS-B also provides the data infrastructure for inexpensive flight tracking, planning, and dispatch. In high complexity environments such as the EU airspace, ADS-B is envisaged to operate in conjunction with existing independent cooperative chains, greatly enhancing accuracy, data availability and reducing frequency load" (retrieved on 4 March 2022: https://ads-b-europe.eu/).
[346] Mode S refers to a type of Secondary Surveillance Radar (SSR). Whereas primary radars are said to be passive as they reflect a radio signal that bounces on the aircraft, SSR technology relies on (aircraft) transponders which emit certain data when interrogated by an active secondary surveillance radar. Whereas primary radar only gives information on the position of the aircraft, Mode S transponders also provide information on pressure altitude.
[347] Skybrary, "Mode S", retrieved on 4 March 2022: https://skybrary.aero/articles/mode-s

Flight tracking services can therefore provide its users with accurate information on a particular aircraft's position, altitude, speed, type of equipment used, registration, etc. These websites also provide real time data on the flights schedule and delay.[348] Some of the flight's information therefore seems to be public.

However, most of these websites require payment in order to access all of their services/information. But there are also some crowdsourcing websites which rely on its users to feed in flight data (such as from terrestrial ADS-B receivers).[349]

Practical guidance for RNE –

- Though outside the ATM sector, there are some information sharing obligations such as in the field of safety occurrences, legally mandated data sharing obligations seem to be scarce.
- Certain types of data are deemed confidential by some aviation stakeholders which therefore protect it through confidentiality (contractual provisions) when they interact with other stakeholders.
- However, it can be noted that some flight data is more or less widely available in practice via flight tracking websites or applications. These latter provide users (sometimes against a fee) access to a flight's path, position, altitude, speed. In most instances, they also provide real time information on the flight's schedule and delay(s). Such aggregated data and resulting information can be useful for the passengers or relatives of passengers who can therefore see if the aircraft is running late or not in real time. Some of these services can be integrated in wider travel service websites or applications.

4.6. The impact of the deployment of Automated ATM/Flying and the U-Space framework: an opportunity for more data sharing?

Though data already plays an important role in the aviation eco-system, it is expected to have an even more prevalent role in the years to come. Indeed, it is expected to help foster new technologies and processes in various fields: operations, U-space and automated flying.[350] Data sharing is an important opportunity in air traffic management as well.[351] A lot of stakeholders recognize the fact that data sharing will be beneficial for them in certain fields. Moreover, the increased reliance on automation and AI related technologies requires more open data or data sharing practices. This is the paradox: data sharing is recognized as an important enabler for the development of future aviation services; however, actors seem unwilling to share such data at the moment. There are currently EU funded projects for data sharing platforms in aviation.[352] But these are still not widespread.

However, things could move with the advent of UAS (or unmanned aircraft systems) and the U-Space. The U-Space concept of operations refers to the traffic management setting surrounding the safe operation of unmanned aircraft. Indeed, current air law regulations on air traffic management do not seem adapted to dealing with low altitude operations of unmanned aircraft systems (UAS). As one

[348] These websites therefore also rely on airlines' published schedules.
[349] See for instance: https://globe.adsbexchange.com/
[350] On the role of automation in ATM and aviation in general, see analysis of the EASA roadmap of AI in aviation: Ivo Emanuilov & Orian Dheu, "Flying High for AI? Perspectives on EASA's Roadmap for AI in Aviation", *Air & Space Law*, vol. 44, n°1, p. 14-16.
[351] Digital European Sky (Phase D) of the European ATM Master Plan.
[352] See for instance the ICARUS or Aviation-driven Data Value Chain for Diversified Global and Local Operations project: https://www.icarus2020.aero/icarus-platform-architecture/.

author puts it, once these aircraft are deployed, there will be "so many UAS that the established air traffic management (ATM) infrastructure risks not having the means to manage all of them".[353] As noted by Huttunen, the U-Space concept of operations is based on the premise that it is important "to facilitate the access of drones, with proper qualifications, into pre-existing segments (…) The U-space concept does not, however, attempt to interfere with the regime already in place for manned aircraft. Rather, U-space is meant to enhance all airspace with a collection of new services and procedures".[354] As explained in a SESAR document, U-Space will be organized as a "federation of U-Space service providers that can cooperatively manage drone traffic in the same or/and adjacent geographical region, under a regulatory framework ensuring the overall performance level and in particular its safety".[355]

In that respect, a new regulatory framework was adopted in 2021.[356] It provides for some data sharing obligations between certain actors of the complex U-Space eco-system which ranges from UAS operators to U-Space service providers. Recital 16 of this Regulation recognizes that "this Regulation should establish requirements for common interoperable open communication protocols between authorities, service providers and UAS operators, as well as data quality, latency and protection requirements for the information exchanged, necessary for safe and interoperable operations in the U-space airspace". The Regulation states that "Member States shall give access to U-space service providers to the relevant data, if required for the application of this Regulation, as regards to" UAS operator's registration system.[357] Member States are required to make certain types of airspace data available as part of the common information services of each U-space airspace.[358] Providers of common information services must ensure that such information complies with the necessary data quality, latency and protection requirements (as prescribed in Annex III to the regulation).[359] The Regulation also states that U-space service providers "shall establish arrangements with the air traffic services providers to ensure adequate coordination of activities, as well as the exchange of relevant operational data and information in accordance with Annex V".[360] Moreover, U-space service providers shall "handle air traffic data without discrimination, restriction or interference, irrespective of their sender or receiver, content, application or service, or terminal equipment".[361]

Practical guidance for RNE -

[353] Mikko Huttunen, "The U-Space Concept", *Air and Space Law*, 44, n°1, p. 71.
[354] *Ibid*., p. 81.
[355] SESAR Joint Undertaking, "European ATM Master Plan; Roadmap for the safe integration of drones into all classes of airspace", SESAR Joint Undertaking, 2018, p. 10.
[356] Commission implementing Regulation (EU) 2021/664 on a regulatory framework for the U-Space of 22 April 2021.
[357] Article 3 (5) of Commission implementing Regulation (EU) 2021/664 on a regulatory framework for the U-Space of 22 April 2021.
[358] Article 5 (1) of Commission implementing Regulation (EU) 2021/664 on a regulatory framework for the U-Space of 22 April 2021.
[359] Article 5 (4) of Commission implementing Regulation (EU) 2021/664 on a regulatory framework for the U-Space of 22 April 2021.
[360] Article 7 (3) of Commission implementing Regulation (EU) 2021/664 on a regulatory framework for the U-Space of 22 April 2021.
[361] Article 7 (4) of Commission implementing Regulation (EU) 2021/664 on a regulatory framework for the U-Space of 22 April 2021.

- It is possible that the advent of new technologies embedded in (autonomous) unmanned aircrafts and the associated U-Space eco-system may push the regulatory balance in favor of more data sharing (albeit being focused on operational data).
- Moreover, a proposed recast of the Single European Sky Regulation may also push for increased data sharing in the field of ATM (see for instance proposed Article 31 on “availability and access to operational data for general air traffic").[362]

4.7. Conclusion

Despite being data driven, the aviation sector, with the exception of ATM, has very few data sharing or confidentiality legal obligations. One can sense a reluctance of actors in sharing data between them and with third parties. When data sharing is mandated, for instance towards the network manager, contractual agreements arrange for certain confidentiality requirements and set the rules of access on use and re-use of data by third parties. However, this data paradox may be called to evolve with the increased need of shared data within automated flying systems and the advent of U-Space operations.

5. Conclusion and way forward

The conclusions are summarized in a table summarizing the challenges identified or the question asked and the propositions for a way forward, where identified.

Challenge identified or question	Further comments	Solution and proposition for a way forward, where identified
Unclear legal framework on data, both in general and more specifically concerning railway data	The lack of clarity of the legal framework concerning data, and especially in their function as an economic resource, is not unique to the railways. It can be found in many sectors, both similarities, *i.e.*, the absence of a by default legal status of data, and differences. The regulation of railway data is characterized by fragmentation across the EU, following the fragmentation of (railway) national law and the differences in status of IMs, under national law. Additionally, railway data are characterized by a large number of regulations at EU level, which result in a complex – and ever-evolving - picture.	The study (1) shed some light on the applicable legal frameworks, both railway-specific and non railway-specific, including the most recent legislative initiatives; (2) brought them together and (3) identified patterns which are currently at work. In this respect, there appears to be a shift from an ‘ownership’ perspective (with the aborted option to create a data producer’s right) to a more granular approach with data rights, possibly allocated to different stakeholders on the same data. The shift to data rights is additionally based on access rights, which takes data yet a step further from ownership.
Confidentiality obligations	SERA Directive confidentiality obligations are vague, in terms of both their scope of application,	The present study cannot fully alleviate the fragmentation of the interpretation of

[362] European Commission, Amended Proposal for a Regulation of the European Parliament and of the Council on the implementation of the Single European Sky (recast), 22 September 2020, COM(2020) 579 final, p. 122: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A579%3AFIN

incumbent on the IMs based on the SERA Directive are not clear and subject to diversified interpretation throughout the EU	the procedure for labelling information as confidential and the legal consequences of confidentiality. Such obligations are further substantiated in contracts or other arrangements between the IM and the RUs, and in particular the contract of use. The contractual (or otherwise legal) provisions regulating confidentiality depend on the nature of such legal instrument, on its regulation under national law and on the balance of powers between the IM and RUs (' representatives). Confidentiality appears to be interpreted more extensively by IMs which are not subject to conflicting obligations such as transparency, data access or data sharing obligations, to the extent that it may, for instance, ban any form of processing beyond what it strictly necessary for the performance of the contract of use by the IM. In such case, confidentiality appears to functionally play the role of a proxy for ownership. When IMs are subject to such obligations, they have to strike a balance between confidentiality on the one hand and transparency / data access / data sharing obligations on the other hand, which results in confidentiality being interpreted more strictly with respect to its scope of application, procedure for labelling information as confidential and legal consequences.	confidentiality, especially when regulated in detailed contractual (or otherwise legal) provisions. This being, (1) the present study brings some clarity on the interpretation and application of confidentiality obligations, based on the combined application the SERA confidentiality obligations with other EU railway-specific legal frameworks. It follows that (i.) the liberalization process and the establishment of a level playing field between RUs shall play a role as overarching objectives of EU law. The liberalization process does however not have a univocal effect on confidentiality obligations. (ii.) A distinction between passenger vs freight traffic shall be made. Information and data which shall be made available to the public pursuant to the (New) PRR, such as train circulation data and punctuality data, cannot be deemed confidential. This is without prejudice to the question whether similar data related to freight services should be deemed confidential. (2) We identify avenues towards harmonized interpretation of confidentiality, in a way which allows for some data monetization and in line with patterns identified in EU law. This is based on the following sources: - The experience of IMs confronted with transparency / data sharing / data access obligations simultaneous to confidentiality; - The Data Governance Act (Chapter II); - Confidentiality in competition law; - the ELI-ALI Principles for the Data Economy. All such sources converge in finding that confidentiality should not necessarily result in a ban on further processing. Some of such sources also provide a range of legal, technical and organizational mechanisms which can be

		leveraged to share data while protecting confidentiality. Some of these sources also suggest that confidentiality claims should be based on transparent and objective reasons, at the initiative of protected entities (in this case, RUs). Confidentiality should indeed neither be confused nor used as a proxy for ownership of data.
	General recommendation: - The study places RNE data (and more generally, railway data) and its attempts to engage into data commercialisation in the broader perspective of the data economy. - It invites to approach confidentiality obligations under the SERA Directive with more granularity, beyond the seemingly 'open vs close' dichotomy. - Confidentiality implies three main components, namely (i.) scope of application, (ii.) procedure for labelling information as confidential and (iii.) legal effects, or in other words legal regime applicable to confidential information. - Pursuant to the recommendations to have more granularity in the level of openness of data and to bring more transparency in the procedure for labelling information as confidential, we recommend the adoption of a data policy, ideally both at IM and RNE level, to support their respective strategies and objectives concerning data. - The data policy serves to have a transparent (at least, internally to the entity, whether IM or RNE but also, to some extent, externally), comprehensive and business-oriented process in place for deciding about the regime applicable to certain information and data and in particular concerning confidentiality. The data policy shall build upon a clear decision-making process, which takes into account all parameters and interests at stake. - The data policy could also enable a shift from a 'close by default' regime to information (as potentially confidential) to an evidence-based policy, where confidentiality claims shall be duly justified.	
There is a dichotomy between sharing vs not sharing data, namely between open vs close data	The analysis shows that there is not only a dichotomy between close vs open data, or between sharing vs not sharing data. The question is also under which conditions RNE (members) are entitled to share data, where appropriate. When data or information are shared, they may be shared either (i.) free or charge or under strictly regulated conditions (such as marginal cost for sharing data, irrespective of the other costs incurred by the generation of data and of the actual value of data) or (ii.) with an economic price.	The analysis shows that IMs and RNE are, in principle, free to levy an economic price, save where prohibited. Such view is notably confirmed by the Open Data Directive. While public undertakings active in utilities (as IMs could be) are in the scope of the Directive, they remain free to set their own price (in contrast to public sector bodies), subject only to transparency and non-discrimination principles. Exceptions can be found with high-value datasets (still pending EC regulations). Pricing regulation for data sharing by IMs remains piecemeal when pursuant to data sharing obligations by law.

		Recent railway legal frameworks (namely, the recently revised TAF TSI and the New PRR) do both reckon that the provision of data is costly and that it is legitimate for the data 'sharer' to recover such costs. Data exchange conditions, including financial conditions, may depend on national legislations (such as transparency / data access / data sharing obligations incumbent on the IM).
Can the railways learn from other sectors, such as the aviation sector, in particular concerning (i.) data sharing practices and (ii.) confidentiality regime?	Drawing a comparison with the aviation sector does not allow us to provide conclusions nor recommendations despite some similar settings and problems. - The aviation sector is indeed confronted with the same difficulties, namely the lack of data sharing, specifically non-operational data, but also the lack of sharing of operational data for non-operational (*i.e.*, commercial) purposes. Such data sharing could prove useful, for instance, for the emergence of new services. - There are data sharing obligations in the ATM field where some operational data must be shared between the operators and the ATM network manager in order for the ATM system to properly function. But this seems to mainly be on a B2G relationship (*e.g*. between the operators, airports, ANSPs and the network manager, appointed by the EC). - This lack of broader data sharing may be (partially) addressed when innovative technologies (automated flying, automated ATM) and operational eco-systems such as U-Space, are developed and deployed. Such new technologies, services and settings will require increased sharing of data, presumably operational data. But there may be a thin line in distinguishing between 'operational' and 'non-operational' data. Indeed, even operational data may potentially have commercial implications. - The foreseen recast of the Single European Sky Regulation seems to be pushing for increased data sharing between stakeholders in ATM within the broader context of mobility data spaces. In that respect, the Commission staff working document on Common European Data Spaces refers to its amended proposal for a recast of the Single European Sky Regulation which would include "among other things, new provisions on data availability and market access of data service providers in the field of air traffic management". This signals that policymakers in the aviation sector are pushing for increased data sharing provisions, as part of the Mobility Data Space.	

Annex 1

RNE questionnaire on confidentiality

RNE Legal Matters Working Group

Questionnaire

on

confidentiality of train information in Europe

RailNetEurope
Oelzeltgasse 3/9

1030 Vienna

Phone: +43 1 907 62 72 21
tsvetan.tanev@rne.eu
www.rne.eu

May 2021

Context

The confidentiality obligation of the infrastructure manager (IM) towards the applicants concerning train information[363] at the level of EU law originates from several short stipulations in Directive 2012/34/EU (e.g., Art. 29(4)[364], Art. 39(2)[365], Art. 42(7)[366] and Art. 46(3)[367]. They are almost identical as a wording, meaning and location with those in the repealed Directive 2001/14/EC, which already amounts to more than 20 years of history of the topic. In general, those norms are not grouped in one single place in the preamble and/or the main body of the Directive but they are rather decentralised and included on a functional principle at the end of different sections of Chapter IV of the Directive (e.g., *Infrastructure and services charges; Allocation of infrastructure capacity*).
In short, the Directive makes it compulsory for the IM to respect the "commercial confidentiality" of the information provided to it by the applicants within the context of charging and capacity allocation. But there are several open points to be considered:

- The Directive does not provide for further explanation about what is to be considered as confidential. Thus, the other major phase of the train life cycle (i.e., traffic management) is somehow omitted. One conclusion could be that the IM shall respect the confidentiality of information of applicants in capacity allocation and, by analogy, as well as in traffic management. However, as there are no explicit confidentiality requirements for the traffic management process, one could also claim that data of the factual train run is not covered by the confidentiality obligation of the IM under the Directive. Understandably, different contractual arrangements IM-applicant, based on the general civil law, could always apply here.
- The directive does neither specify what legal regime the notion "confidential information" entails[368], nor the sanctions incurred in case of violation of confidentiality. Therefore, it falls within the legislative competence of the Member State and the contractual freedom of IMs and applicants to regulate the topic.

[363] Please note that for the purposes of this questionnaire 1) train information and train data are used as synonyms and 2) train information/data means the data collected by the IM for the train paths allocated to the applicants (i.e., timetable information) and the factual train running information, collected and processed in particular IT tool(s).

[364] Article 29

Establishing, determining and collecting charges

[…] 4. An infrastructure manager shall respect the commercial confidentiality of information provided to it by applicants.

[365] Article 39

Capacity allocation

[…] 2. Infrastructure managers shall respect the commercial confidentiality of information provided to them.

[366] Article 42

Framework agreements

[…] 7. While respecting commercial confidentiality, the general nature of each framework agreement shall be made available to any interested party.

[367] Article 46

Coordination process

[…] In accordance with Article 39(2), that information shall be provided without disclosing the identity of other applicants, unless applicants concerned have agreed to such disclosure.

[368] For example, 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 and its national transposition acts in the Member States.

- The technical regulations on data exchange in the sector (e.g. TAF TSI Regulation[369], TAP TSI Regulation[370], OPE TSI Regulation) do neither deal with the issue of confidentiality.

On the other hand, in the fast-growing data economy in 2021, the issue of confidentiality in railways could be among the potential obstacles for free flow of data to all stakeholders involved in the logistic chain (e.g., shippers, freight forwarders, combined transport operators, service facilities operators, etc.) and any other sort of ventures benefiting from data in the sector (e.g., manufacturers, start-ups, IT companies, data brokers).
Therefore, this set of questions aims at identifying 1) the transposition of the above stipulations in your national law and 2) the contractual relations IM-applicant when it comes to confidentiality of train information and the whole concept of the IM-applicant confidentiality, including the national particularities. The summarised results of this questionnaire will be an input to the project 'External legal study on marketing of RNE data' ordered from RNE to KU Leuven, Belgium.

Note:
Indeed, the last question is not related to the issue of confidentiality. However, with the amended TAF TSI Regulation in force as of 18 April 2021 (see footnote 7 below), the possibility for charging for some of the messages for freight trains by the IM is now officially allowed by the EU legislator. To this end, it would be important to understand your current practice and future plans regarding data exchange of messages for both freight and passenger trains.

[369] Commission Regulation (EU) No 1305/2014 on the technical specification for interoperability relating to the telematics applications for freight subsystem of the rail system in the European Union and repealing the Regulation (EC) No 62/200
[370] Commission Regulation (EU) No 454/2011 on the technical specification for interoperability relating to the subsystem 'telematics applications for passenger services' of the trans-European rail system

Name of your company: ……

1. Does your company have the legal obligation to keep confidential train information of applicants (e.g., RUs)?

☐ Yes; If yes, what is the legal basis of the IM obligation (multiple selection is possible):

- ☐ National law (e.g., Railway act, Competition Act, decree of the government, etc.)
- ☐ Network statement
- ☐ General terms and conditions of the IM
- ☐ Contract of use of infrastructure/track access agreement
- ☐ Other (please briefly explain): ……

☐ No

2. What is considered confidential between IM and applicants when it comes to train information in the capacity allocation process (multiple selection is possible)?

☐ Path request
☐ Allocated train path
☐ Allocated path modifications and/or alternations
☐ All of the above
☐ None of the above
☐ Other (please briefly explain): ……..

3. What is considered confidential between IM and applicants/RUs when it comes to train information in the traffic management process?

☐ Train running information, for example (multiple selection is possible):

- ☐ RU name
- ☐ train number
- ☐ train type (e.g., passenger or freight)
- ☐ origin
- ☐ destination
- ☐ train delay
- ☐ train weight
- ☐ train length
- ☐ train maximum speed
- ☐ wagons numbers
- ☐ cargo/freight type (e.g. goods in the wagon)
- ☐ other elements (please briefly explain): …….

☐ All of the above
☐ None of the above
☐ Other (please briefly explain): ……..

4. Does your company apply different rules on confidentiality of train information for freight trains/RUs and passenger trains/RUs? (e.g., different confidentiality clauses in the contract of use of infrastructure, different elements of the train as listed above).

☐ Yes; If yes, please briefly explain the difference and the reasons: …….
☐ No
☐ Other (please briefly explain): ……

5. Does your company's contractual arrangements with the Applicants/RUs envisage specific sanctions for the IM in case of violation of confidentiality obligation (e.g. penalties)?

☐ Yes; If yes, please briefly explain the preconditions for infringement and the amount(s): …….
☐ No
☐ Other (please briefly explain): ……

6. Respecting your internal rules, would you share with RNE the text of your confidentiality clause relevant for the train information?

Please copy it here - preferably in English (if available); alternatively in your national language:

……..

7. Has your company been involved in any significant case before a regulator or/and a court regarding confidentiality issues between IM and applicants/RU(s)?

☐ Yes; if yes please include the name of the regulator/court, the parties, the number and the year of the case and briefly summarize the key questions addressed and conclusions or provide a link to the decision (if available): ……..

☐ No

8. Does your company charge the applicants (e.g., RUs, other stakeholders) for data exchange of TAF/TAP TSI messages in the respective IT tools used for capacity and traffic management?

☐ Yes, we do charge for some/all messages sent by the IM to the RUs.

8.1. If the IM does charge, is the charge then

☐ considered a part of the minimum access package and included in the infrastructure charges/track access charges;
☐ considered as additional or ancillary services;
☐ handled in other way (please briefly explain): ……

☐ No, we do not charge for some/all messages sent by the IM to the RUs

8.2 If the IM does not charge at the moment, do you plan in near future starting to charge and in what way?

☐ No
☐ Yes ☐ We apply other approach to data exchange with the RUs (please briefly explain): ……

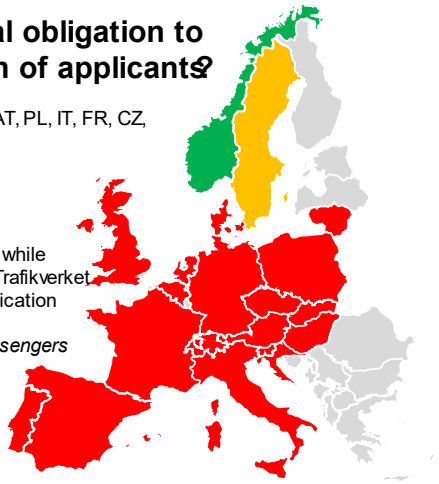
Annex 2

RNE overview of the IMs replies on confidentiality

Question N 1

Does your company have the legal obligation to keep confidential train information of applicants?

- National law(16): BE,CH, ES, DK, HR, PT, LT, HU, UK, AT, PL, IT, FR, CZ, SK, NL, DE
- NS(3): CH, HU, IT
- GTC(8): CH, HR, HU, UK, AT, FR, SI, NL
- CUI/TAA(11): DK, HR, PT, LT, HU, UK, PL, IT, FR, SI, NL
- Other(3): CH(IT), ES(FA), CZ(Internal)
- SW: the general rule is that the information is public while confidentiality is the exception. Information reported to Trafikverket by a RU/Applicant prior to train departure via a web application *"is only available Trafikverket and contracting parties, with the exception oftraffic information that benefits passengers and the public. The information is also available to market actors who are developing traffic information services for passengers and the public*



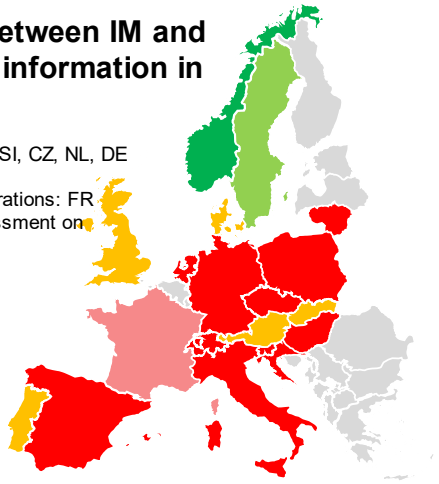
RNE RailNetEurope

2

Question N 2

What is considered confidential between IM and applicants when it comes to train information in the capacity allocation process?

- All allocation info (11) BE, CH, ES, HR, LT, HU, PL, IT, SI, CZ, NL, DE
- Only path request (5): DK, PT, UK, AT, SK
- Only path request and allocated path modifications/alterations: FR
- The applicant's understanding is not decisive; the assessment on confidentiality is made by the IM
- None: NO



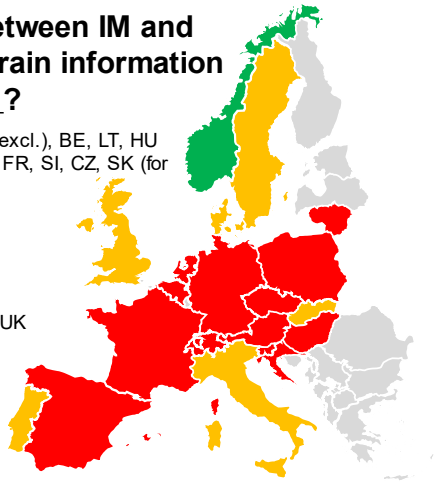
All info
None
Path request

All info = path request, allocated train path, allocated path modifications and/or alterations, etc.

Questions N 3

What is considered confidential between IM and applicants/RUs when it comes to train information in the traffic management process?

- All train running info: CH (pass. excl.), ES, HR (delay excl.), BE, LT, HU (train type excl.), ATPL (RU name and train type excl.), FR, SI, CZ, SK (for freight trains), NL, DE (train type excl.)
- Cargo/freight type (e.g. goods in the wagon): DK
- Train weight, wagons numbers, cargo/freight type: PT
- Origin, delay, cargo/freight type, performance regime: UK
- Train weight, train length, train maximum speed, wagons numbers, cargo/freight type: IT
- None: NO, for passenger trains in CH, SW and SK

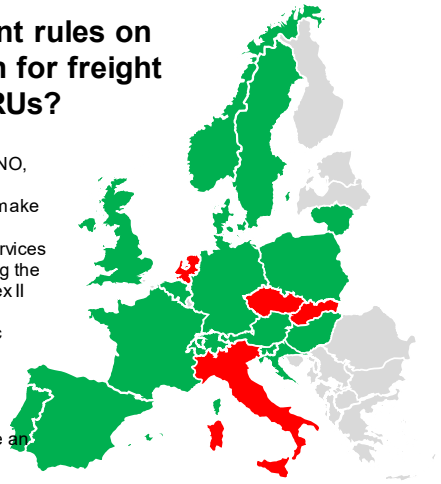


All info
None
Other

Question N 4

Does your company apply different rules on confidentiality of train information for freight trains/RUs and passenger trains/RUs?

- No (14): BE, CH, ES, DK, HR, PT, LT, HU, UK, AT, PL, FR, NO, SI, SW
- IT: The Italian Regulatory Body (ART) has required RFI to make available to RUs in a non-discriminatory way real-time data relating to the trains of other RUs operating passenger services in order to allow all RUs to provide their passengers during the journey at least the information referred to in Part II of Annex II to Regulation (EC) no. 1371/2007
- CZ: there is some non-confidential information about public passenger trains
- SK: in the case of public passenger transport, there is an obligation to publish timetables and information on train movements
- NL: Basis is Art. 6 of the GTC. In addition, freight RUs have an article in the CUI about sharing data about arrival and departure times with terminals, neighbour IM's, etc.



YES
NO

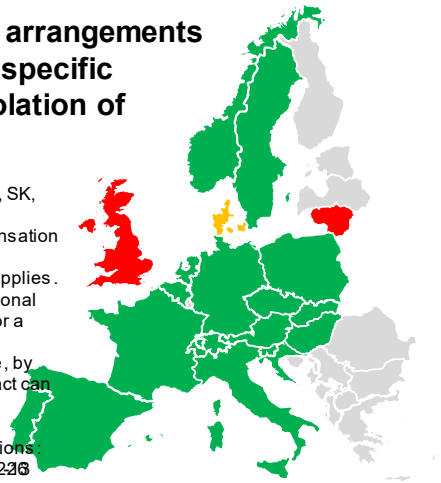
RailNetEurope

5

Question N 5

Does your company's contractual arrangements with the Applicants/RUs envisage specific sanctions for the IM in case of violation of confidentiality obligation?

- No (15): BE, CH, ES, DK, HR, PT, HU, AT, PL, FR, NO, SI, SK, CZ, IT, SW
- LT: Damage compensation. Concrete amount of compensation depends on suffered damage which should be proven
- UK: 1)The general law around confidentiality remedies applies. 2) Where the specific provisions of the Railways Act (national law) have been broken, then the Railways Act provides for a fine and/or potentially prison for extreme/criminal cases
- DK: Disputes are settled via mediation and if impossible, by arbitration. In the event of a substantial breach the contract can be terminated
- FR remark: SNCF Réseau personnel who discloses confidential information to third parties risks penal sanctions: one year's imprisonment and a fine of EUR15 000 (Art. 226-13 of the Penal Code)



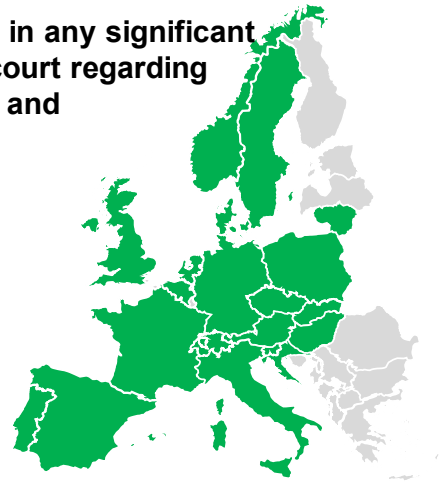
YES
NO
Other

RailNetEurope

6

Question N 7

Has your company been involved in any significant case before a regulator or/and a court regarding confidentiality issues between IM and applicants/RU(s)?



Question N 8

Does your company charge the applicants for data exchange of TAF/TAP TSI messages in the respective IT tools used for capacity and traffic management?

- No and no plans (11): CH, ES, NO, DK, HR, PT, HU, PL, SI, SZ, SK, SW, DE
- Yes (5):
  - Part of the minimum access package LT, UK(?), AT (for messages), FR, NL
  - Additional services: AT (for access to the I-Tool), FR
- Other (2):
  - BE: data flow may be charged (i.e., interfaces); applied to SNCB only
  - IT: upon the signature of a specific contract, RFI provides the RUs with a system-to-system interface to exchange paid messages that are NOT compliant with TAF/TAP TSI standard even though most of these messages include the same information provided by the TAF/TAP ones.