MOBIDATALAB

Labs for prototyping future mobility data sharing solutions in the cloud

D2.1 Legal and Regulatory Data Sharing Gap Analysis

08/08/2022

Author(s): Emre BAYAMLIOĞLU (KUL), Aliki BENMAYOR (KUL), Alberto BLANCO-JUSTICIA (URV), Didier de RYCK (KISIO)

MobiDataLab is funded by the EU under the H2020 Research and Innovation Programme (grant agreement No 101006879).

Summary sheet

Deliverable Number	D2.1
Deliverable Name	Legal and Regulatory Data Sharing Gap Analysis
Full Project Title	MobiDataLab - Labs for prototyping future Mobility Data sharing cloud solutions
Responsible Author(s)	Emre BAYAMLIOĞLU (KUL), Aliki BENMAYOR (KUL)
Contributing Partner(s)	Alberto BLANCO-JUSTICIA (URV) Didier de RYCK (KISIO)
Peer Review	AKKA, ICOOR, POLIS
Contractual Delivery Date	31-01-2022
Actual Delivery Date	28-01-2022
Status	Final
Dissemination level	Public
Version	V1.0
No. of Pages	120
WP/Task related to the deliverable	WP2 / T2.1
WP/Task responsible	AKKA / KUL
Document ID	MobiDataLab-D2.1-LegalRegulatoryDataSharingGapAnalysis-v1.0
Abstract	This deliverable compiles the current EU legal and regulatory frameworks for data sharing and re-use in the transport sector (covering all transport modes) and identifies potential legal gaps that need to be addressed for the smooth operation of transport/mobility data spaces. The analysis provided in this document deals with both horizontally applicable and sector-specific (vertical) legislation.

Funded by the European Union

Legal Disclaimer

MOBIDATALAB (Grant Agreement No 101006879) is a Research and Innovation Actions project funded by the EU Framework Programme for Research and Innovation Horizon 2020. This document contains information on MOBIDATALAB core activities, findings, and outcomes. The content of this publication is the sole responsibility of the MOBIDATALAB consortium and cannot be considered to reflect the views of the European Commission.

Project partners

Organisation	Country	Abbreviation
AKKA I&S	France	AKKA
CONSORZIO INTERUNIVERSITARIO PER L'OTTIMIZZAZIONE E LA RICERCA OPERATIVA	Italy	ICOOR
AETHON SYMVOULI MICHANIKI MONOPROSOPI IKE	Greece	AETHON
CONSIGLIO NAZIONALE DELLE RICERCHE	Italy	CNR
KISIO DIGITAL	France	KISIO
HERE GLOBAL B.V.	Netherlands	HERE
KATHOLIEKE UNIVERSITEIT LEUVEN	Belgium	KUL
UNIVERSITAT ROVIRA I VIRGILI	Spain	URV
POLIS - PROMOTION OF OPERATIONAL LINKS WITH INTEGRATED SERVICES	Belgium	POLIS
F6S NETWORK IRELAND LIMITED	Ireland	F6S

Document history

Version	Date	Organisation	Main area of changes	Comments
0.1	01/12/2021	KUL		Draft for internal Review
0.2	13/01/2022	KUL		Submission for partner review
0.3	3/01/2022	AKKA, ICOOR, POLIS	all	End of review process
0.4	19/01/2022	KUL	all	End of rework phase
0.5	28/01/2022	AKKA		End of Quality check
1.0	28/01/2022	KUL - AKKA		Final version

Executive Summary

Data are increasingly viewed as a commodity to be traded in their own rights. This has created a growing interest from policy-makers in the creation of so-called “data markets” and “data spaces”, viewed as a mean to foster data sharing.

However, the legal framework is not quite well-aligned with this new pattern towards the commodification of data. On the one hand, it is generally agreed that there is no “ownership right” or general exclusive rights on data in the acquis of the European Union (EU). Thus, data cannot be legally ‘sold’ like a physical object. On the other hand, a variety of legal frameworks may apply to data and data transactions.[1]

For example, data protection law is applicable when personal data are processed, competition law may apply as well if data is shared between or pooled by competitors (actual or potential) resulting in the distortion of competition in the relevant markets. In addition, mobility sectoral regulations lay down various types of obligations relating to data directly or indirectly, such as an obligation to provide access for third parties to re-use the data. The legal frameworks have indeed accumulated over time, with various rationales.

[1] Charlotte Ducuing, Lidia Dutkiewicz and Yuliya Miadzvetskaya, ‘TRUSTS Trusted Secure Data Sharing Space - D6.2 Legal and Ethical Requirements’ (2020) p.49, https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf, accessed 14 January 2022.

This report analyses the current EU legal and regulatory frameworks for data sharing and re-use in the transport sector (covering all transport modes), in particular:

Horizontal legislation:

- Privacy and Data Protection (the General Data Protection Regulation, the e-Privacy Directive and forthcoming Regulation);
- Competition law;
- The Public Sector Information Directives (including the 2019 Open Data and Public Sector Information Directive);
- The Regulation on the free flow of non-personal data;
- Legislation concerning digital platforms and/or intermediaries (the e-Commerce Directive, the Platform-to-Business Regulation and the recent Digital Services Act Package);
- The proposal for a Data Governance Act.

Sector-specific legislation:

- The Intelligent Transport Systems Directive (including its Delegated Regulations).

A separate chapter is dedicated to the use case of Mobility-as-a-Service. Through this analysis, several potential legal gaps have been identified that need to be addressed for the smooth operation of transport/mobility data spaces. The gaps have been identified in the following areas:

- The application of the GDPR;
- Competition law;
- The Open Data & Public Sector Information Directive;
- The proposal for a Data Governance Act;
- The Intelligent Transport Systems Directive & Delegated Regulations (namely with regard to their interface with the other horizontal legal frameworks).

An overview of the legal and regulatory gaps can be found in Chapter 6 (Annexes).

Table of contents

Funded by the European Union

List of figures

List of tables

Abbreviations and acronyms

Abbreviation	Meaning
AI	Artificial Intelligence
API	Application Programming Interfaces
CJEU	Court of Justice of the EU
DGA	Data Governance Act [Proposal]
DMA	Digital Markets Act
DSA	Digital Services Act
DSS	Data Sharing Services

EC	European Commission
ECD	E-Commerce Directive
ECHR	European Convention of Human Rights
ECJ	European Court of Justice
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
FCO	German Federal Cartel Office
FRAND	Fair, Reasonable and Non-Discriminatory
GDPR	General Data Protection Regulation
IoT	Internet of Things
MMTIS	Multimodal Travel Information Services [Delegated Regulation]
NAP	National Access Point
P2B	Platform to Business [Regulation]
PSBs	Public Sector Bodies
PTA	Public Transport Authority
PTO	Public Transport Operator
RTTI	Real-Time Traffic Information Services [Delegated Regulation]
TFEU	Treaty on the Functioning of the European Union
T&Cs	Terms & Conditions
VLOP	Very Large Online Platforms

1. Introduction

1.1. Project overview

There has been an explosion of mobility services and data sharing in recent years. Building on this, the EU-funded MobiDataLab project works to foster the sharing of data amongst transport authorities, operators and other mobility stakeholders in Europe. MobiDataLab develops knowledge as well as a cloud solution aimed at easing the sharing of data. Specifically, the project is based on a continuous co-development of knowledge and technical solutions. It collects and analyses the advice and recommendations of experts and supporting cities, regions, clusters and associations. These actions are assisted by the incremental construction of a cross-thematic knowledge base and a cloud-based service platform, which will improve access and usage of data sharing resources.

1.2. Purpose of the deliverable

This deliverable focuses on a legal and regulatory data sharing gap analysis.

The objective of this deliverable is to compile the current EU legal and regulatory frameworks for data sharing and re-use in the transport sector (covering all transport modes) and identify potential legal gaps that need to be addressed for the smooth operation of transport/mobility data spaces. The analysis provided in this document deals with both horizontally applicable and sector-specific (vertical) legislation.

Specific focus has been given on examining the interplay between horizontal & sector-specific legislation, for example, on the one hand, the General Data Protection Regulation and the Open Data and Public Sector Information Directive, and the other hand, the Intelligent Transport Systems Directive.

Several examples are also provided, including by drawing inspiration from deliverable D2.9 on transport use cases, to analyse concrete legal issues arising in different mobility scenarios. Examples from the relevant national legislation are also provided, where available from the literature.

Finally, it should be noted that at the time of writing of this deliverable, part of the draft legislations analysed below are still under discussion by the EU Institutions while others are under review by the European Commission. As such, the provisions analysed may not reflect the final legislative text while some of the legal gaps we have identified in our analysis may be addressed by the review.

1.3. Structure of the deliverable and its relationship with other work packages/deliverables

This deliverable is organised as follows. Section 2 sets the scene by providing an overview of the European Commission's strategy on data and data sharing. Section 3 identifies the horizontal and sector-specific EU legal frameworks applicable to data sharing in the transport sector as well as the gaps that need to be solved to improve data sharing. Section 4 conducts a similar analysis to that of Section 3 through the use case of Mobility-as-a-Service.

2. Setting the scene: the European Commission's strategy on data & data sharing

2.1. The 2014 Communication "Towards a thriving data-driven economy"

In its 2014 Communication[2], the European Commission ("EC" or "Commission") pledged the creation of a single market for big data and cloud computing. It recognised however that the complexity of the current legal environment along with the insufficient access to large datasets created barriers and stifled innovation. To reap the benefits of the data economy, the EU must: (i) extensively share, use and develop its public data resources, and (ii) make sure that the relevant legal framework and the policies, such as on interoperability and data protection are data-friendly, leading to more regulatory certainty for business and creating consumer trust in data technologies.

The EC sets out that data is at the centre of the future knowledge economy and society and 'open data' (i.e. data made freely available for re-use to everyone for both commercial and non-commercial purposes[3]) in particular will play a significant role in data-driven innovation. To facilitate exploitation and reduce transaction costs, restrictions on data re-use should be minimised, leading to more harmonisation.

2.2. The 2017 Communication "Building a European Data Economy"

In the 2017 Communication, the EC reiterates its objectives set out in the Digital Single Market Strategy to create a clear and adapted policy and legal framework for the data economy, by removing remaining barriers to the movement of data and addressing legal uncertainties created by new data technologies. The document focuses on the following issues[4]:

[2] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Towards a thriving data-driven economy', 2 July 2014, COM (2014) 442 final.
[3] *Ibid*, p.5.
[4] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Building a European Data Economy', 10 January 2017, COM (2017) 9 final.

Funded by the European Union

i) **Free flow of data**: any barriers to the free movement of data in the EU, such as data localisation requirements need to be abolished. The Commission introduces the "principle of free movement of data within the EU", which should guide Member State action affecting data storage or processing, alongside the principles of free movement of services and the free establishments provisions of the EU Treaty. This principle should also apply in cases where the GDPR allows Member States to regulate specific matters. To implement this action point in relation to non-personal data, the Regulation on the free flow of non-personal data was adopted in November 2018 (further analysed under section 3.7 below).

ii) **Access and transfer in relation to machine-generated data**: The Commission recognises that to extract the maximum value from machine-generated data (including in the transport sector), market players need to have access to large and diverse datasets. Machine-generated data can be personal or non-personal or mixed datasets. The current landscape suggests that companies holding large quantities of data keep them in silos and exchange of data remains limited. Data marketplaces are emerging, but slowly, and are not widely used. The Commission sets out a number of ways so as to set up an EU framework that allows data access, for example by providing guidance on facilitating and incentivising the sharing of such data or setting out default contract rules that could act as a benchmark balanced solution for contracts relating to data.

iii) **Liability and safety in the context of emerging technologies**: this is particularly relevant to applications related to the Internet of Things (IoT) (e.g. connected vehicles) and autonomous connected systems more generally, where malfunction or manipulation may cause consumer harm not due to a manufacturing error but for example, due to the transmission of erroneous data. The question arises of how to apply the EU rules on liability (the EU Products Liability Directive) in this context. The Commission is keen to provide legal certainty in this area and identifies several possible ways forward, starting with stakeholder consultations on the adequacy of the current legal regime.

iv) **Portability of non-personal data, interoperability and standards**: while the General Data Protection Regulation provides a data portability right[5], the same is not envisaged for non-personal data. Data portability considerations are closely linked to data interoperability which will allow digital services to communication and exchange data. In the same vein, portability is closely linked with the existence of the appropriate technical standards that will allow portability to be implemented. Like point (iii), the Commission is keen to address these three issues and identifies several possible ways forward, starting with stakeholder consultations.

[5] The right of a data subject to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and transmit those data to another controller without hindrance from the controller to which the personal data have been provided. GDPR, Article 20.

2.3. The 2018 Communication "Towards a common European data space"

In its 2018 Communication[6], the EC introduces the concept of 'data spaces' in the EU, defining it as "*a seamless digital area with the scale that will enable the development of new products and services based on data*". The Commission proposes a package of measures that will set the ground for the creation of data spaces, namely:

i) **A proposal for the review of the Directive on the re-use of public sector information ("PSI Directive"):** public sector bodies produce and collect large quantities of data which constitute valuable raw material for the development of innovative digital services. The review of the PSI Directive aims to ensure that more data will become available and re-usable, for example, by enlarging the scope of the Directive to include valuable data such as those held by public undertakings in the transport sector, and by encouraging the publication of dynamic data and the update of application programming interfaces (APIs).

Further information about the PSI Directive and the review can be found in section 3.4.

ii) **Guidance on sharing private sector data:** The Commission recognises that access to and re-use of private sector data is a cornerstone of a common European data space. The EC distinguishes between two scenarios: a) business-to-business (B2B) data sharing, and b) business-to-government (B2G) data sharing.

Regarding B2B data sharing, the EC sets out key principles that should guide contractual agreements for non-personal machine generated data[7]:

- Transparency on the actors, the types of data and the purposes of using the data;
- Recognition of shared value creation where several parties have contributed to creating the data;
- Respect for the protection of commercial interests and secrets of data holders and data users;
- Ensure that competition is not distorted when exchanging commercially sensitive data;
- Minimise data lock-in, by enabling data portability as much as possible.

[6] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Towards a common European data space', 25 April 2018, COM (2018) 232 final.
[7] *Ibid*, p.10.

Funded by the European Union

Similar principles are set out concerning B2G data sharing[8]:

- Ensuring that the proportionality principle is respected when governments request private sector data (e.g. the request should be adequate and relevant to the intended public interest purpose);
- Purpose limitation ;
- Respect for the protection of trade secrets and other commercially sensitive information;
- Collaboration agreements should be mutually beneficial while acknowledging the public interest goal by giving the public sector body preferential treatment over other customers;
- Companies supplying the data should offer support to help assess the quality of the data for the intended purposes;
- Transparency about the parties to the agreement and their objectives.

Further details are provided in the Commission's "Guidance on sharing private sector data", a document which accompanies the 2018 Communication.[9]

2.4. The 2020 Communication "European strategy for data"

In February 2020, the Commission presented its Communication on a European strategy for data,[10] setting out its vision towards the creation of a single European data space, a single market for data where personal as well as non-personal data are created, processed and shared within the EU, boosting growth and creating value. To this end, the legal framework and governance mechanisms should also ensure availability of data. The Communication states that common European rules and efficient enforcement mechanisms should ensure that:

- Data can flow within the EU and across sectors;
- European rules and values, in particular: personal data protection, consumer protection legislation and competition law, are fully respected;
- The rules for access to and use of data are fair, practical and clear, and there are clear and trustworthy data governance mechanisms in place; there is an open, but assertive approach to international data flows, based on European values.[11]

[8] *Ibid*, p.13-14.
[9] Commission Staff Working Document, 'Guidance on sharing private sector data in the European data economy', *Accompanying the document* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Towards a common European data space', 25 April 2018, COM(2018) 125 final.
[10] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European Strategy for data', 19 February 2020, COM (2020) 66 final.
[11] *Ibid*, p.5.

The actions of the strategy are based on four pillars[12]:

A. **A cross-sectoral governance framework for data access and use**, which includes the following key actions:

- The proposal for a 'legislative framework for the governance of common European data spaces', facilitating the use and voluntary sharing of data while prioritising interoperability requirements and relevant standards;
- The proposal for an implementing 'Act on high-value data-sets' —complementing the Open Data Directive[13] to make high-quality public sector data available for re-use across the EU in machine-readable format;
- The proposal for a 'Data Act' —fostering B2G and B2B data sharing by addressing contractual matters related to the (re)use of co-generated data, and
- An analysis and revision of the existing policy framework through the 'Digital Services Act' package[14], considering systemic issues related to digital platforms and their data monopoly.

B. **Enablers: Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability**, which includes the following key actions:

- Investing in a High Impact project on European data spaces, encompassing data sharing architectures and governance mechanisms, as well the European federation of energy-efficient and trustworthy cloud infrastructures and related services;
- Signing Memoranda of Understanding with Member States on cloud federation;
- Launching a European cloud services marketplace, integrating the full stack of cloud service offering, and
- Creating an EU (self)regulatory cloud rulebook.

C. **Competences: Empowering individuals, investing in skills and in SMEs,** which includes as key action the enhancement of the portability right for individuals, giving them more control over who can access and use machine-generated data.

D. **Common European data spaces in strategic sector and domain of public interest**, including a **Common European mobility data space**, which will facilitate access, pooling and sharing of data from existing and future transport and mobility databases to advance intelligent transport systems, including connected cars and other modes of transport.

In the Appendix to the Communication that analyses the Commission's idea of a mobility data space, the EC recognises that digitalisation and data play an increasing role in supporting transport

[12] *Ibid*, pp. 12-23.
[13] See further below, section 3.4.
[14] See further below, section 3.6.3.

Funded by the European Union

sustainability and points out that several legislative frameworks already contain data-sharing obligations, establishing lists of transport related datasets. The strategy states that wide availability and use of data in public transport systems has the potential to make them more efficient, greener and customer friendly. On smart cities, data use to improve transport systems is also central. To that end, the Commission will put forward a number of actions to update the relevant legislative framework.[15]

[15] Appendix to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European Strategy for data',19 February 2020, COM (2020) 66 final, pp. 28-29.

Funded by the European Union

3. Horizontal legal and regulatory data sharing gap analysis

This section attempts to identify the EU legal frameworks that are relevant to data sharing in the transport sector.[16] It covers general and horizontal legislation (the GDPR, the e-Privacy Directive and forthcoming Regulation, Competition Law, the Open Data and PSI Directive, the Regulation on the free flow of non-personal data, legislation applicable to intermediaries and the proposal for a Data Governance Act) as well as sector-specific rules (the Intelligent Transport Systems Directive). A description is provided for each framework analysing the main concepts, followed by a brief explanation of the practical relevance to MobiDataLab.

3.1. The General Data Protection Regulation

The General Data Protection Regulation (GDPR)[17] adopted in 2016 establishes a detailed and comprehensive data protection system in the EU.[18] The GDPR regulates the territorial, material, and personal scope of the right to personal data protection, directly imposing obligations on private and public parties. It became applicable on the 25th of May 2018 in all EU Member States. The GDPR applies to the "*processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*".[19] The GDPR covers personal data, that is, any data related to an identified or an identifiable natural person. It also provides a stricter regime for data that is listed as "special categories" that may be regarded as "sensitive".[20]

Data sharing activities will inevitably include some sort of processing activity, and to the extent that they contain personal data (see section 3.1.1 for an explanation of the terms), the GDPR will be *prima facie* applicable. However, if data have been anonymised, GDPR is not applicable. But it needs to be ensured that data cannot be returned to a "normal" state (deanonymized) when relying on the

[16] An overview of the Intellectual Property Rights framework will be provided under D2.7 given that it constitutes an essential pillar of data governance, covering a substantive right pertinent to data transactions and taking into account the upcoming review of the Database Directive that is expected under the upcoming Data Act that will also be analysed under D2.7.
[17] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[18] The right to privacy and personal data protection are also protected under the European Convention on Human Rights (ECHR) and the Treaty for the Functioning of the European Union (TFEU), including the European Charter of Fundamental Rights (CFR) – Article 8 ECHR and Articles 7 and 8 CFR.
[19] GDPR, Article 2(1).
[20] GDPR, Article 9.

Funded by the European Union

way that personal details have been obfuscated.[21] This means that the threshold for anonymisation is quite high.

This section will examine the key notions determining the material scope of application of GDPR, the legal bases for processing, the principles of personal data processing and the data subjects' rights. It does not analyse anonymisation and pseudo anonymisation as this constitutes the core of the analysis of another WP2 deliverable, D2.3.

3.1.1. Key notions of the GDPR

3.1.1.1. Personal data

Personal data is broadly defined as any type of information that relates to an identified or identifiable natural person ("data subject").[22] The Court of Justice of the EU ("CJEU") has clarified that personal data is not limited to sensitive or private information, but potentially encompasses all types of information, both subjective and objective provided that it relates to the data subject.[23] The possible extent of "personal data" was clarified by the CJEU in the *Breyer* case, which concerned IP addresses. The CJEU clarified that a piece of information can be considered personal data whenever additional information can be sought from third parties to identify a data subject.[24] The European Convention of Human Rights ("ECHR") has also interpreted the term "personal data" as not being limited to matters of the private sphere of an individual.[25]

The information about a person can be clear, *i.e.*, directly identifying an individual (*e.g.*, name, surname), or it can indirectly allow for the individual to be identified (*e.g.*, by combining information on the specific hour a ticket is validated and footage from surveillance cameras). Personal data is further categorised as *volunteered*, *observed*, and *inferred* data. *Volunteered* (provided) data originate from direct actions of the data subject, in full awareness of the consequences that result with the disclosure of his/her personal data. Examples of volunteered data include data disclosed in the context of a loan application, credit card use or shared (actively) via online social networks.

[21] Andrew Denley, Mark Foulsham, Brian Hitchen GDPR, *How to achieve and maintain compliance* (1rst edn, Routledge 2019) Section 1.
[22] GDPR, Article 4(1).
[23] Case C-434/16, *Peter Nowak v. Data Protection Commissioner* [2017], ECLI:EU:C:2017:994, para. 34.
[24] Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland* [2016], ECLI:EU:C:2016:779. The Court of Justice held that dynamic internet protocol (IP) address may constitute personal data even if a third party (e.g. internet service provider) is in possession of additional data, which would make it possible to identify the individual. The possibility to identify the individual must constitute means reasonably likely to be used to identify the individual, whether directly or indirectly.
[25] *Amann v. Switzerland*, App no. 27798/95 (ECHR 16 February 2000), para.65.

Observed data such as IP addresses, meta-data, device ID, browser information or interaction data is either captured for a purpose as a result of a deliberate measurement or it is simply the *exhaust* data which comes into being as a by-product of ICT systems (e.g., firewalls, load balancers, routers, switches, etc.) deployed for other purposes.

Inferred (a.k.a. *derived*) data is the output of data processing as an aggregate. It is the data/information resulting from a subsequent analysis of the raw data either provided (volunteered) by the data subject or actively observed by the data controller. Inferred data could include user profiles, spending habits, peak hours of a commercial establishment or an assessment of one's physical condition based on the data collected by a smartphone application.[26]

To determine whether a person is identifiable, a controller or another person must consider all reasonable means that are likely to be used directly or indirectly to identify the individual, such as, singling out. To determine whether identification is possible, one should consider all means that are reasonably likely to be used by the data controller (see below on the definition) or another person.[27]

When assessing such means, one should consider all factors at stake, such as the cost of conducting identification, the available technology, the risk of organisational dysfunctions (*e.g.*, breaches of confidentiality duties), technical failures, etc.[28] Moreover, the possibility of identification has to be assessed taking into account technological developments during the period for which the data will be processed, keeping in mind that identification that may not be possible today given the current state of technology, may be possible in the future.[29]

Personal data in smart mobility

The easiness with which one activity can include personal data can be demonstrated in smart mobility systems. One particular privacy concern arising is the capability of these systems to locate and track users.[30] Even if privacy preserving techniques are applied to location data, there is still the risk that users could be identified when mobility information is matched with data from other sources.

For example, the provision of additional non-transport functionalities and services through smart mobility cards may reveal users' social relations and activities. This is the case of travel cards that also provide access to parking areas or grant discounts at public services (museums, concert

[26] For an argument for the inclusion of derived data in the scope of data portability, see Bertin Martens and others, 'Business to Business Data Sharing: An Economic and Legal Analysis' (Digital Economy Working Paper 2020-05, European Commission, Seville, 2020 JRC121336) 4 https://ec.europa.eu/jrc/sites/default/files/jrc121336.pdf, accessed 14 January 2022.
[27] GDPR, recital. 26.
[28] *Ibid*; Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data (01248/07/EN WP 136) p.15 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, accessed 14 January 2022.
[29] *Ibid*
[30] Alessandro Mantelero, 'Data Protection, E-Ticketing, and Intelligent Systems for Public Transport' (2015), International Data Privacy Law, pages 309-320, Available at SSRN: https://ssrn.com/abstract=2659732, accessed 14 January 2022.

Funded by the European Union

halls, etc.) or commercial services. Mobility information may reveal that two different users travelled from their home/office to reach the same place, attended the same play in the same theatre, then made the same journey, and had dinner in the same restaurant, which adopts discount rates for travel cardholders. Social relationships and related interactions can be better monitored when mobility data are coupled with publicly available information (e.g. Twitter postings, blogs entries).[31]

Similar concerns can arise when tourist information is integrated with mobility information. For example, let's imagine a scenario where local authorities that organise tourism in their area (e.g. tourist offices) provide an application that integrates all available mobility services, if possible, in real time, with their data - especially to improve the tourist information they provide (e.g. with car parks, public transport services, tourist buses, and even data from bike sharing companies).[32]

This app may collect information about a user's location, the means of transport he/she has used, the exact sightseeing route he/she has taken, the museums visited and even perhaps the places where he/she had lunch. Even if some of these data are pseudonymised, their collective reading may lead to the user being identifiable.

Arguably, anonymous mobility data can be used to know the frequency of use of specific lines or part of them. But without identified or pseudonymous data, it is not possible to map the flows of passengers through itineraries composed of different lines and these flows represent the most valuable information for mobility planning **[Identified Gap 1]**.[33]

In addition, the use of anonymised data cannot exclude the risk of re-identification, since the power of analytics undermines many strategies based on de-identification.[34]

Personal data in connected vehicles

In its Guidelines on the processing of personal data in the context of connected vehicles and mobility related applications, the European Data Protection Board ("EDPB") notes that connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers.[35]

Even if the data collected by a car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. For example, data

[31] *Ibid*
[32] See MobiDataLab D2.9, Use case for research, 3.3, Transport data sharing within the Linked Open Data vision.
[33] *Mantelero* (n 30).
[34] *Ibid*
[35] EDPB, 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications', 28 January 2020, paras 3, 27-28 https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, accessed 14 January 2022.

Funded by the European Union

relating to the driving style or the distance covered, data relating to the wear and tear on vehicle parts or data collected by cameras may concern behaviour as well as information about other people who could be inside or outside the vehicle. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status.

Geolocation data & connected vehicles

In the same Guidelines mentioned in example 1, the EDPB makes a specific reference to geolocation data as a category that warrants special attention.[36] The EDPB notes that geolocation data are particularly revealing of one's life habits. The journeys carried out are very characteristic and can reveal private details about a person's life (e.g. residence, places of leisure, places of worship etc.). Vehicle and equipment manufacturers need therefore to be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purposes of processing. The EDPB further mentions a number of principles that need to be complied with when collecting geolocation data.

Data revealing criminal offences or other infractions & connected vehicles

The EDPB has also drawn the attention to "offence-related data".[37] For example, the instantaneous speed of a vehicle combined with precise geolocation data or data indicating that the vehicle crossed a white line could be considered offence-related data. Processing of such data can only take place under the control of official authority or when the processing is permitted by EU or national law, providing for appropriate safeguards for the rights and freedoms of data subjects.

3.1.1.2. Processing

Processing of personal data means "any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means".[38] The concept of

[36] *Ibid*, paras 60-61.
[37] *Ibid*, paras 64-65.
[38] GDPR, Article 4(2).

Funded by the European Union

processing activities is very broad. Examples of processing activities include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction of data.[39]

Automated data processing concerns operations performed on "personal data wholly or partly by automated means".[40] Practically, this means that any personal data processing through automated means with the help of, for example, a computer or a mobile device is covered under the GDPR. But processing is not restricted to automation only; processing personal data in a manual filing system, that is, a specially structured paper file also falls within the scope of the Regulation.[41]

3.1.1.3. Data subject

The person whose personal data is protected under the GDPR is a living natural person, which is defined as the data subject. Legal persons do not benefit from protection under the GDPR.[42] The GDPR grants data subjects several rights, i.e., the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and the right not to be subject to a decision based solely on automated processing.[43]

3.1.1.4. Controller

The controller is "any natural or legal person, public authority agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designed by national or Community law".[44] The controller is, essentially, the entity having control over the personal data processed, is responsible for the data processing and for ensuring that such processing – including any processing carried out by a third party (i.e. processor) - complies with the GDPR.

The assessment of controllership should be made based on the facts of a particular case. The key criterion to assess who is a controller is to designate the person who determines the "purposes" (the "why") and the "means" (the "how") of the processing of personal data.[45] It seems however the purpose may take precedence over the means. As such, determining the purpose of the processing,

---

[39] *Ibid*
[40] GDPR, Article 2(1) and 4(2).
[41] European Union Agency for Fundamental Rights (2018), *Handbook on European Data Protection Law*, Publications Office of the European Union, p. 233, pp. 99-100.
[42] There have been however cases where legal entities were able to rely on Article 8 ECHR, if they are directly affected by a measure which breaches their right to respect for their "correspondence" or "home". See Guide to the case-law of the ECtHR, Data protection, 31 December 2020, p. 8.
[43] GDPR, Articles 15 onwards.
[44] GDPR, Article 4 (7).
[45] EDPB, 'Guidelines 7/2020 on the concepts of controller and processor in the GDPR', 2 September 2020, section 2.1.4, p. 13 https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf, accessed 14 January 2022.

in any case, leads to a qualification as a controller. Determining the means would lead to control only when it concerns the essential means, such as which data is processed, the duration of the processing, which third parties have access to the data.[46] The determination of the technical and organisational elements of the means (e.g., which hardware or software to use) does not necessarily imply control and can hence be done exclusively by the processor.[47]

Under the GDPR, both natural, legal persons and a public authority can be considered as a controller. But normally it would be the company or a body that would qualify as a controller, rather than a specific individual within the company or the body.[48]

Joint controllership

When two or more parties jointly determine the purpose and means of processing, they are considered joint controllers.[49] "Jointly" must be interpreted as meaning "together with" or "not alone", in different forms and combinations.[50] Joint controllership exists when the parties decide together to process data for the same or common purpose. Joint controllership also requires that two or more entities have exerted influence over the means of the processing.

Joint participation

Joint participation through a *common decision* means deciding together and involves a common intention following the most common understanding of the term "jointly" referred to in Article 26 of the GDPR.[51] However, joint controllers could also adopt converging decisions. But they would need to complement each other and be necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing, where, for example, processing by each party is inextricably linked.[52]

The CJEU has broadened the scope of joint controllership in several cases. In *Jehovah's Witnesses*, the CJEU even considered that the entire community was considered a controller jointly with its members as the community participated in the determination of the purposes and means by organizing and coordinating the activities of its members, which helped to achieve the objective of the entire community.[53]

The Court also confirmed that the fact that one of the parties does not have access to the personal data processed is not enough to exclude joint controllership. For example, in *Jehovah's Witnesses*, the CJEU considered that it was not necessary that the community had access to the data in

[46] *Ibid*. p.14.
[47] *Ibid*
[48] *Ibid*, section 2.1.1, p.9.
[49] GDPR, Articles 4(7) and 26.
[50] EDPB Guidelines on the concepts of controller and processor (n 45), p. 17.
[51] *Ibid*, para.52.
[52] *Ibid*, para.53.
[53] Case C-25/17, *Jehovan todistajat* [2018], ECLI:EU:C:2018:551, para.71.

Funded by the European Union

question, or to establish that that community had given its members written guidelines or instructions about the data processing.[54] The community participated in the determination of purposes and means and knew on a general level of the fact that such processing was carried out to spread its faith.[55]

Jointly determined purpose

In *Fashion ID*[56] and *Wirtschaftsakademie*[57], the CJEU suggested that even when the entities do not have the same purpose for the processing, they may still be considered joint controllers, if their purposes are closely linked or complementary, for example, when there is a mutual benefit, provided that each of the entities involved participates in the determination of the purposes and means of the relevant processing operation. Yet, the mere existence of a mutual benefit (e.g., commercial) arising from a processing activity does not give rise to joint controllership. If the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity but is merely being paid for the services rendered, it is acting as a processor rather than as a joint controller.[58]

Jointly determined means

For joint controllership to exist, each entity involved does not need to determine all the means in each case. Indeed, as clarified by the CJEU, different entities may be involved at different stages of that processing and to different degrees.[59] It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. This scenario can notably arise in the case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up.[60]

Also, the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing).[61]

Joint controllers must determine and agree on their respective responsibilities on how to comply with the obligations under the GDPR, namely concerning the exercise of data subjects' rights and the duties to provide information (e.g. on the identity and contact details of the controller, the purposes

[54] *Ibid*, para.75.
[55] *Ibid*, para.71.
[56] Case C-40/17, *Fashion ID* [2019], ECLI:EU:C:2019:629.
[57] Case C-210/16, *Wirtschaftsakademie Schleswig-Holstein* [2018], ECLI:EU:C:2018:388.
[58] EDPB Guidelines on the concepts of controller and processor (n 45), para. 60.
[59] *Ibid*, p. 19.
[60] *Ibid*, paras 62-63.
[61] EDPB Guidelines on the concepts of controller and processor (n 45), para. 66.

and the legal basis for processing, any data recipients, etc.[62]).[63] In addition to this, the distribution of responsibilities should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities.[64] In short, they need to decide "who does what". But they have flexibility in distributing and allocating obligations amongst them as long as they ensure full compliance with the GDPR with respect of the given processing.[65]

There is no obligation for the joint controllers to have a written contract, but the EDPB recommends drafting a legally binding document to ensure legal certainty. In any event, the main points ("essence") of the arrangement made on each controller's role and responsibilities needs to be made available to data subjects so that they know which of the controllers is responsible for what.[66] For efficiency purposes, joint controllers can designate in the arrangement a contact point for handling data subjects' requests.[67] But data subjects are not bound by this and remain free to contact either of the joint controllers to exercise their rights under the GDPR.[68]

Finally, each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected.[69]

3.1.1.5. Processor

The processor is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.[70] In principle, there is no limitation as to which type of actor might assume the role of a processor. It might be an organisation, but it might also be an individual. Two characteristics define who can qualify as a processor: i) being a separate entity in relation to the controller, and ii) processing personal data on the controller's behalf.[71]

However, it has been noted that not every service provider that processes personal data while delivering a service is a "processor" within the meaning of the GDPR. The role of a processor is granted not from the mere processing of data but its concrete activities in a specific context. It is the

[62] The information obligations are set out in Articles 13 and 14 of the GDPR.
[63] GDPR, Article 26(1).
[64] EDPB Guidelines on the concepts of controller and processor (n 45), p.4.
[65] *Ibid*, para. 165.
[66] GDPR, Article 26 (2).
[67] GDPR, Article 26 (2); EDPB Guidelines on the concepts of controller and processor (n 45), paras 180-183.
[68] EDPB Guidelines on the concepts of controller and processor (n 45), paras 184-187.
[69] *Ibid*, p.4.
[70] GDPR, Article 4(8).
[71] EDPB Guidelines on the concepts of controller and processor (n 45), section 4, p. 24.

Funded by the European Union

nature of the service that will determine whether the processing activity amounts to the processing of personal data on behalf of the controller within the meaning of the GDPR.[72]

3.1.2. Legal bases for personal data processing

According to the GDPR, personal data can be lawfully processed only based on the following[73]:

i) the consent of the subject;
ii) contractual necessity;
iii) legitimate interests of the data controller or a third party;
iv) compliance of the data controller with a legal obligation;
v) protecting the vital interests of a data subject or another person;
vi) necessity arising out of the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.

Data-driven activities heavily rely on consent to collect and process personal data in a lawful manner.[74] Consent must be "given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data".[75] Usually, this is gathered by a user accepting the service's terms and conditions of the privacy policy.

Consent is not characterised by the person to whom it is provided (the controller) but concerns each act of personal data processing. It must be a) **freely given**, b) **specific**, c) **informed** and an d) **unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered *a genuine choice* with regard to accepting or declining the terms offered or declining them without detriment.

When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.[76] Furthermore, as the requirement of informed consent is to ensure

[72] *Ibid*
[73] GDPR, Article 6.
[74] Eleni Kosta, *Consent in European Data Protection Law* (Martinus NIJHOFF Publishers 2013).
[75] GDPR, Article 4(11).
[76] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679', 4 May 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, accessed 14 January 2022

that data subjects will not be deceived or coerced and thereby wronged, it could facilitate data transactions by contributing to the building of trust between businesses and data subjects.[77]

Before obtaining valid consent, the controller(s) need to define the specific, explicit and legitimate purpose for the intended processing activity.[78] This acts as a safeguard against possible widening or blurring of purposes for which data is processed after a data subject has agreed to the initial collection of the data (so-called "function creep").[79] It is also important that **consent is specific to the purpose of processing**. A controller cannot seek one consent to cover different operations if these operations do not serve the same purpose (see also the principle of purpose limitation under 3.1.3 below in that regard). If a controller wants to use the personal data he has collected and is processing for another purpose, a compatibility assessment needs to be carried out.[80]

Providing information to data subjects before obtaining their consent is essential to enable them to make informed decisions, understand what they are agreeing to and exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.[81] A controller needs to provide to data subjects at least the following information: i) the controller's identity, ii) the purpose of each of the processing operations for which consent is sought, iii) what (type of) data will be collected and used and iv) the existence of the right to withdraw consent.[82]

According to Article 7(3) of the GDPR, the data subject has the right to withdraw his or her consent at any time. The withdrawal must be as easy as providing consent. For example, if consent was provided by clicking "I agree" on the privacy policy of a service, it should be as easy to withdraw consent.

As mentioned above, in case of joint controllership, the data subject can exercise his/her rights against each of the controllers. This right makes consent the "weak spot" of data transactions as they can be prone to invalidation. Withdrawal of consent results in an ex-post invalidation of data processing while keeping processing made prior to withdrawal valid. If there is no other lawful basis justifying the processing of the data, they should also be deleted by the controller.[83] The possibility for the data subject to exercise his/her right to withdrawal creates significant uncertainty for data

[77] Laurens Naudts, 'The Right Not to Be Subject to Automated Decision-Making: The Role of Explicit Consent.' (*CITIP Blog*, 2 August 2016) <https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/> accessed 14 January 2022; Aurelia Tamò-Larrieux , 'Privacy and Data Protection Regulation in Europe' in Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework*, vol 40 (Springer International Publishing 2018).
[78] GDPR, Article 5(1)(b) – "purpose limitation".
[79] EDPB Guidelines on consent (n 76), para. 56.
[80] GDPR, Article 6(4).
[81] EDPB Guidelines on consent (n 76), para. 62.
[82] *Ibid*, paras 64-65.
[83] GDPR, Article 17(1)(b) and (3).

Funded by the European Union

sharing as it may result in the collapse of a chain of data sharing transactions. Similar considerations apply if it is found that consent did not fulfil the conditions analysed above **[Identified Gap 2].**

3.1.3. Principles of personal data processing

Article 5 of the GDPR sets out the principles governing the processing of personal data. These principles are:

a) Data processing must be lawful, fair and transparent (lawfulness, fairness and transparency);
b) Data must be collected for specified, explicit and legitimate purposes and not further processed for purposes other than specified (purpose limitation);
c) Data must be adequate, relevant and limited to what is necessary in relation to the specified purposes for processing (data minimization);
d) Personal data must be "accurate and, where necessary, kept up to date" (accuracy);
e) Personal data must be stored only as long as it is necessary for the purpose of data processing. (storage limitation);
f) The security of personal data must be ensured "against unauthorised or unlawful processing and against accidental loss, destruction or damage" (integrity and confidentiality).

It falls upon the data controller to moreover demonstrate compliance with these principles (accountability).[84]

Purpose limitation (which includes purpose specification) holds a prominent position in data protection. It requires that personal data should be collected for specified, lawful, and legitimate purposes and should not be processed in ways that are incompatible with those purposes.[85] The processing of personal data for undefined and/or unlimited purposes is thus unlawful. The principle prevents the use or disclosure of personal data for purposes other than those that the data controller had originally specified and to which the data subject had consented. Under the principle, the use of

[84] GDPR, Article 5(2).
[85] Article 29 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation', 2 April 2013, p.4, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, accessed 14 January 2022.

a one-time permission for a single instance of data processing cannot be relied upon as a blanket legitimisation for subsequent operations.[86]

Every new purpose for processing data that is not compatible with the original one must have its own particular legal basis and cannot rely on the fact that the data were initially acquired or processed for another legitimate purpose. In turn, legitimate processing is limited to its initially specified purpose and any new purpose of processing will require a separate new legal basis. For example, disclosure of personal data to third parties for a new purpose will have to be carefully considered, as such disclosure will likely need an additional legal basis, distinct from the one for collecting the data.[87]

Purpose limitation may be seen as the kernel of EU data protection, supported and complemented with other data protection principles. That is, to ensure that data collection and analysis rest on clearly defined purposes, the data minimisation principle requires that the amount of personal data collected must be proportionate to what is necessary to achieve the specified purposes. As such, data minimisation builds upon the principles of purpose limitation and proportionality. In addition to Article 5, data protection by design incorporated in Article 25 of the GDPR provides a framework for the technical implementation of data protection principles.

3.1.4. Data subjects' rights

Under the GDPR data subjects are granted certain rights with respect to their personal data. The controller is required to establish mechanisms to facilitate the exercise of such rights. Particularly relevant for a data-driven and automated context is the right not to be subject to an automated decision that has legal effects on the individual or significantly affects him in any other way.[88]

An automated decision is a decision taken without any human intervention exclusively by automated means. It includes profiling, which amounts to the automatic evaluation of personal aspects relating to a natural person, in particular, to predict that person's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements.[89] There are however exceptions to this prohibition if the decision is necessary for entering into or performing a contract between the controller and the data subject, if it is authorized by Union or Member State law which contains appropriate safeguards or if the individual consented to it.

'Profiling' and 'automated decision making' in the transport sector

[86] Tamò-Larrieux (n 77), p. 91. Also see Nadezhda Purtova, Eleni Kosta and Bert-Jaap Koops, 'Laws and Regulations for Digital Health' in Samuel A Fricker, Christoph Thümmler and Anastasius Gavras (eds), *Requirements Engineering for Digital Health* (Springer International Publishing 2015).
[87] Handbook on European Data Protection Law (n 41), p.122.
[88] GDPR, Article 22.
[89] Handbook on European Data Protection Law (n 41), p. 233.

The Article 29 Working Party has provided an example, in the transport sector, to illustrate the difference between 'profiling' and 'automated decision making'[90]:

- Automated decision-making: "*imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision-making process that does not necessarily involve profiling;*"
- Becoming a decision based on profiling: "*if the driving habits of the individual were monitored over time, and, for example, the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations.*"

The GDPR also provides the following rights to the data subject:

- **Right to information:** the individual whose personal data is being processed must be informed about such processing. To this end, GDPR obliges controllers to provide certain information regarding the processing of personal data to the data subject (such as the categories of personal data that are being processed, the purposes of processing, the categories of recipients of these data);[91]
- **Right of access:** individuals have the right to request information about the processing of personal data relating to them, obtain a copy of such data and other supplementary information;[92]
- **Right to rectification:** individuals have the right to have inaccurate, outdated or incomplete personal data about them corrected;[93]
- **Right to erasure:** in certain cases, individuals have the right to have personal data erased ("right to be forgotten");[94]
- **Right to restriction of processing:** in certain cases, individuals have the right to temporarily limit the processing of their data;[95]
- **Right to data portability:** in certain cases, individuals have the right to have their data transmitted directly from a controller to another, if technically possible;
- **Right to object:** in certain cases, individuals have the right to object to the processing of their personal data.

[90] Article 29 Data Protection Working Party Guidelines, 'Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 6 February 2018, p.8 https://ec.europa.eu/newsroom/article29/redirection/document/49826, accessed 14 January 2022.
[91] GDPR, Articles 12 and 13.
[92] GDPR, Article 15.
[93] GDPR, Article 16.
[94] GDPR, Article 17.
[95] GDPR, Article 18.

Funded by the European Union

3.1.5. Short assessment of impact for MobiDataLab

Data sharing activities occurring in the context of transport mobility are likely to include personal data, falling therefore under the scope of the GDPR. Even when some types of data may appear not to be "personal", a careful examination is required as with big data and automated activities such as Artificial Intelligence ("AI"), the distinction between what constitutes personal and non-personal data may not be evident **[Identified Gap 3].** This is accentuated by the wide interpretation given by the ECHR[96] and ECJ (European Court of Justice) [97] of what constitutes "personal data" which does not merely cover aspects of a person's private sphere.

Data categorisation in optimising the transport flow and ETA

Let's assume a scenario where a commercial operator wants to optimise its transport flow by calculating the Estimated Time of Arrival (ETA). This scenario is envisaged in the MobiDataLab deliverable D2.9, Section 2.1, Use case for operations, Optimisation of Transport flow and ETA.

The user is a dispatcher, who plans routes and schedules for several vehicles. Planning tours is supported by dispatcher software, which applies advanced routing and stop sequence optimisation algorithms. Vehicles in turn have telematics devices that can give feedback on their location and progress in their tour, i.e., the information about which customers have been served. This data is continuously compared with the original tour plan and the arrival time at upcoming stops is estimated.

Based on that comparison, several sub-use cases are enabled:

- Alerts for delayed stops to the dispatcher/driver;
- (Semi-)automatic update of the tour plan to meet delivery time windows;
- Sharing the arrival time with customers (planning dock availability etc.);
- Rest time planning of the driver;
- Post-trip reporting and analysis (what causes missed delivery time windows, how narrow can delivery time windows be set, etc.).

Two types of data are required to make the above scenario workable: a) **user-independent data** (real-time traffic data, historic traffic data, weather data) and b) **data on the transport operations of the user** (vehicles location, completed stops, tour plan, driver shift time).

Concerning real-time traffic data, some service providers continuously monitor the location of their users (e.g., via smartphones) and obtain traffic information aggregating the speed, location, and density of their users, and enrich this data with publicly available information, such as static map data. Collecting information directly from users implies the collection of personal data since these data include unique identifiers of individuals and their positions in real-time. A high-level aggregation of these data, such as providing an indicator of road congestion should be enough to

[96] For further information see Guide to the Case-Law of the of the European Court of Human Rights on data protection, 30 April 2021, https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, accessed 14 January 2022.

[97] See section 3.1.1. above.

protect the identities of users. On the other hand, real-time location information from individuals is hard to anonymise with provable guarantees.[98]

Historic traffic data would refer to static datasets compiled from real-time traffic data. These can be collected from road sensors, which would not imply the use of personal data. On the other hand, archived GPS traces from individual users become trajectory microdata. Even if unique identifiers are removed, the location information in trajectory microdata can serve as both quasi-identifiers and sensitive information, which imply a privacy risk to individuals.[99]
Historic aggregated traffic data come in the shape of mobility models. These aggregated data, if detailed enough, could be vulnerable to reconstruction attacks, that is, individual trajectories from users could be recovered from the aggregated information.[100]

Weather data does not seem to include personal data at first sight. However, it is possible to use barometric sensors in personal devices such as smartphones to crowdsource weather information.[101] This approach implies the collection of personal data, including identifiers and location information (along with the sensors readings). More experimental works propose the collection of weather-related information from social media, such as Twitter posts discussing weather conditions.[102] This approach is similar to sentiment analysis and includes identifiers, location information and other data, such as photos. All these constitute personal data.

Vehicles location data is directly sourced from users, via their mobile phones or GPS-enabled vehicles. This information includes personal data since it contains identifiers and real-time location information. This information is mandatory for navigation services. Any secondary uses, such as analysis for mobility patterns, traffic status and prediction, or sharing could pose privacy risks.[103]

Data sharing can take different forms to correspond to diverging legal relationships which may be difficult to recognise and each bringing differing requirements[104]:

[98] See Section 5 of D2.3 for examples of anonymisation techniques that might cover this kind of data.
[99] Privacy risks, such as reidentification attacks from trajectory microdata are described in Section 6 of D2.3, along with anonymisation techniques specific for this kind of data.
[100] These risks are described in Section 7 of D2.3, where we also provide anonymisation techniques to deal with aggregated mobility data.
[101] Larry Dignan, 'IBM aims to use crowdsourced sensor data to improve local weather forecasting globally', ZDNet, 2019. https://www.zdnet.com/article/ibm-aims-to-use-crowdsourced-sensor-data-to-improve-local-weather-forecasting-globally/, accessed 14 January 2022.
[102] Zhu, Yifan, Sifan Zhang, Yinan Li, Hao Lu, Kaize Shi, and Zhendong Niu. "Social weather: A review of crowdsourcing-assisted meteorological knowledge services through social cyberspace." Geoscience Data Journal 7, no. 1 (2020): 61-79.
[103] If data are shared in real time, it should be anonymised following techniques in Section 5 of D2.3 or aggregated and anonymised following techniques in Section 7 of D2.3. Compiled data, corresponding to mobility traces of individual users falls under the category of trajectory microdata, and these should be anonymised following techniques in Section 6 of D2.3 if they are to be shared for secondary purposes.
[104] European Commission Support Centre for Data Sharing, 'Analytical report on EU law applicable to sharing of non-personal data', 24 January 2020, p.14, https://eudatasharing.eu/sites/default/files/2020-02/EN_AR%20on%20EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf, accessed 14 January 2022.

Funded by the European Union

- A controller may “share” data with its service provider, who is bound to the controller by a written agreement. If the service provider acts only on behalf of the controller with the latter entrusting certain contractually defined processing activities to it, this would qualify as a controller - data processor relationship, provided that the processor is selected carefully and that an appropriate written agreement has been implemented (as required under Article 28 of the GDPR);
- A controller may share data with another controller, where that second data controller will use the data for entirely separate purposes and using separate means than the first one. This constitutes a controller to controller relationship. This type of interaction presents a series of unique challenges, notably in ensuring that there is a clear legal basis for the transfer and the further processing and that the further processing is compatible with the initial purposes of processing;
- A more complex case is that of joint controllership where multiple legal entities are jointly responsible for a common (shared) data processing activity as it requires the joint controllers to implement appropriate arrangements - habitually but not necessarily taking the form of contracts –to ensure that the GDPR is complied with.

At the same time, the fact that several actors are involved in the same data processing operations does not mean that they are necessarily acting as joint controllers of such processing. Not all kinds of partnerships, cooperation or collaboration imply qualification as joint controllership as such qualification requires a case-by-case analysis of each processing at stake and the precise role of each entity with respect to each processing.[105]

Given the multitude of actors active in a data-sharing ecosystem in the transport sector (see Figure 1 below), the correct characterisation of each actor’s role under the GDPR can be quite challenging **[Identified Gap n.4].**

[105] EDPB Guidelines on the concepts of controller and processor (n 45), para.67.

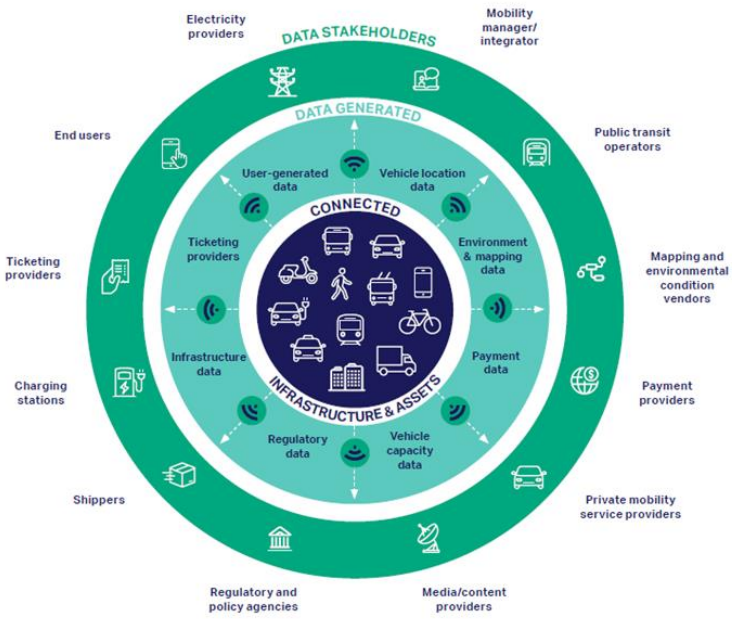

Figure 1: Data stakeholder framework (WBCSD, 2020)

This becomes crucial as otherwise, it is not possible to define the obligations for each actor and comply with the GDPR provisions to ensure lawful data sharing.

The same applies to cloud data-sharing that MobiDataLab seeks to prototype, which adds another layer of complexity as in its simplest form, the setting involves from the one hand, a data provider, from another hand, data users and an intermediary between them. The number and role of intermediaries may differ as well as the *modus operandi* of the cloud (centralised or not). The more decentralised the ecosystem, it is more likely that the chain of legal responsibilities may get blurred.

3.2. The e-Privacy Directive and the upcoming Regulation

The Directive on privacy and electronic communications ("e-Privacy Directive[106]") consists along with the GDPR the two main strands of the personal data protection regime in the EU.

[106] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002, p. 37–47.

The e-Privacy Directive builds on EU telecoms[107] and data protection frameworks to ensure that all communications over public networks (e.g. cellular, satellite) maintain respect for fundamental rights.[108]

According to the Commission, there should be a high level of data protection and of privacy regardless of the technology used.

The general obligations derived from the e-Privacy Directive apply to the processing of personal data with regards to the provision of publicly available electronic communications services in public communications networks in the EU.[109] The e-Privacy Directive aims to "particularise and complement" the provisions of the GDPR, concerning the processing of personal data in the electronic communication sector.[110]

For purposes of its general material scope, the e-Privacy Directive applies when each of the following conditions is met:

- There is an electronic communications service (ECS)[111];
- This service is offered over an electronic communications network[112];
- The service and network are publicly available;
- The service and network are offered in the EU.

The Directive targets the providers of a public communications network or publicly available electronic communications service (i.e. traditional telecom operators)[113] but also all actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the EEA.[114]

The Directive contains high-level provisions requiring such communications to be appropriately secured, and in relation to the confidentiality of electronic communications. In addition, it contains rules relating to location data and other traffic data, restricting the conditions under which such data

[107] https://digital-strategy.ec.europa.eu/en/policies/electronic-communications-laws, accessed 14 January 2022.
[108] https://digital-strategy.ec.europa.eu/en/policies/digital-privacy, accessed 14 January 2022.
[109] e-Privacy Directive, Article 3.
[110] Article 1(1)-(2) of the e-Privacy Directive, to be read in light of article 94(2) GDPR.
[111] An electronic communications service is defined as "*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks",* e-Privacy Directive, Article 2.
[112] 'Electronic communications network' is currently defined by article 2(1) of the Electronic Communications Code.
[113] As defined under the Electronic Communications Code.
[114] EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications (n 35).

Funded by the European Union

can be collected and used.[115] The concept of consent under the e-Privacy Directive is the same as under the GDPR, meaning that it must be freely given, specific, informed, and unambiguous. The user must also receive clear and comprehensive information under the e-Privacy Directive, including about the purposes of processing.

e-Privacy Directive & connected vehicles

The e-Privacy Directive could be relevant for connected vehicles and devices connected to it.[116] That would be the case if they are considered as a "terminal equipment" (just like a computer, a smartphone or a smart TV). A "terminal equipment" is defined as "*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment*".[117] If these criteria are met, and to the extent that the information stored in the end-user's device constitutes personal data, then the subscriber or user concerned needs to be provided with all the relevant information dictated by the GDPR, including about the purposes of the processing, and needs to be offered the right to refuse such processing by the data controller. Prior consent is therefore required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user (Article 5 (3), e-Privacy Directive).[118]

3.2.1. The e-Privacy Regulation

The Commission adopted a proposal for an e-Privacy Regulation in 2017. The rationale was to update the legislation to keep up with the latest technological developments and provide a similar level of protection as the one under the GDPR. The proposal suggests several changes, including[119]:

- **Extension of the scope to other market players**: the new Regulation is intended to apply to new players providing electronic communications services such as WhatsApp, Facebook Messenger and Skype as well as machine-to-machine communication. This will ensure a level playing field by ensuring that these services guarantee the same level of confidentiality of communications as traditional telecoms operators;
- **Communications content and metadata**: privacy is guaranteed for communications content and metadata. Metadata — data that describes other data, such as author, date

[115] European Commission Support Centre for Data Sharing, Analytical report on EU law applicable to sharing of non-personal data (n 104), p.47.
[116] EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications (n 35), p.7.
[117] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version), OJ L 162, 21.6.2008, p. 20–26.
[118] EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications (n 35), paras 14-18.
[119] https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation, accessed 14 January 2022.

created and location — has a high privacy component and should be anonymised or deleted if users did not give their consent unless the data is needed for billing;

- **More effective enforcement**: the enforcement of the confidentiality rules in the Regulation will be the responsibility of data protection authorities, already in charge of the rules under the GDPR.

On 5 January 2021, the Portuguese Presidency released a new draft version of the proposed e-Privacy Regulation. On 10 February 2021, the Member States agreed on a mandate for negotiations with the European Parliament and trilogues began on 20 May 2021.[120]

3.2.2. Short assessment of impact for MobiDataLab

Although the Directive does not directly deal with data sharing, location and traffic data constitute inputs for many mobility services and applications, including some of the activities/use cases considered under MobiDataLab. Traffic data is defined as "*data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*" and location data as "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".*[121]

The Directive imposes strict rules for such data types. Traffic data may only be retained by the provider of a public communications network or publicly available electronic communications service for as long as required to enable the service or billing; thereafter it must be deleted or anonymised. Any other use (notably for added value services) requires the prior informed consent of the users involved, which must be revocable at any time. Location data other than traffic data similarly require either consent or anonymisation.

Collectively, the rules imply that such data cannot be shared with third parties by providers of a public communications network or publicly available electronic communications service, except for third parties that they have authorised to engage in processing activities that the service providers themselves are already permitted to engage in.[122]

If the scope of the Regulation is indeed extended to cover automated machine-to-machine communications, this will cover Internet of Things ("IoT") applications in mobility (e.g. smart cities). It should be noted, however, that the EDPB in its guidelines on connected cars has set out the e-

[120] https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform, accessed 14 January 2022.
[121] e-Privacy Directive, Articles 2(b) and (c).
[122] European Commission Support Centre for Data Sharing, Analytical report on EU law applicable to sharing of non-personal data (n 104), p.48.

Funded by the European Union

Privacy Directive already applied to connected cars by virtue of the connected vehicle and every device connected to it being a "terminal equipment".[123]

In any event, as the Commission has officially expressed its intent to extend the scope and discussions are still ongoing, we will not consider the fact that machine-to-machine communications are not covered under the e-Privacy Directive as a legal gap for the purposes of this report. The same applies to other potentially thorny issues, such as the interface of the e-Privacy Directive and the GDPR[124].

3.3. EU Competition law

As a general proposition, competition law consists of rules that are intended to protect the process of competition to maximise consumer welfare.[125] The CJEU has emphasised in its case law that competition law protects not only the interests of competitors or consumers, but also the market structure, or competition *as such*.[126] Competition law is principally regulated by the Treaty on the Functioning of the EU ("TFEU"), namely Articles 101 and 102. Article 101 TFEU regulates restrictive practices, while Article 102 TFEU deals with abusive conduct. This section will provide the general framework covering these two articles and their link with data and data sharing. One particular case of Article 102 TFEU and data (that is, data access under the essential facilities doctrine) is analysed in section 4 about Mobility-as-a-Service.

As a preliminary remark, it can be argued that competition law can act both as an enabler for data sharing, and it can also raise barriers.

3.3.1. Agreements restrictive of competition (Article 101 TFEU)

Article 101 TFEU provides that "*all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market shall be prohibited as incompatible with the internal market.*

[123] EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications (n 35), p.5.
[124] In March 2019, the EDPB issued Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.
[125] Richard Wish, David Bailey, *Competition Law* (8th edn, Oxford University Press 2015), p.1-2.
[126] E.g. : Case C-209/10, *Post Danmark I* [2012], EU :C :2012 :172, para. 44 ; Case C-23/14, *Post Danmark II* [2015], EU :C :2015 :651, para. 69 ; Case T-213/01, *Österreichische Postsparkasse v Commission* [2006], EU : T :2006 :151, para. 115 ; Case T-286/09, *Intel v Commission* [2014], EU : T :2014 :547, para. 105; Case C-280/08 P, *Deutsche Telekom v Commission* [2010], EU:C:2010:603, para. 182.

In particular, those which:

(a) Directly or indirectly fix purchase or selling prices or any other trading conditions;

(b) Limit or control production, markets, technical development, or investment;

(c) Share markets or sources of supply;

(d) Apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(e) Make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts".

Any agreements or decisions prohibited pursuant to this article will be automatically void (art. 101(2) TFEU). However, under art. 101(3) TFEU, some agreements which may fall within the scope of art. 101(1) may still be compatible with the internal market. This is the case when the following cumulative conditions are met:

- The agreement contributes to improving the production/distribution of goods or to promoting technical/economic progress;
- The agreement benefits consumers ;
- The restriction of competition is indispensable to the achievement of these objectives; and
- The restriction does not prevent competition in respect of a substantial part of the products in question.

Some practices, such as price-fixing and market sharing, are considered so harmful that in practice are never eligible for an exemption under Article 101 (3) TFEU.

3.3.1.1. Data pooling: pro-competitive effects may facilitate data sharing

A data pool is a data-sharing system between companies "which involves an element of reciprocity, whereby at least some companies contribute data".[127]

[127] European Commission, 'Press release: Antitrust: Commission opens investigation into Insurance Ireland data pooling system' (14 May 2019), https://europa.eu/rapid/press-release_IP-19-2509_en.htm, accessed 14 January 2022.

On the one hand, data sharing and pooling[128] may be considered as pro-competitive. The pooling of data of the same type or complementary data resources may enable firms to develop new or better products or services or to train algorithms on a broader, more meaningful basis.[129] In its European Strategy for Data, the Commission announced that it will assess what measures are necessary to establish *data pools* for data analysis and machine learning.[130]

The Commission (through an update of the Horizontal Cooperation Guidelines[131]) is expected to provide further guidance to the stakeholders on the compliance of data sharing and pooling arrangements with EU competition law, while also reviewing individual project-related guidance on the compatibility with EU competition rules if needed. Gaining more clarity on this issue will act as an enabler for data sharing. Given that the revision of the Guidelines has been announced, we will not consider the lack of guidance on data pooling as a legal gap for the purposes of this report.

3.3.1.2. Data pooling: risks of information exchange may restrict data sharing

On the other hand, data sharing and pooling may fall foul of Article 101 TFEU by qualifying as anticompetitive information exchange. That would be the case when market players that are (actual or potential) competitors share competitively sensitive information and this action enables them to become aware of each other's market strategies, or where the conditions of access to and participation in a data pool result in placing certain market operators at a competitive disadvantage.[132]

Information exchange can take place in different contexts:

- Through agreements, decisions by associations of undertakings, or concerted practices under which information is exchanged, where the main economic function lies in the exchange of information itself; or
- Information exchange can be part of another type of horizontal co-operation agreement (for example, the parties to a production agreement share certain information on costs). The

[128] Björn Lundqvist, 'Competition and Data Pools', (2018), 7, Journal of European Consumer and Market Law, Issue 4, pp. 146-154, https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/7.4/EuCML2018031, accessed 14 January 2022.
[129] J. Cremer, Y-A. de Montjoye, H. Schweitzer, 'Competition policy for the digital era', European Commission final report (2019); OECD, "Roundtable on information exchange between competitors under competition law – Note by the Delegation of the European Union", DAF/COMP/WD (2010) 118 (2010).
[130] European Commission, A European strategy for data (n 10), p. 14.
[131] Communication from the Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, OJ C 11, 14.1.2011.
[132] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2509, accessed 14 January 2022.

assessment of the latter type of information exchanges should be carried out in the context of the assessment of the horizontal co-operation agreement itself.[133]

Information exchange can only be addressed under Article 101 if it establishes or is part of an agreement, a concerted practice or a decision by an association of undertakings.[134] Once it has been established that there is an agreement, concerted practice or decision by an association of undertakings, it is necessary to consider the main competition concerns of information exchanges:

(i) Collusion: the exchange of strategic information can facilitate coordination (that is to say, alignment) of companies' competitive behaviour and result in restrictive effects on competition.[135]

(ii) Anticompetitive foreclosure: this for example can occur when the exchange of commercially sensitive information places unaffiliated competitors at a significant competitive disadvantage as compared to the companies affiliated within the exchange system.[136]

As a rule of thumb, information exchange is more likely to be considered anticompetitive when it concerns strategic data (particularly current and future) that reduces the uncertainty of the competitive process.[137] Sharing of strategic data can give rise to restrictive effects on competition because it reduces the parties' decision-making independence by decreasing their incentives to compete.[138] The Guidelines provide examples of strategic information: it can be related to prices (for example, actual prices, discounts, increases, reductions or rebates), customer lists, production costs, quantities, turnovers, sales, capacities, qualities, marketing plans, risks, investments, technologies and R&D programmes and their results. However, these concerns mostly sectors that rely on traditional price competition and may not accurately reflect data-intensive (digital) sectors, where other types of information may equally be considered strategic.

The state of technology may also need to be taken into account, as data pools may not include directly commercially sensitive information, but information shared may concern a large number of customers in a way that it may ultimately enable a member of the pool to extract competitive insights based on data analytics.[139]

Exchanges of genuinely aggregated data, that is to say, where the recognition of individualised company-level information is sufficiently difficult, are much less likely to lead to restrictive effects on

[133] Horizontal Cooperation Guidelines, para. 56.
[134] *Ibid*, para. 60.
[135] *Ibid*, paras 65-68.
[136] *Ibid*, paras 69-71.
[137] *Ibid*, para. 86.
[138] *Ibid*, para. 86.
[139] Van Gorp, N., de Bijl, P., Graef, I., Molnar, G., Peeters, R., & Regeczi, D. (2020). *Exploring data sharing obligations in the technology sector*, p.37 https://www.government.nl/documents/reports/2020/11/30/exploring-data-sharing-obligations-in-the-technology-sector, accessed 14 January 2022.

competition than exchanges of company-level data.[140] Similarly, the exchange of historic data is unlikely to lead to a collusive outcome as it is unlikely to be indicative of the competitors' future conduct or to provide a common understanding on the market.[141] Exchanges of genuinely public information are also unlikely to constitute an infringement of Article 101. Genuinely public information is information that is generally equally accessible (in terms of costs of access) to all competitors and customers.[142]

According to the Horizontal Cooperation Guidelines, information exchange can take various forms: data can be directly shared between competitors or indirectly through a common agency (for example, a trade association) or a third party such as a market research organisation or the companies' suppliers or retailers[143] (so-called "*hub and spoke*" or "ABC" collusion). Particularly relevant for the data economy are the latter given the Commission focus on intermediaries to facilitate data sharing. The case of *Eturas*[144] is very interesting as it concerns collusion via a third party not via human coordination, but rather through automated means. The Lithuanian National Competition Authority fined 30 travel agents and Eturas for their participation in a concerted practice to fix the discounts offered on bookings made through the Eturas systems.[145] Eturas was an online travel booking system used by several travel agents. The administrator of Eturas had sent an email to other travel agents asking for a vote on whether discounts should be reduced (there is only record of one agent having received it).

Following those emails:

- A system notice was sent via the internal Eturas messaging system announcing that based on the declarations, suggestions and wishes of agents, discounts were in principle capped at 3% (*the message was available and could only be consulted in a section of the system called "information messages"; there is only evidence that two agents accessed it; no one replied and no one took public distance from the message either*) and, subsequently;
- A technical restriction was set in the Eturas system (integrated in the websites of the agents) limiting to a maximum 3% the discounts available for online bookings (the technical restriction did not preclude larger individual discounts, but those required additional technical actions).

The Lithuanian National Competition Authority found an infringement as it observed that agents had not publicly distanced themselves from the initiative, could have reasonably assumed that others had received the same message and were likely to abide by it, and it inferred that agents had previously discussed these actions.[146]

[140] Horizontal Cooperation Guidelines (n 131), para. 89.
[141] *Ibid*, para. 90.
[142] *Ibid*, para. 92.
[143] *Ibid*, para. 55.
[144] Case C-74/14, *Eturas and Others* [2016], ECLI:EU:C:2016:42.
[145] Bellamy & Child, *European Union Law of Competition* (8th edn, Oxford University Press 2018), para. 6.032.
[146] https://chillingcompetition.com/2016/01/22/ecjs-judgment-in-case-c-7414-eturas-on-the-scope-of-concerted-practices-and-on-technological-collusion/, accessed 14 January 2022.

The case reached the ECJ, it ruled that a travel agency that understood the measure communicated and did not distance itself from it would be presumed to participate in a cartel unless it could demonstrate that it objected to the communication or systematically set prices disregarding the rule.[147]

In *Asnef-Equifax*[148], a Spanish court asked the ECJ whether a system for the exchange between financial institutions of credit information concerning the identity and economic activity of debtors was compatible with Article 101 TFEU.[149] The objective of the register was to exchange solvency and credit information about customers to evaluate the risks of engaging in lending and credit activities.[150] The Court acknowledged that by reducing the risk of defaults, the information exchange could bring down the overall cost of borrowing, while by reducing the significance of the information held by financial institutions regarding their customers, such registers were, in principle, capable of increasing the mobility of consumers of credit, making it easier for new competitors to enter the market.[151]

The Court argued that the information exchange would in principle not be anticompetitive if the following conditions were met:

a) Supply on the market is not highly concentrated;
b) The system does not allow for the identity of lenders to be revealed, directly or indirectly; and
c) That the conditions of access and use by financial institutions are not discriminatory.[152]

The Horizontal Cooperation Guidelines also recognise that information exchange may lead to efficiency gains.[153] It has been argued that a similar analysis to that applied in *Asnef-Equifax* can be applied to test the compatibility of sharing arrangements of other types of data.[154]

(Alleged) Anticompetitive agreements in the transport sector[155]

On 23 November 2018, the Commission opened a formal investigation to assess whether agreements between booking system providers Amadeus and Sabre on the one hand, and airlines and travel agents on the other, may restrict competition in breach of EU antitrust rules.[156]

[147] https://www.bakermckenzie.com/-/media/files/insight/publications/2017/10/ar_antitrust_digitalage_oct17.pdf, accessed 14 January 2022.
[148] Case C-238/05, *Asnef-Equifax* [2006], ECLI:EU:C:2006:734.
[149] Bellamy & Child (n 145), para. 6042.
[150] Van Gorp, N., de Bijl, P., Graef, I., Molnar, G., Peeters, R., & Regeczi, D. REGECZI (n 139), p.37.
[151] *Bellamy & Child* (n 145), para. 6.032.
[152] *Asnef-Equifax* (n 148), paras 58-61.
[153] Horizontal Cooperation Guidelines (n 131), paras 95-104.
[154] *Van Gorp, N., de Bijl, P., Graef, I., Molnar, G., Peeters, R., & Regeczi, D*. (n 139), p. 37.
[155] Itai Rabinovici, 'The Application of EU Competition Rules in the Transport Sector' (2019), Journal of European Competition Law & Practice, Volume 10, Issue 3, Pages 187–195, https://doi-org.eres.qnl.qa/10.1093/jeclap/lpz011, accessed 14 January 2022, p.187.
[156] https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6538, accessed 14 January 2022.

Amadeus and Sabre are leading worldwide suppliers of Computerised Reservation Systems ('CRS'), also known as Global Distribution Systems ('GDS'). CRS act as technical intermediaries in a market of a two-sided nature, connecting two separate categories of players: airlines and travel agencies (including online agencies). Airlines provide CRS information on their booking inventory and the content (e.g. fares, schedules and availability), while the CRS supply in return booking capabilities and a distribution channel to the travel agents. CRS provide travel agents reservation, booking and ticketing services by means of a comprehensive tool which allows comparison of prices and conditions from hundreds of airlines. CRS provide their customers with immediate information about the availability of air and rail transport services, the fares and schedules for such services. They permit travel agents to make immediate confirmed reservations on behalf of the consumers. When a travel agent books a ticket using a CRS, the airline pays a booking fee to the CRS. The travel agent usually charges a service fee to the consumer for the booking of the ticket. Travel agents pay a subscription fee to the CRS. CRS providers usually offer incentive payments to travel agents for the booking of a ticket (which might go beyond the subscription fee paid by the travel agent).

As these distribution channels might influence the consumer choice, the EU has adopted the Code of Conduct for CRS, Regulation 80/2009, that ensures that air services by all airlines are displayed in a non-discriminatory way on the travel agencies' computer screens, includes safeguards that protect against potential competitive abuses by airlines owning or controlling a CRS (parent carriers) and include rules for the protection of passenger/personal data.

In its antitrust investigation the Commission examined whether certain terms in Amadeus' and Sabre's agreements with airlines and travel agents may restrict their ability to use alternative suppliers of ticket distribution services. This may make it harder for suppliers of new ticket distribution services to enter the market, as well as increase distribution costs for airlines, which are ultimately passed on in the ticket prices paid by consumers.

The Commission ultimately decided to close its investigation as the evidence collected was not sufficiently conclusive to justify pursuing the investigation further.[157] However, the closure of the investigation did not imply that the agreements in question complied with the EU competition rules and the Commission pledged to continue to monitor developments in the airline ticket distribution sector.

3.3.1.3. Short assessment of impact for MobiDataLab

Article 101 TFEU is relevant to any party (data provider, data consumer or data sharing platform itself), to an agreement, decisions or concerted practices concerning data sharing. Data sharing agreements may be found anti-competitive, and therefore contrary to Article 101 where companies in the data economy share data on terms that exclude fair competition, are discriminatory or make

[157] https://ec.europa.eu/commission/presscorner/detail/en/mex_21_3785, accessed 14 January 2022.

market entry for third parties prohibitively impractical[158], as long as they affect trade between Member States. As a consequence, when defining terms under which data is shared, a party to the agreement must ensure that it does not infringe Article 101 TFEU.

Data pooling is increasingly becoming an area of interest for the EU antitrust authority, witnessed both by the intention to update the Horizontal Guidelines in that respect, but also by recent antitrust enforcement. In 18 June 2021, the Commission sent a Statement of Objections to Insurance Ireland, an association of domestic insurers, accusing it of restricting competition on the auto insurance market. The Commission takes issue with certain conditions of access to the Insurance Link platform, a data-sharing system, which Insurance Ireland administers. The Commission considers that Insurance Ireland arbitrarily delayed or de facto denied access to the system to companies that had a legitimate interest in joining it, and that hurdles remain in place that might affect companies seeking to enter the Irish motor insurance market (anticompetitive foreclosure).[159] Executive Vice-President Margrethe Vestager, in charge of digital & competition policy noted that "[*n]on-discriminatory access to data sharing systems is important to foster competition in markets relying on data".*

3.3.2. Abusive conduct (Article 102 TFEU)

Article 102 TFEU deals with unilateral conduct of a firm that holds a dominant position and acts in a manner that abuses that position. It provides that: "*Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.*

Such abuse may, in particular, consist in:

(a) Directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;

(b) Limiting production, markets or technical development to the prejudice of consumers;

(c) Applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(d) Making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts".

[158] European Commission Support Centre for Data Sharing, Analytical report on EU law applicable to sharing of non-personal data (n 104), 17.

[159] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3081, accessed 14 January 2022.

3.3.2.1. The concept of dominance in a delineated product and geographic market

Article 102 applies only where one undertaking has a "dominant position", or where two or more undertakings are "collectively dominant".[160] According to the ECJ in *United Brands*, a dominant position is "*a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained on the relevant market by affording it the power to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers*".[161]

Before assessing dominance, the relevant product market and the geographic market need to be defined[162]**:**

- **Product market**: the relevant product market is made of all products/services which the consumer considers to be a substitute for each other due to their characteristics, their prices and their intended use.
- **Geographic market**: the relevant geographic market is an area in which the conditions of competition for a given product are homogenous.

The Court has found in *AKZO v Commission* that an undertaking with a market share of 50% or more will be presumed dominant.[163] In its Guidance on Article 102 Enforcement Priorities, the Commission says that dominance is not likely if the undertaking's market share is below 40% in the relevant market.[164] However, it does not exclude the possibility of cases with that figure, so we cannot argue that a safe harbour exists.[165] In the Guidance, the Commission also notes that market shares provide a useful first indication of the market structure and of the relative importance of the various undertakings active on the market, but the Commission will interpret market shares in the light of the relevant market conditions, and in particular of the dynamics of the market and of the extent to which products are differentiated.[166]

The Commission also takes other factors into account in its assessment of dominance, including the ease with which other companies can enter the market - whether there are any barriers to this; the existence of countervailing buyer power; the overall size and strength of the company and its

[160] *Whish, Bailey* (n 125), p.190.
[161] Case C-27/76, *United Brands v Commission* [1978], ECLI:EU:C:1978:22, para. 65.
[162] https://ec.europa.eu/competition-policy/system/files/2021-05/antitrust_procedures_102_en.pdf, accessed 14 January 2022.
[163] Case C-62/86, *AKZO v Commission* [1991], ECLI:EU:C:1991:286, para. 60.
[164] Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, OJ C 45, 24.2.2009, para.14.
[165] *Whish, Bailey* (n 125), p.194.
[166] Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (n 164), para. 13.

Funded by the European Union

resources and the extent to which it is present at several levels of the supply chain (vertical integration).[167]

Holding a dominant position as such is not illegal. But undertakings that are in a position of dominance on a specific market bear a special responsibility not to distort competition on such market.[168] Moreover, it is also considered that dominant platforms with regulatory powers have a responsibility to use that power in a pro-competitive manner.[169]

3.3.2.2. Market definition & dominance in data

Looking at data, in particular, so far, the Commission has not yet had to define a market for personal data or for any of its particular usages.[170] In its *Facebook/WhatsApp* merger decision, the Commission explicitly stated that it had not investigated any possible market definition concerning the provision of data or data analytics services, since neither of the parties involved was active in any such potential markets.[171] Under current competition law standards, a correct market definition requires the existence of supply and demand for the product or service.[172] Since all online platforms that have been under scrutiny by the Commission do not trade data, a relevant market was not possibly identified. The Commission delineated the relevant market for online platforms around the services or functionalities offered (e.g. web search, online search advertising intermediation[173]). But once data are established as a tradeable good, which the Commission pursues through the creation of an "internal market for data", a 'real' data market may arise.

The question is how the existence of a dominant position in a market for data can be measured and in particular how value can be attributed to data **[Identified Gap 5]**.[174] The amount or quality of data that an undertaking controls do not seem to constitute adequate indicators for market power because the datasets of different providers cannot be easily compared in this regard. It may be hard, if not impossible, to distinguish different pieces of information and assign value to each of them individually. A more objective way to measure the competitive strength of providers active in a market for data would be to look at their ability to monetise the collected information. The revenue gained by a provider through licensing of data to third parties, delivering targeted advertising services or

[167] https://ec.europa.eu/competition-policy/system/files/2021-05/antitrust_procedures_102_en.pdf.
[168] Case C-322/81, *Michelin v Commission* [1983], ECLI :EU :C:1983:313.
[169] *J. Cremer, Y-A. de Montjoye, H. Schweitzer* (n 129), p. 16.
[170] Graef, Inge, 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015), World Competition: Law and Economics Review, Vol. 38, No. 4 (2015), p. 489., Available at SSRN: <https://ssrn.com/abstract=2657732> or <http://dx.doi.org/10.2139/ssrn.2657732>, accessed 14 January 2022.
[171] European Commission Case No COMP/M.7217 – Facebook/WhatsApp, para. 72.
[172] Commission Notice on the definition of relevant market for the purposes of Community competition law, 97/C 372 /03, paras 13-23.
[173] https://ec.europa.eu/commission/presscorner/detail/en/IP_13_371, accessed 14 January 2022.
[174] *Graef* (n 170), pp.501-502.

offering other paid products and services to customers having data as input indicates how successful it is in the market.[175]

GRAEF provides the following non-exhaustive conditions which may point towards a potential market power in a data-related market: "(1) data is a significant input into the end products or services delivered on online platforms; (2) the incumbent relies on contracts or on intellectual property and trade secret law to protect its dataset as a result of which competitors cannot freely access the necessary data; (3) there are few or no actual substitutes readily available on the market for the specific information needed to compete on equal footing with an incumbent; (4) it is not viable for a potential competitor to collect data itself to develop a new dataset with a comparable scope to that of the incumbent (for example due to network effects or economies of scale and scope)".[176]

3.3.2.3. Abuse of dominance

Article 102 TFEU contains a non-exhaustive list of all the practices that can amount to an abuse. The CJEU case law has not provided a standard definition of what is meant by abuse.[177] In *Hoffman-La Roche*, the ECJ gave the contours of what abuse is: "*The concept of abuse is an objective concept relating to the behaviour of an undertaking in a dominant position which is such as to influence the structure of a market where, as a result of the very presence of the undertaking in question, the degree of competition is weakened and which, through recourse to methods different from those which condition normal competition in products or services on the basis of the transactions of commercial operators, has the effect of hindering the maintenance of the degree of competition still existing in the market or the growth of that competition".*[178]

In order to determine whether the undertaking in a dominant position has abused such a position, it is necessary to consider all the circumstances and to investigate whether the practice tends, for example, to bar competitors from access to the market, to apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage, or to strengthen the dominant position by distorting competition.[179]

Article 102 TFEU prohibits not only practices by an undertaking in a dominant position that tend to strengthen that position, but also the conduct of an undertaking with a dominant position in a given market that tends to extend that position to a neighbouring but separate market by distorting competition. Therefore, the fact that a dominant undertaking's abusive conduct has adverse effects on a market distinct from the dominated one does not preclude the application of Article 102. The dominance, the abuse and the effects of the abuse do not need to be all in the same market.[180]

---

[175] *Ibid*
[176] *Ibid*, pp.504.
[177] *Whish, Bailey* (n 125), p.208.
[178] Case 85/76, *Hoffmann-La Roche v Commission* [1979], ECLI :EU :C:1979:36**,** para. 91.
[179] Case C-280/08 P, *Deutsche Telekom v Commission* [2010], EU:C:2010:603, paragraph 175 and case-law cited there.
[180] European Commission Case AT.39470, *Google Search (Shopping),* para.334.

In general, there can be different categories of abusive conduct. The most typical classification is by reference to its effects on others:

- **Exclusionary abuse:** conduct that is likely to lead to the anti-competitive foreclosure effect of eliminating, weakening or marginalising effective competition on the relevant market (by forcing out or marginalising existing competitors and/or raising barriers to entry for potential competitors);
- **Exploitative abuse:** conduct that is unfair or unreasonable towards those persons who depend on the dominant firm for the supply of goods or services on the relevant market.[181]

However, it should be kept in mind that the distinction is not absolute and some conduct may fall under both categories (e.g. refusal to supply).

In practice, competition authorities will seek to identify a credible "theory of harm" that explains how the conduct alleged to be abusive has or is likely to have, adverse effects on competition.[182] A theory of harm is an economic narrative that enables a competition authority or a court to apply economic principles to the facts of a case.[183] This will be facts-specific.

3.3.2.4. The interface of competition law & data protection

It is worth mentioning the 2019 investigation and ruling of the German Federal Cartel Office ("FCO") against Facebook as it demonstrates the increased focus of competition authorities on data protection, which may have an impact on data sharing practices in the EU. In 2019, the FCO accused Facebook of having abused its dominant position in the market for social networks by collecting and processing data of Facebook users when visiting other websites outside of Facebook that were then connected to its users.

In its Terms & Conditions (T&Cs), Facebook said that private use of the network is subject to Facebook being able to collect an almost unlimited amount of any type of user data from third party sources, allocate these to the users' Facebook accounts and use them for numerous data processing processes. Third-party sources are Facebook-owned services such as Instagram or WhatsApp, but also third-party websites which include interfaces such as the "Like" or "Share" buttons.[184]

The FCO found that Facebook's terms of service and the manner and extent to which it collects and uses data are in violation of the GDPR and also constitute an exploitative abuse. The FCO held that when access to the personal data of users is essential for the market position of a company, the question of how a company handles users' personal data is not only relevant for data protection

[181] *Bellamy & Child* (n 145), para.10.072.
[182] *Ibid*, para 10.059.
[183] *Ibid*, para 10.059.
[184] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html, accessed 14 January 2022.

authorities, but also for competition authorities.[185] While there were judgments by the German courts disputing FCO's rationale[186], it cannot be overlooked that this was the first case where non-compliance with the GDPR was considered a competition law violation. However, it should be noted that the FCO relied on a specific national provision, which is not clear if it is possible to replicate at the EU level. We expect to get more clarity on the interplay between competition law and data protection as the Higher Regional Court of Düsseldorf filed a request for preliminary ruling to the ECJ seeking guidance on specific questions around this issue.[187]

3.3.2.5. Short assessment of impact for MobiDataLab

Article 102 TFEU can be relevant to data sharing practices. Potential abusive practices may take the form of a refusal to share, abusive discrimination and exploitation by unlawful processing or unfair terms. One could consider the situation where company A (e.g. a MaaS service provider) would like to access and use particular data held by company B (e.g. related to bike sharing). Normally, company A would approach company B to enter into a data-sharing agreement.

However, company B holding the commercially important information may not be interested in granting the other company access to the information (e.g. because the two companies are competitors).[188] This scenario could equally apply to cloud service providers (similar to the MobiDataLab prototype) that have gathered a significant amount of valuable data and refuse to grant access to those to interested third parties.

This becomes problematic if the company holding the information enjoys a dominant position under Article 102 and abuses its position to refuse the other company access to data and the market by allowing data sharing only under unequal or discriminatory terms. However, as discussed above, how dominance will be defined in such a situation remains still an open question (starting with the definition of the relevant market) **[Identified Gap 5].** But in those cases, the dominant company could be forced by competition authorities, if certain conditions are met, to provide access to data under its "essential facilities" doctrine. This is further analysed in section 4 of this report.

3.4. Open Data and Public Sector Information Directive

[185] European Commission Support Centre for Data Sharing, Analytical report on EU law applicable to sharing of non-personal data (n 104), p.20.
[186] Further information can be found here: http://competitionlawblog.kluwercompetitionlaw.com/2021/02/11/the-german-facebook-antitrust-case-a-legal-opera/, accessed 14 January 2022.
[187] Case C-252/21, *Facebook and Others,* Request for a preliminary ruling: https://curia.europa.eu/juris/document/document.jsf?text=&docid=244555&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=34462811, accessed 14 January 2022.
[188] European Commission Support Centre for Data Sharing, Analytical report on EU law applicable to sharing of non-personal data (n 104), p.17.

Funded by the European Union

In June 2019, the EU institutions adopted the Open Data and Public Sector Information Directive[189] ("Open Data Directive"), which replaced the 2003 Directive on the re-use of public-sector information ("PSI Directive"), as amended in 2013.[190] EU countries had to transpose the Open Data Directive by 16 July 2021.

3.4.1. Overview of the first PSI Directives

The PSI Directive provided a regulatory framework for the re-use of public sector information, including the minimum rules for public authorities to make their data available for commercial or non-commercial purposes.[191] The rationale behind the adoption of the Directive was to harmonise the basic re-use conditions across the EU and to remove major barriers to re-use in the internal market, thus ensuring a competitive environment conducive to the development of a market for information-based products and services. The Directive introduced provisions on non-discrimination, charging for re-use, exclusive arrangements, transparency, licensing and practical tools facilitating the re-use of public sector documents.[192] It is important to note that the Directive did not oblige the Member States to allow the re-use of documents but it had the merit to lay down concrete modalities surrounding their re-use.

The Directive was revised in 2013. The modifications introduced an obligation to allow the re-use of public sector information (thereby departing from the optional character of the 2003 Directive), access to which is granted under national legislation, expanded the scope of the Directive to include documents from public libraries, museums and archives, established a default charging rule limited to the marginal cost for reproduction, provision and dissemination of the information, and obliged public sector bodies ("PSBs") to be more transparent about the charging rules and conditions they apply.[193]

3.4.2. The Open Data Directive

Similarly to the 2013 Directive, it lays down an obligation for Member States to make all existing documents reusable[194] unless access is restricted or excluded under national rules on access to

[189] 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, 26.6.2019, p. 56–83.
[190] Directive 2003/98/EC as amended by Directive 2013/37/EU.
[191] PSI Directive, Article 3 (2).
[192] European Commission, Commission Staff Working Document, Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information, COM (2018) 234 final, SWD (2018) 128 final, p.4.
[193] *Ibid*
[194] "Re-use" means the use by persons or legal entities of documents held by (a) public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced, except for the exchange of documents between public sector bodies purely in

documents or subject to other exceptions laid down in the Directive, for example, security-sensitive information, commercially confidential information or information protected by intellectual property rights of third parties.[195]

It applies to documents held by PSBs (and public undertakings as explained further below). For PSBs, it applies to documents the supply of which forms part of the *public tasks* of the PSBs concerned, as defined by law or by other binding rules in the Member States. In the absence of such rules, the public tasks should be defined under common administrative practice in the Member States, provided that the scope of the public tasks is transparent and subject to review. The public tasks could be defined generally or on a case-by-case basis for individual PSBs.[196] It also applies to documents that are made accessible for re-use when PSBs license, sell, disseminate, exchange or provide information.[197]

The term "document" covers any representation of acts, facts or information — and any compilation of such acts, facts or information — whatever its medium (paper, or electronic form or as a sound, visual or audio-visual recording).[198] As provided in the PSI Directive, documents (and their metadata) should be in an open format, that can be machine-readable, ensuring interoperability, re-use and accessibility, while complying, where possible, with formal open standards.[199]

The main changes brought by the Open Data Directive are the following:

i) **Extending the application to public undertakings**: originally the PSI Directive applied to PSBs (see table [1] below for further details). The inclusion of "public undertakings" in the scope of the Directive is meant to capture undertakings in the utility sectors (including transport). The Commission argued that data generated by these sectors have tremendous re-use potential (e.g. in Spain, of all the applications with a business model behind, 47% are created with transport data) but was not capitalised as the entities active in these sectors were not covered by the PSI Directive.[200] For example, in some Member States only 3.9% of all the open data published is from the transport area.[201]

   Also, equal treatment needed to be ensured between PSBs and public undertakings, as entities in the utilities sector performed "public sector tasks", i.e. have organisational or management

pursuit of their public tasks; or (b) public undertakings, for commercial or non-commercial purposes other than for the initial purpose of providing services in the general interest for which the documents were produced, except for the exchange of documents between public undertakings and public sector bodies purely in pursuit of the public tasks of public sector bodies. Open Data Directive, Article 2(11).

[195] Open Data Directive, recital 23, Article 1(2) and Article 3(1).

[196] Open Data Directive, recital 21.

[197] Open Data Directive, recital 22.

[198] Open Data Directive, recital 30.

[199] Open Data Directive, recital 31 and Article 5 (1).

[200] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.13.

[201] *Open data re-use: an opportunity for Spain?* COTEC report, 2017.

links to the public sector, or those that lack such links may benefit from public funding (public undertakings). In some cases, public sector tasks are also performed by private entities which act based on special or exclusive rights or concessions from PSBs.[202]

Once the public undertakings make such data available, they will have to comply with the principles of transparency, non-discrimination and non-exclusivity set out in the Directive and ensure the use of appropriate data formats and dissemination methods. They will still be able to set reasonable charges to recover the costs of producing the data and of making it available for re-use.[203]

An overview of the personal scope of application of the Open Data Directive along with the respective definitions is provided in the following table:

Public sector bodies (PSBs)	The State		
	Regional or local authorities		
	Bodies governed by public law	i) Established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; AND	
		ii) Have legal personality; AND	
		iii) Financed for the most part by the State, or regional or local authorities, or other bodies governed by public law OR Subject to management supervision by bodies governed by public law; OR Have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law	
	Associations formed by one or several regional or local authorities		
	Associations formed by one or several bodies governed by public law		
Public undertakings	Undertakings active in the water, energy, transport and postal services sectors	Over which the PSBs may exercise directly or indirectly a dominant influence by virtue of	A dominant influence from the PSBs will be presumed if any of the below apply:

[202] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.13.
[203] https://digital-strategy.ec.europa.eu/en/policies/psi-open-data, accessed 14 January 2022.

	Undertakings acting as "public service operators" for rail and road services, i.e. any public or private undertaking or group of such undertakings which operates public passenger transport services by rail and by road or any public body which provides public passenger transport services by rail and by road	their ownership of it, OR their financial participation therein, OR the rules which govern it	i) The PSBs hold **most of the** undertaking's subscribed capital; OR ii) Control **most of** the votes attaching to shares issued by the undertaking; iii) Can appoint more than half of the undertaking's administrative, management or supervisory body
	Undertakings acting as air carriers fulfilling public service obligations[204] under Article 16 of Regulation 1008/2008		
	Undertakings acting as Community shipowners fulfilling public service obligations under Article 4 of Regulation 3577/92		

Table 1: Personal scope of application of the Open Data Directive

However, the Directive does not contain a general obligation to allow the re-use of documents produced by public undertakings. The decision whether or not to authorise re-use should remain with the public undertaking concerned, except where otherwise required by the Directive or by EU or national law (e.g. the Intelligent Transport Systems Directive, see further below under section 3.8).

In the Impact Assessment accompanying the Open Data proposal, the Commission suggested that giving the freedom to public undertakings on whether they want to open up their data or not, would minimise the effect of imbalance (in terms of openness requirements) between the private companies and public undertakings in transport and utility domains active in the same markets.[205] It could be perceived to harm innovation, investment in sensors and data collection by entities active in those domains, out of fear of strengthening competitors who would not be subject to such an obligation. Critical infrastructure concerns have also been raised. These reasons have often been brought as an argument against a strong horizontal intervention at the EU level in this area.[206]

[204] A public service obligation usually refers to a requirement defined or determined by a competent authority in order to ensure public passenger transport services in the general interest that an operator, if it were considering its own commercial interests, would not assume or would not assume to the same extent or under the same conditions without reward.

[205] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.39.

[206] *Ibid*, Annex 2.

Only after the public undertaking has made a document available for re-use, should it observe the relevant obligations laid down in the Open Data Directive, in particular as regards format, charging, transparency, licences, non-discrimination and prohibition of exclusive arrangements. Public undertakings are also not covered by the requirements applicable to the processing of requests for the re-use of their data.[207]

The Directive encourages Member States to go beyond the minimum requirements set out therein by applying its requirements to documents held by public undertakings.[208] Interestingly, it gives room to Member States to also apply its requirements to private undertakings, in particular those that provide services of general interest.[209]

ii) **Encouraging the dissemination of dynamic data via application programming interfaces (APIs):** The Commission recognises that dynamic data is one of the most commercially valuable types of data, as it can be used for products and services that provide information in real-time, such as travel or transport apps. However, the provision of real-time access to dynamic data held by PSBs through APIs is rare.[210] Dynamic data are defined 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*".[211]

Apart from the fact that public data is not systematically provided through APIs, there are considerable differences between Member States in this area. This is for example clear in the way in which their national portals can be accessed. Austria tops the list, with 71-85% of all visits to its portal deriving from machine traffic. Romania comes second, with 41-55% of its traffic coming via API calls, followed by the UK with 26-40% of visits. 22 out of 28 Member States had API traffic of less than 10%. The figures are encouraging in the sense that the costliest investments on the national level have already been made. Yet, it can be safely assumed that on the lower levels of government, the provision of APIs and their actual usage are less widespread, despite clear benefits: cities produce data in many forms and from many sources, and the wide variety of formats makes it difficult to scale open data applications from city to city.[212]

The Open Data Directive provides that "*Dynamic data should be made available immediately after collection, or in the case of a manual update immediately after the modification of the dataset, via an application programming interface (API) so as to facilitate the development of internet, mobile and cloud applications based on such data. Where this is not possible due to technical or financial*

[207] Open Data Directive, recital 26.
[208] Open Data Directive, recital 19.
[209] Open Data Directive, recital 19.
[210] In a recent study based on a representative sample of the total volume of public sector information (20,000 datasets), it was found that while the majority of services generated from open data are based on real-time data (66%), less than 1% of the data published in open portals are updated in real time. Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.10.
[211] Open Data Directive, Article 2(8).
[212] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.10.

constraints, public sector bodies should make the documents available in a timeframe that allows their full economic potential to be exploited".

Recital 32 of the Directive notes that this consists of a "soft" obligation as "*it would be useful to ensure access to dynamic data through well-designed APIs*". At the same time, in the same recital, both PSBs and public undertakings are requested to make dynamic data available immediately after collection via APIs.

As an exception to the above "soft" provisions, the Open Data Directive imposes a hard obligation to make "**high-value datasets**" for re-use free of charge in machine-readable formats and via APIs and, where relevant, as a bulk download.[213] High-value datasets are defined as "*documents the re-use 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*".[214]

The thematic scope of high-value datasets is provided in Annex I to the Directive and consists of the following datasets:

1. Geospatial
2. Earth observation and environment
3. Meteorological
4. Statistics
5. Companies and company ownership
6. Mobility

The Commission has announced that it will adopt a list of specific high-value datasets by way of an implementing act, which may also specify the arrangements for the publication and re-use. To that end, Deloitte has conducted an impact assessment study on the list of High-Value Datasets to be made available by the Member States under the Open Data Directive.[215]

iii) **Charging rules**: The Commission realised that several PSBs continued to charge well above what is needed to cover reproduction and dissemination costs for the re-use of public sector data. It argued that such charges constitute a market barrier for SMEs and that getting rid of charges typically results in a surge in demand for public sector data, which translates into more innovation, more business growth and, ultimately, higher budget revenues (via taxes) for the public sector.[216]

Pricing variations across the EU for re-use of data

[213] Open Data Directive, recitals 66-69, Articles 5(8), 13 and 14.
[214] Open Data Directive, Article 2(10).
[215] Deloitte, 'Impact Assessment study on the list of High Value Datasets to be made available by the Member States under the Open Data Directive', 2020, <https://www.access-info.org/wp-content/uploads/Deloitte-Study-2020.pdf> accessed 14 January 2022.
[216] https://digital-strategy.ec.europa.eu/en/policies/psi-open-data.

A Swedish company Seapilot produces digital navigation apps based on marine chart data from hydrographic offices across the EU. However, widely divergent pricing models (e.g. one-off payment, royalties, fees linked to updates) and the resulting charges applied (EUR 2,745 in France to EUR 18,900 in Italy) make it increasingly difficult to compete on a global scale, especially given that equivalent US data is free of charge.[217]

The Open Data Directive stipulates that documents should in principle be made available free of charge. But where charges are necessary, they should be limited to the marginal costs.[218] This rule however does not apply to public undertakings.[219] The Directive also provides specific exceptions allowing public bodies to charge for the re-use of their data more than the marginal costs of dissemination.[220] As mentioned above, high-value datasets must be free of charge.

iv) **Non-exclusivity & transparency**: The Directive has reinforced transparency requirements for public-private agreements involving public sector information. Arrangements between data holders and data re-users which do not expressly grant exclusive rights, but which can reasonably be expected to restrict the availability of documents for re-use will be subject to additional public scrutiny. The essential aspects of such arrangements should therefore be published online at least two months before coming into effect, namely two months before the agreed date on which the performance of the obligations of the parties is set to begin. The publication should allow interested parties to request the re-use of the documents covered by those arrangements and prevent the risk of restricting the range of potential re-users.[221]

The rationale of this provision is to minimise the risk of excessive first-mover advantage (benefiting large companies) that could limit the number of potential re-users of the data and create a lock-in of public sector data.[222]

3.4.2.1. The interface with the GDPR

The Open Data Directive must be applied in full compliance with the data protection legislation. The Directive provides that "*it does not affect the protection of individuals with regard to the processing of personal data under Union and national law, particularly Regulation [the GDPR]. This means, inter alia, that the re-use of personal data is permissible only if the principle of purpose limitation as set out in point (b) of Article 5(1) and Article 6 of [the GDPR] is met. [..] Rendering information*

[217] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.12.
[218] Open Data Directive, recital 36 and Article 6.
[219] Open Data Directive, Article 6(2)(c).
[220] When public sector bodies are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks; Open Data Directive, Article 6(2)(a).
[221] Open Data Directive, recital 50.
[222] Open Data Directive, recital 51.

Funded by the European Union

anonymous is a means of reconciling the interests in making public sector information as re-usable as possible with the obligations under data protection law, but it comes at a cost. It is appropriate to consider that cost to be one of the cost items to be considered to be part of the marginal cost of dissemination as referred to in this Directive".[223]

Recital 154 of the GDPR also states that the PSI Directive "*leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in [the GDPR]*".

The Article 29 Working Party on Open Data and Public Sector Information Re-use[224] stated in its opinion: "*wherever personal data are involved, data protection law must help guide the selection process of what personal data can or cannot be made available for re-use and what measures to take to safeguard personal data*". Any processing of personal data needs to be based on one of the legal grounds prescribed in the GDPR.

While the principle of precedence of data protection (which rules over the Open Data Directive) is undisputed and well understood, PSBs and public undertakings (if they choose to open up their data) may encounter practical implementation questions on how to facilitate re-use while ensuring compliance with the GDPR in case of certain public registers that also contain personal data (e.g. car registration databases or ticket data). This most often concerns the suitability of the techniques that can be used for anonymisation or ways by which purpose limitation and other personal data protection principles can be ensured **[Identified Gap 6].**[225]

A 2018 Deloitte study to support the review of the PSI Directive[226] confirms the above. It notes that stakeholders have already emphasised the need to receive more guidance on the protection of personal data under PSI (e.g. in terms of limits to anonymisation, opportunity to carry out data protection impact assessments) and they also advocated for an update of the Article 29 Opinion. Stakeholders expect more to be done in this area and especially in terms of implementation of technical (e.g. anonymisation, pseudonymisation) and legal solutions (such as consent oriented or privacy by design rules) but also in terms of development of training for public officials and the procedures for organisations to safeguard data protection. Moreover, the potential fines in the GDPR (up to 20 million EUR or 4% of annual worldwide turnover in extreme cases) could create a significant

[223] Open Data Directive, recital 52.
[224] Article 29 Data Protection Working Party, 'Opinion 06/2013 on open data and public sector information ('PSI') re-use', 5 June 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf accessed 14 January 2022.
[225] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.4.
[226] Deloitte, 'Study to support the review of Directive 2003/98/EC on the re-use of public sector information', published 24 April 2018, p.47 https://op.europa.eu/en/publication-detail/-/publication/45328d2e-4834-11e8-be1d-01aa75ed71a1/language-en accessed 14 January 2022.

disincentive for PSBs to make data available if a qualification as personal data cannot be categorically excluded.

Open data, privacy and data protection in the transport sector[227]

One interesting example to showcase the risks for user identification when opening up datasets is the London bike-sharing project. There, the local administration made publicly available the dataset of users' bicycle journeys. In the dataset, there was enough information to track the mobility habits of cyclists across London, since unique customer identifiers were included in the dataset, as well as the location and date/time for the start and end of each journey.

Based on the most frequent itineraries and date/time of journey, it was possible to identify the places where cyclists had their home and workplace and use this information for users' re-identification.

Member State approaches for ensuring compliance with the GDPR[228]

In Belgium, the legislation implementing the PSI Directive foresaw that PSBs can seek advice from the data protection authority on the specific techniques to be used.

In Spain, this is tackled at the level of the licensing agreements between the data holder and the re-user.

3.4.3. Short assessment of impact for MobiDataLab

The PSI regime in total, including the latest Open Data Directive is a clear manifestation of the "Open Data" mandate[229]. It is grounded in the observation that documents produced by public bodies constitute 'a vast, diverse and valuable pool of resources that can benefit society'.[230] Although the Directive applies only to re-use and in principle not the production and original use of the data, it lays down the obligation for Member States to "*encourage public sector bodies and public undertakings to produce and make available documents [. . .] in accordance with the principle of "open by design and by default*"'[231], namely introducing the 'taste' of re-use as from the earliest stages of the

[227] *Mantelero* (n 30), pp. 309-320.
[228] The national examples are set out in the Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.4.
[229] https://digital-strategy.ec.europa.eu/en/policies/open-data, accessed 14 January 2022.
[230] Open Data Directive, recital 8.
[231] Open Data Directive, Article 5(2).

production and first use of the data.[232] Overall, by harmonising the conditions for making data available for re-use, it is expected to facilitate and increase data-sharing.

As the Open Data Directive became applicable recently, there are insufficient data publicly available to understand how Member States have transposed the 2019 Directive and whether there remain any gaps. However, for the purposes of this analysis we could use the 2013 PSI Directive as a yardstick. The 2018 Deloitte study suggests that divergence already exists amongst Member States **[Identified Gap 7]**. Some examples of this divergence are provided in figures 2 and 3 below. Annex D of the same study includes a summary of the legal regime applicable in 10 EU Member States.[233]

Type of action taken	Member States
Adoption of specific measures providing for re-use of public sector information	13 Member States: • Belgium • Cyprus • Germany • Greece • Spain • Hungary • Ireland • Italy • Luxembourg • Malta • Romania • Sweden • United Kingdom
Combination of new measures specifically dealing with re-use and existing legislation	3 Member States: • Austria • Denmark • Slovenia
Adaptation of the legislative framework for access to documents to include re-use of public sector information	12 Member States: • Bulgaria • Czech Republic • Estonia • Finland • France • Croatia • Latvia • Lithuania • Netherlands • Poland • Portugal • Slovakia

Figure 2: State of transposition of the PSI Directive

[232] Charlotte Ducuing, 'Data as Infrastructure? A Study of Data Sharing Legal Regimes' (2020), Competition and Regulation in Network Industries 21, no. 2, pages 124–42. https://doi.org/10.1177/1783591719895390, accessed 14 January 2022.
[233] Deloitte study (n 226), p.45 and p.62 onwards.

MS	Documents for which citizens or companies need to prove a particular interest to obtain access	Documents relating to national security, statistical confidentiality or commercial confidentiality	Documents the supply of which is an activity falling outside the public task	Documents containing personal data	Documents held by educational and research establishments (other than university libraries) and documents held by cultural establishments other than libraries, museums and archives	Documents held by public service broadcasters and their subsidiaries	Documents for which 3rd parties hold intellectual property rights
Estonia	Yes	Yes	Yes	Yes	Yes	No	Yes
France	Partly	Yes	No	No	No	No	Yes
Germany	Yes	No	Yes	No	Yes	Yes	Yes
Greece	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ireland	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Italy	No	Yes	Yes	Yes	Yes	Yes	Yes
The Netherlands	No	No	No	No	Yes	Yes	Yes
Poland	No	No	No	No	Yes	Yes	No
Slovenia	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sweden	No	Yes	Yes	Yes	Yes	Yes	Yes

Source: Spark Legal Network, 2018

Figure 3: Categories of documents excluded under the rules on re-use

The national rules on documents containing personal data are particularly interesting. The national rules on re-use exclude documents containing personal data in Estonia, Greece, Ireland, Italy, the Netherlands, Slovenia and Sweden. In Estonia, for instance, access and re-use of documents containing information that violates private life is excluded. In Greece, data to which access is permitted but re-use is incompatible with personal data rules is excluded from the rules on re-use. In the Netherlands, the rules do not apply to information relating to public personal data, re-use of which is incompatible with the purposes for which the data were collected.

In France, Germany and Poland, documents containing personal data are not excluded. However, in practice, the re-use of such documents may still be restricted. In Germany, for instance, there is no right to access to this data. Additionally, in Poland, the privacy of individuals can be one of the reasons to limit the right to re-use PSI (although documents containing personal data are not generally excluded).

It is not clear whether these rules have changed since 2018 with the more extensive application of the GDPR.

Concerning the extension of the scope to public undertakings and the inclusion of dynamic data and “high-value datasets”, targeting particularly undertakings and datasets in the transport sector is a positive step forward. The added value of the provisions to mobilise openness of data also remains to be seen, taking into consideration any obligations imposed under the Intelligent Transport Systems Directive (for further thoughts on this issue, see section 3.8.5.1.).

Open Data success stories in the transport sector[234]
Deutsche Bahn's Mindbox, driver of its digitisation process, has opened 27 datasets (mostly static) and 9 APIs for dynamic data. The former German railways is today a group of companies providing the physical tracks, the train stations, open access and subsidised passenger rail services as well as cargo rail services. They are now experimenting with opening up data via CC BY 4.0 and for certain datasets CC0 and see the future value this could have in creating their own developers' community and better services for their customers.
SNCF (Société Nationale des Chemins de Fer Français) has opened 208 datasets since it started their open data policy in 2014 and receives 20 million requests for real-time data through their APIs every month. They share data on infrastructure description (static data), maintenance and modernisation work on a weekly basis and social, environmental and financial data. The SNCF platform shares data necessary to plan and compare different journeys from station to station, to research upcoming trains (theoretical and real-time) and to consult timetables in different stations. Zac, a virtual assistant, incorporates SNCF real time data for trains via APIs. Thus, Zac can alert users of train changes and cancellations in real time.
Swiss Railways considers that transport data is also infrastructure thus belongs to the public service. The legal uncertainty regarding the status of these data in Switzerland stifles innovation. For that reason, Swiss railways has a data platform which enables access to target timetable, up-to-date data, information about stops and transport companies, rail time forecast for direct journeys via APIs. However, the data in question is not entirely open as Swiss railways has established some terms of use and limits and costs according to the intensity of the use.
The Estonian Road Administration (ERA) decided to make open data available in view of meeting the need of users of public transportation. The ERA realised that setting APIs for providing facilitated access to its dynamic data would translate in new applications and services that would benefit the end user. Now, a big number of developers and companies make use of their open data. The only barrier that the ERA came across was to adapt the data to GTFS (General Transit Feed Specification) standard. The open data of the public transport register consists of data entered in the national public transport register with other kinds of data content, including descriptions, timetables and the locations of stops of domestic public transport routes. Examples of open data are real-time train information, timetables, public transport stops, travel ticket prices, travel fare concessions; soon ferries and domestic airlines will also be included. This open data is freely accessible to all interested parties and updated daily. When reusing the open data in publicly accessible channels (including websites, applications in smart devices), the party reusing the data commits to providing references to the original source of the data and guarantees that any data used in any publicly accessible applications is no older than 7 days from the moment the data is downloaded. While some of the open data users are big companies, there are other companies and developers who use this data and make competitive apps such as Ridango (a ticketing solution provider**)** or

[234]Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (n 192), p.14 & Annex 9.

App Moovi (a public transit guide). Moreover, many shopping malls use ERA's open data to display public transport timetables of nearby stops.

Transport for London (TfL) released via an API over 200 datasets (bus and metro arrivals, departures, status, cycle hire docking station status, etc.) which created a community of 14,400 developers with over 600 apps. London has gained around 100 million GBP direct value by technological investment and TfL's open data ecosystem has led to the creation of about 500 directly and 230 indirectly related jobs. TfL praises the effect that the re-use of its data has had in reducing the commuting time of the passengers and thereby improving TfL's efficiency.

Open data & cross-border dimension in the transport sector[235]

Several examples of new services created from public open data and having a cross-border element exist.

The most famous are undoubtedly those apps combining geolocalisation with data from local authorities and local transport to provide customised journeys and commuting experiences to citizens. Amongst these apps, the Lithuanian app *Trafi* provides this service for both Lithuanian and Estonian cities.
Similar apps are developed in the domain of whether forecasts*. WeatherPro* for instance builds on meteorological data for providing accurate forecasts for thousands of European locations.

In the domain of cultural data*,* the French app *Monument Tracker* re-uses data from cultural institutions and combines them with many other datasets in order to provide personalised touristic experience in 55 cities worldwide including 49 in Europe. Many other touristic apps with such characteristics are currently emerging (e.g. *Tur4all, WeCity, Historic Atlas* etc.).

3.5. The Regulation on the free flow of non-personal data

In November 2018, the EU adopted a Regulation on the free flow of non-personal data[236] ("Free flow of non-personal data Regulation"), which became applicable in EU Member States from 18 June 2019. The rationale behind the Regulation was to take advantage of the plethora of machine-generated data and foster data-driven innovation by encouraging the free flow of data across EU borders.[237] This is the first legislation dealing with non-personal data, creating what was perceived to be a counterpart to GDPR that deals only with processing of personal data. The Regulation lays

[235] Deloitte study (n 226), p.109.
[236] 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.
[237] European Parliament, European Parliamentary Research Service (EPRS) briefing, 'Free flow of non-personal data in the European Union', January 2019, https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614628/EPRS_BRI(2017)614628_EN.pdf, accessed 14 January 2022.

down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users.[238] Data localisation and the porting of data are the two issues most relevant from a data-sharing perspective, the latter particularly important for the operation of cloud services.

This section will firstly examine the scope of the Regulation and secondly, provide an overview of the main provisions of the Regulation.

3.5.1. Scope of the Regulation

The Regulation applies to the processing of electronic data other than personal data in the Union, which is:

(a) Provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union; or
(b) Carried out by a natural or legal person residing or having an establishment in the Union for its own needs.[239]

(Non-personal) data is defined as "*data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679 [the GDPR]*".[240] This means that one should first examine whether the data qualify as personal data (thereby covered by the GDPR), and if not, they will be considered non-personal data covering by the Free flow of non-personal data Regulation.

Specific examples of non-personal data include 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. These are data that by definition do not relate to an identified or identifiable natural person. Anonymised data should in principle also be considered non-personal data, to the extent however that it is impossible to turn them into personal data (as in that case the GDPR will apply).[241]

3.5.1.1. The case of mixed datasets

[238] Free flow of non-personal data Regulation, Article 1.
[239] Free flow of non-personal data Regulation, Article 2(1).
[240] Free flow of non-personal data Regulation, Article 3(1).
[241] Free flow of non-personal data Regulation, recital 9. For examples of re-identification of supposedly anonymised data see the study on future data flows conducted for the European Parliament's ITRE Committee by Blackman C., Forge S. 'Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee', 2017, p. 22, Box 2, http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf, accessed 14 January 2022.

In the era of machine learning, big data analytics and AI, mixed datasets represent the reality of data in the data economy. Article 2(2) of the Regulation provides that if a dataset is composed of both personal and non-personal data, the Regulation applies to the non-personal data part of the dataset. Where personal and non-personal data in a dataset are inextricably linked, the application of the GDPR cannot be excluded.

However, in practice, it may be difficult to distinguish what is personal and what non-personal data, considering, as was mentioned in section 3.1.1, the wide interpretation of the notion of "personal data". Indeed, data items that in the first place seem to constitute non-personal data, may probably fall under the scope of the GDPR's definition of personal data. This leads to uncertainty as to what information will fall within the scope of the free flow of non-personal data Regulation.[242]

Furthermore, in some situations – e.g., in the case of data porting, where a customer wishes to obtain all of their data back - personal and non-personal data in a dataset can be inextricably linked, and it may not even be possible for a service provider to limit its application of the Regulation to only personal data. It will be complex to determine which Regulation applies to which part of the dataset.[243]

To assist businesses with the ambiguity that follows from mixed datasets, the EC published guidance on this issue in May 2019.[244] The Commission clarified that in a case of a dataset composed of both personal and non-personal data[245]:

- The free flow of non-personal data Regulation applies to the non-personal data part of the dataset;
- The GDPR's free flow provision (Article 1(3)) applies to the personal data part of the dataset; and
- If the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the GDPR fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset.

The guidance attempts to also explain what is meant by "inextricably linked". It suggests that it can refer to a situation whereby a dataset contains personal data as well as non-personal data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible.[246] In any event, businesses are not obliged to separate the datasets they are controlling or processing.

[242] European Commission Support Centre for Data Sharing, Analytical report on EU law applicable to sharing of non-personal data (n 104), p.27.
[243] *Ibid*
[244] European Commission, Communication to the European Parliament and the Council, 'Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union', COM (2019) 250 final.
[245] *Ibid*, p.9.
[246] *Ibid*, p.10.

Funded by the European Union

3.5.2. Overview of the main provisions

With the purpose to ensure the free movement of non-personal data in the EU, the Regulation provides for:

a) **The removal of unjustified or disproportionate data storage location restrictions** (i.e. national rules that require data to be stored/processed in a specific territory):

Many Member States restrict the geographical location and storage of data related to the financial and health sectors, as well as company records, accounting and tax data, telecommunications, and government data.[247] Under the Regulation, this restriction must be abolished and businesses must be able to store and process data anywhere in the EU, unless there are public security reasons that would justify localisation requirements in national legislation (but always respecting the principle of proportionality).[248] Data localisation requirements are defined as "*any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State"*.[249]

b) **Easier switching between cloud service providers for professional users**:

The Regulation seeks to allow the 'porting of data' for professional users[250] to avoid anticompetitive vendor 'lock in' due to a data format or contractual arrangement.[251] It concerns business-to-business scenarios, rather than business-to-consumers. It does not create a data portability right, similar to the one under the GDPR[252], but has a self-regulatory approach, with voluntary codes of conduct for the industry, while also targeting a situation where a professional user has outsourced the processing of its data to a third party offering a data processing service.[253]

The burden is therefore on the Commission to action this provision by encouraging and facilitating the development of self-regulatory codes of conduct at EU level ('codes of conduct') to contribute to

[247] European Parliament briefing (n 237).
[248] Free flow of non-personal data Regulation, Article 4(1).
[249] Free flow of non-personal data Regulation, Article 3(5).
[250] 'Professional user' means a natural or legal person, including a public authority or a body governed by public law, using or requesting a data processing service for purposes related to its trade, business, craft, profession or task; Free flow of non-personal data Regulation, Article 3(8).
[251] Free flow of non-personal data Regulation, recitals 29-31, Article 6.
[252] GDPR, Article 20. Under that provision, the data controller is obliged to transfer the personal data to the data subject or directly to a third-party of the data subject's choice where such transfer is 'technically feasible'.
[253] European Commission Guidance on the Regulation on a framework for the free flow of non-personal data (n 244), p.18.

a competitive data economy. It provides a basis for the industry to develop self-regulatory codes of conduct on the switching of service providers and the porting of data between different IT systems.[254]

Several aspects should be taken into account when developing such codes of conduct on the porting of data, notably:

- Best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format;
- Minimum information requirements to ensure that the professional users, before a contract is concluded, are provided with sufficiently detailed and clear information about the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or the porting of data back to its own IT systems;
- Approaches to certification schemes for better comparability of cloud services; and
- Communication roadmaps to raise awareness of the codes of conduct.[255]

In its Guidance on the Regulation, the Commission gives examples of such codes of conduct developed by the cloud industry: the 'EU Cloud Code of Conduct' developed "on the basis of" data protection law, the Code of Conduct of the Cloud Infrastructure Services Providers in Europe (CISPE) concerning cloud computing service providers acting as 'processors' within the meaning of data protection law, the Cloud Security Alliance's Code of Conduct for GDPR Compliance. The Commission expects that model contractual clauses will complement the various Code of Conducts.

3.5.3. Short assessment of impact for MobiDataLab

Mobility data/datasets may include, apart from personal data, non-personal data. That could be the case for example where anonymised aggregated data (e.g. statistics on most favourable routes per day/week in multimodal transport) are combined with the raw data initially collected (route data of individuals), or IoT data where some of the data allow assumptions to be made about identifiable individuals (e.g. presence at a particular address and usage patterns).[256]

However, classifying data as "non-personal" data may in practice prove very difficult **[Identified Gap 8]**. The best-case scenario includes data that are aggregated to the extent that individual events (such as a person's individual trips abroad or travel patterns that could constitute personal data) are no longer identifiable and can qualify as (irreversibly) anonymous data. But if non-personal data can be related to an individual in any way, causing them to be either directly or indirectly identifiable, the

[254] *Ibid*, p.17.
[255] *Ibid*, p.17.
[256] In line with the examples provided by the European Commission at its Guidance on the Regulation on a framework for the free flow of non-personal data (n 244), p.8.

data must be considered as personal data. The same rules apply when developments in technology and data analytics make it possible to convert anonymised data into personal data.[257]

The practical significance of the Regulation can therefore be disputed. The distinction between "personal" and "non-personal" can have a negative impact when it comes to mixed datasets. Businesses may have difficulty categorising data as non-personal, thereby obliged to consider data as personal – even though they might not be - and apply the GDPR out of fear of non-compliance (given the threat of hefty fines) with all the obligations that flow from the GDPR for controllers and processors.[258] This in turn will create further obstacles in data sharing.

The data localisation provisions are particularly relevant for cloud services and will thus facilitate the creation and operation of the Transport Cloud that MobiDataLab seeks to prototype. The abolition of national data localisation rules means that regardless of where the data will be stored, it could host and process data from private and public actors that are established wherever in the EU, thereby facilitating data sharing. Conversely, the provisions of data porting might lead to businesses retrieving their data and switching to other cloud providers (assuming they exist), which could diminish the value of the Transport Cloud. But these provisions are subject to industry Codes of Conduct, so it remains to be seen how it will work in practice.

3.6. Legislation concerning digital platforms[259] and intermediaries

This section outlines the legislation applicable to digital platforms and intermediaries, namely the e-Commerce Directive, the Platform-to-Business Regulation and the latest EC legislative initiatives - the Digital Services Act and the Digital Markets Act.

In the past decade, digital platforms have played a prominent role in creating digital value. The term "digital platform" covers digital services that have the following characteristics: they facilitate interactions via the internet between two or more distinct but interdependent sets of users (whether firms or individuals), collect and use data about such interactions (often to optimise the experience of users), while generating and taking advantage of so-called network effects. Examples of such online platforms include online marketplaces, app stores, search engines, social media and platforms for the collaborative economy.[260] But there is no single definition of an "online platform" and the list of examples is not exclusive. Digital platforms cover different businesses and sectors.

[257] In line with the examples provided by the European Commission at its Guidance on the Regulation on a framework for the free flow of non-personal data (n 244), p.7.
[258] Laura Somaini, 'Regulating the Dynamic Concept of Non-Personal Data in the EU: From ownership to Portability', European Data Protection Law Review, 6(1), p. 90.
[259] Also referred to as "online platforms" or simply "platforms". The two terms will be used interchangeably in this section.
[260] European Parliament, European Parliamentary Research Service (EPRS) study, 'Online Platforms: Economic and societal effects', March 2021, <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU(2021)656336_EN.pdf>,

On a more general level, online platforms can be described as a digital infrastructure allowing the supply side (the suppliers) to meet the demand side (the customers). They are working in the interests of suppliers and customers, facilitating the process of concluding contracts. Online platforms thus function as a triangular structure based on relations between the platform and the supplier, the platform and the customer, and the supplier and the customer.[261]

Intermediaries can be classified as middlemen, acting between one internet user and another party, also using the internet.[262] The term was first used in the context of the e-Commerce Directive (see further below under section 3.6.1) to classify mere conduit, caching and hosting services that simply facilitated an exchange without any further involvement in the content/data that was being exchanged.

Data sharing platforms could also qualify as a "digital platform" and/or an intermediary. The Commission has suggested that data sharing can take place under the following models[263]:

- **Data monetisation on a data marketplace** (B2B data sharing): The data marketplace can act as an intermediary based on bilateral contracts against remuneration. This mechanism appears suitable when either (1) there are limited risks of illicit use of the data in question, (2) the data supplier has grounds to trust the (re-)user, or (3) the data supplier has technical mechanisms to prevent or identify illicit use;
- **Data exchange in a closed platform** (B2B data sharing): The platform can be either set up by one core player in a data-sharing environment or by an independent intermediary. The data, in this case, may be supplied against monetary remuneration or added-value services, provided e.g. inside the platform;
- **Intermediaries** (B2G data sharing): In cases when there is no previous relationship between a company and a public sector body and trust between the two is absent, an intermediary can be tasked to obtain insights necessary for public interest purposes.

Depending on the business needs, different models and variations/combinations thereof can be set up.[264]

---

accessed 14 January 2022. The study provides a deep analysis of the main characteristics of online (digital) platforms.

[261] European Parliament, IMCO Committee briefing note on 'Online Platforms: How to Adapt Regulatory Framework to the Digital Age?', September 2017, < https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607323/IPOL_BRI(2017)607323_EN.pdf> , accessed 14 January 2022.

[262] Christina Angelopoulos, *European intermediary liability in copyright: a tort-based analysis* (2017, Kluwer Law International).

[263] European Commission, Staff Working Document, 'Guidance on Sharing Private Sector Data in the European Data Economy' Accompanying the Document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a Common European Data Space".

[264] An overview of data governance models will be provided in D2.7.

Funded by the European Union

3.6.1. The e-Commerce Directive

The e-Commerce Directive[265] ("ECD") regulates legal aspects of information society services, i.e. any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services[266]. It was considered a milestone at the time, as it created a legal framework to ensure the free movement of information society services in the EU, allowing for the setup and development of electronic commerce in the internal market, as at the time (2001) "information society services" started to appear in the digital scene but there was no EU-wide instrument to regulate those in a harmonised way.

The ECD only indirectly impacts data sharing through its provisions on the liability of intermediary online services. The Directive does not actually establish liability for these services but provides the conditions under which they can escape liability (under civil, criminal or administrative national laws) – the so-called "safe harbour" provisions. The provisions cover mere conduit, cache and hosting providers. Mere conduit consists of the "transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network"[267]. Caching covers "the transmission in a communication network of information provided by a recipient of the service, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request"[268]. Hosting is described as "the storage of information provided by a recipient of the service"[269].

In these cases, such service providers are not liable for the use of their services provided that they do not curate the data passing through their services, that they have no actual knowledge of unlawful use of their services, and that they act expeditiously when they received notifications of unlawful use. The reasoning behind this is to protect intermediaries who are not actively involved in the creation, identification, promotion of the harmful activity but who are only involved in the passive transit or hosting of the infringing content.[270]

At the same time, they cannot be subject to generally monitor their services for illegal activities, but eventually only to inform competent public authorities of illegal activities they happen to have knowledge for and of information enabling the identification of recipients of their services with whom they have storage agreements.[271]

The relevance of the ECD safe harbour has been recently questioned by many stakeholders given the developments in digital technologies and the rise of AI, IoT and Big Data. In response to that,

[265] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, OJ L 178, 17.7.2000, p. 1–16.
[266] ECD, recitals 17-18, Article 2(a). Most recently, the CJEU opined on the what constitutes an "information society service" in its judgments concerning *Uber* (C-434/15) *Airbnb* (C-390/18) and *Star Taxi App* (C-62/19).
[267] ECD, Article 12.
[268] ECD, Article 13.
[269] ECD, Article 14.
[270] European Commission Support Centre for Data Sharing, Analytical report on EU law applicable to sharing of non-personal data (n 104).
[271] ECD, Article 15.

the Commission decided to introduce its Digital Services Act package (see further below under 3.8.3).

3.6.2. The Platform to Business Regulation ("P2B Regulation")

The Regulation on promoting fairness and transparency for business users of online intermediation services ("Platform to Business Regulation" or "P2B Regulation"[272]) was adopted in 2019 to restore balance in the relationship between online platforms and businesses that use the platforms. The Regulation essentially includes provisions akin to those under consumer legislation (e.g. transparency, notification in case of change in T&Cs, class action type of lawsuits or other types of redress). The Commission considered this essential as consumer legislation does not only apply in a B2B context, taking also into account the role that online platforms play in today's digital economy and the *de facto* dependency of businesses on platforms to reach users.

The P2B Regulation targets "online intermediation services" and "providers of online search engines".[273] For the purposes of this report, we will solely focus on the former as search engines are not relevant for this analysis. Online intermediation services are defined as "services which meet all of the following requirements: (a) they constitute information society services; (b) they allow business users to offer goods or services to consumers, to facilitate the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users based on contractual relationships between the provider of those services and business users which offer goods or services to consumers".[274]

Like the ECD, the P2B Regulation may only indirectly impact data sharing through the introduction of several obligations on online intermediation services[275]:

- **Transparency on T&Cs[276]:** providers of online intermediation services would be required to ensure that their terms and conditions for professional users are easy to understand, easily available for business users, and that there are objective grounds for suspending or terminating the services. A breach of this transparency measure would result in the contractual terms and conditions becoming non-binding on the business users. Such providers would be required to notify their business users in advance of any envisaged modifications of their T&Cs, unless they would be subject to a specific legal obligation;

[272] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.7.2019, p. 57–79.
[273] P2B Regulation, Article 1(2).
[274] P2B Regulation, Article 2(2).
[275] European Parliament, European Parliamentary Research Service (EPRS) briefing, 'Fairness and Transparency for business users of online services', April 2019, https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625134/EPRS_BRI(2018)625134_EN.pdf accessed 14 January 2022.
[276] P2B Regulation, recitals 14-20, Article 3.

- **Transparency on access to data[277]:** providers of online intermediation services must provide business users with a clear description of the scope, nature and conditions of their (technical and contractual) access to and use of certain categories of data (personal/not personal). The description might refer to general access conditions, rather than an exhaustive identification of actual data, or categories of data. However, identification of and specific access conditions to certain types of actual data that might be highly relevant to the business users could also be included in the description. The description should enable business users to understand whether they can use the data to improve their business themselves, including by possibly retaining third-party data services (e.g. data analytics).[278]

Business users should also be made aware of any sharing of data (which has been generated using the intermediation service by the business user) with third parties, for example where the provider monetises data under commercial considerations. Providers of online intermediation services should also be explicit about possibilities to opt-out from the data sharing where they exist under their contractual relationship with the business user.[279]

However, the Regulation clarifies that the above requirements do not translate to an obligation for providers of online intermediation services to either disseminate or not to disseminate personal or non-personal data to their business users. Conversely, the increased transparency measures are seen as a means to contribute to increased data sharing by allowing business users to benefit from data they need and enhance the aims to create a common European data space[280].[281]

3.6.3. The new proposals for a Digital Services Act ("DSA proposal") & a Digital Markets Act ("DMA proposal")[282]

On 15 December 2020, the Commission published its Digital Services Act package, which proposed two new pieces of legislation: the Digital Services Act and the Digital Markets Act.[283] According to the Commission, they have two main goals: (1) to create a safer digital space in which the fundamental rights of all users of digital services are protected; (2) to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally. The Commission deemed it necessary to propose new legislation to make sure that the law does not stay behind technological developments and digital platform-related evolutions, considering that the latest (horizontal) EU legislation on platforms/intermediaries is the ECD, dating back to 2001.

[277] P2B Regulation, Article 9. For further details see also the Commission's Q&A 'Establishing a fair, trusted and innovation driven ecosystem in the Online Platform Economy', July 2020, pages 23-24, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68300 accessed 14 January 2020.
[278] P2B Regulation, recital 33.
[279] P2B Regulation, recital 34.
[280] For further details, see section 3.7 on the Data Governance Act.
[281] P2B Regulation, recital 35.
[282] This section analyses the initial Commission proposals and does not take into account proposals tabled by the European Parliament and the Council of the EU. At the time of drafting, the European Parliament was scheduled to vote on its report in January 2022 while trilogue negotiations between the Council of the EU and the European Parliament had not yet commenced.
[283] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package, accessed 14 January 2022.

The new rules, once adopted, will transform the rights and obligations of digital service providers, online users, customers and business users in the EU.[284]

In brief, the DSA proposal targets intermediary services in a broad sense, imposing a number of obligations (e.g., transparency reporting, redress, notice and action etc.) based on the exact intermediary category depending on their role, size and impact in the online ecosystem. Conversely, the DMA proposal targets so-called "gatekeepers", i.e. large digital platforms that play an important role in the digital economy and satisfy specific criteria set out in the proposed law (e.g. their positioning in the relevant market, their user base). The obligations it imposed on them seek to redress perceived power asymmetries between the platforms, their business users and end-users (consumers) as well as general market structure issues, which, arguably, competition law cannot resolve. Some companies may be subject to both the DSA and the DMA proposal.

3.6.3.1. The DSA proposal

The DSA proposal sets out a horizontal framework for transparency, accountability and regulatory oversight of the EU online space.[285] A lot of discussions had taken place about the proposal replacing the ECD and especially the liability regime, but the new legislation will not replace the ECD. However, to provide greater harmonisation, it incorporates the existing rules exempting online intermediaries from liability of the content they host under certain conditions to ensure innovative services can continue to emerge and scale-up in the single market.[286]

The material scope of the DSA proposal is quite broad. It applies to "intermediary services" (that cover mere conduit, caching and hosting services)[287] and imposes different sets of obligations for distinct categories of online intermediaries according to their role, size and impact in the online ecosystem.

Accordingly, the draft DSA differentiates rules on:

- **Intermediary services** provided by network infrastructure providers;
- **Hosting services** provided by providers storing and disseminating information to the public, such as cloud and webhosting services;

[284] At the time of writing, the legislative procedure is still ongoing. Information for the DSA can be found here: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-services-act and for the DMA here: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-markets-act accessed 14 January 2022.

[285] European Parliament, European Parliamentary Research Service (EPRS) briefing, 'Digital Services Act', https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf, accessed 14 January 2022.

[286] European Commission Q&A on the Digital Services Act, https://digital-strategy.ec.europa.eu/en/digital-services-act-questons-and-answers, accessed 14 January 2022.

[287] DSA proposal, Article 1(3) and Article 2(f).

Funded by the European Union

- **Online platform services** by providers bringing together sellers and consumers, such as online marketplaces, app stores, collaborative economy platforms and social media platforms; and
- **Very large online platforms (or VLOP) services** provided by platforms that have a particular impact on the economy and society and pose particular risks in the dissemination of illegal content and societal harms.

Specific rules are set out for platforms that reach more than 45 million active recipients in the EU monthly. The methodology to designate VLOPs will be set out in a delegated act by the Commission and a list of VLOPs will be drawn up and revised regularly.[288]

An overview of the different obligations is summarised in the following figure[289]:

	Intermediary services	Hosting services	Online platforms	Very large online platforms
Transparency reporting (A13, R39)	•	•	•	•
Requirements on terms of service due account of fundamental rights (A12, R3)	•	•	•	•
Cooperation with national authorities following orders (A8 and A9; R29,30,31,32,42)	•	•	•	•
Points of contact and, where necessary, legal representative (A10, R36; A11; R37)	•	•	•	•
Notice and action/obligation to provide information to users (A14 and A15. R40-42)		•	•	•
Complaint and redress mechanism and out of court dispute settlement (A17 and A18, R44 and 45)			•	•
Trusted flaggers (A19, R46 and 47)			•	•
Measures against abusive notices and counter-notices (A20, R46 and 47)			•	•
Vetting credentials of third party suppliers ("KYBC") (A22, R49)			•	•
User-facing transparency of online advertising (A24, R52)			•	•
Reporting criminal offences (A21, R48)			•	•
Risk management obligations and compliance officer (A26, 27 and A32, R57, 59 and 65)				•
External risk auditing and public accountability (A28 and 33, R60, 61 and 65)				•
Transparency of recommender systems and user choice for access to information (A29 and A30, R62 and 63)				•
Data sharing with authorities and researchers (A31, R64)				•
Industry Standards and Codes of conduct (A35 and A36, R66-70)				•
Crisis response cooperation (A37, R71)				•

A — Refers to Articles in the proposed Digital Services Act Regulation R — Refers to Recitals in the proposed Digital Services Act Regulation

Figure 4: The obligations imposed under the DSA proposal per category of operator

The main provisions that may impact data sharing are the following[290]:

[288] EPRS briefing (n 285).
[289] https://www.connectontech.com/wp-content/uploads/sites/38/2021/01/Baker-McKenzie-Digital-Services-Act.pdf, accessed 14 January 2022.
[290] EPRS study (n 260), pp.65-66. The study does not focus on data sharing, but rather sets out the main provisions of the DSA Act.

- **Liability regime for intermediary services**: The key principles from the ECD remain generally unchanged, but the DSA proposal adds obligations to address notifications of content considered as illegal. The DSA proposal requires every hosting provider or online platform to put user-friendly notice and takedown mechanisms that allow the notification of illegal content. Online platforms will need to establish internal complaint-handling systems, engage with out-of-court dispute settlement bodies to resolve disputes with their users, give priority to notifications of entities that have been qualified as so-called trusted flaggers by the authorities and suspend repeat infringers;
- **Transparency obligations** for online platforms relating to the measures taken to combat illegal information: If content is removed, an explanation needs to be provided to the person who uploaded that content. Online platforms must also publish detailed reports on their activities relating to the removal and the disabling of illegal content or content contrary to their terms and conditions;
- **Transparency on information related restrictions:** An obligation on intermediaries to include in their terms and conditions information on any restrictions on the use of information provided by the users, with reference to the content moderation mechanisms applied, algorithmic decision-making and human review. This information must be in clear and unambiguous language and publicly available in an easily accessible format.

3.6.3.2. The DMA proposal

The DMA proposal focuses on the largest platforms – mostly US-based – and seeks to redress perceived power asymmetries between platforms, their business users and end-users (consumers) - as well as issues around general market structure - to ensure markets remain "fair and contestable". The Commission's concern is that existing competition law enforcement is too slow and cumbersome to rectify problems before markets "tip" irrevocably in favour of the strongest players.[291] In practice, the Commission is trying to legislate on platform-related issues that current competition law rules have been insufficient to address. This marks a shift from *ex post* intervention under competition law to *ex-ante* legislation.

The scope of the DMA proposal is quite narrow/specific. It applies to core platform services acting as “gatekeepers”.

The following services would qualify as “core platform services”:

- Online intermediation services, including marketplaces and app stores (e.g. Amazon marketplace);
- Online search engines (e.g. Google Search);
- Social networks (e.g. Facebook);
- Video sharing platforms (e.g. YouTube);
- Number-independent communication platforms (e.g. WhatsApp or Skype);

[291] https://www.connectontech.com/wp-content/uploads/sites/38/2021/01/Baker-McKenzie-Digital-Markets-Act-2.pdf, accessed 14 January 2022.

- Operating systems (e.g. Microsoft Windows or Google Android);
- Cloud computing services (e.g. Microsoft Azure); and
- Advertising services offered by a provider of any of the 7 core platforms services mentioned above.

A platform will be considered a "gatekeeper" if it (cumulatively):

- Has a strong economic position, significant impact on the internal market and is active in multiple EU countries;
- Has a strong intermediation position, meaning that it links a large user base to a large number of businesses;
- Has (or is about to have) an entrenched and durable position in the market, meaning that it is stable over time.[292]

The DMA proposal further sets out (rebuttable) thresholds under which a gatekeeper will be presumed to have a significant impact on the internal market[293]:

- If it has an annual EEA turnover equal or above EUR 6.5 billion in the last three financial years or has an average market capitalisation of EUR 65 billion; and
- If it provides a core platform service in at least three Member States.

In addition, the provider of core platform services shall be presumed to satisfy the criteria of operating one or more important gateways to customers where the relevant core platform service has 45 million monthly active end-users in the EU and more than 10,000 yearly active business users in the last three years.[294]

In practice, where a provider of core platform services meets all the above thresholds, it must notify the Commission within three months after those thresholds are satisfied. However, a failure by a provider to notify the required information will not prevent the Commission from designating these providers as gatekeepers at any time.[295] The Commission will examine the information submitted before her and will designate the provider of core platform services that meets all the above thresholds as a gatekeeper, unless that provider, with its notification, presents arguments to demonstrate that, in the circumstances in which the relevant core platform service operates, the provider does not satisfy the 3 cumulative criteria of Article 3(1).[296]

Digital platforms identified as "gatekeepers" would need to implement a set of do's and don'ts, as set out in the following figures[297]:

[292] DMA proposal, Article 3 and European Commission, 'The Digital Markets Act: ensuring fair and open digital markets', https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en accessed 14 January 2022.
[293] DMA proposal, Article 3(2)(a).
[294] DMA proposal, Article 3(2)(b) and (c).
[295] DMA proposal, Article 3(3).
[296] DMA proposal, Article 3(4).
[297] Baker McKenzie (n 291).

Figure 5: Summary of obligations imposed on gatekeepers

The proposed DMA is not a conventional competition tool as such, but rather a type of market regulation aiming to guarantee equal opportunities for digital players through an *ex-ante* designation of expected or prohibited behaviours. The proposal seeks to create a fair-trading environment and thus unleash the innovative potential of online platform ecosystems. Online gatekeepers are subjected to a wide range of upfront constraints to address unfair practices and the ensuing harms in a timely and effective manner.[298] As such, certain potentially anticompetitive conducts in online markets are prevented by way of *ex-ante* rules, without the need to prove any actual harm. These rules reduce the control of gatekeepers and curb their corresponding ability to leverage data gathered in one area of activity to improve or offer services in adjacent markets.

The proposal distinguishes between the directly applicable obligations and those that need further articulation or elaboration within the framework of a dialogue between the Commission and the gatekeepers concerned. Where platforms compete with their own users, the gatekeepers are prohibited from prioritising their own services, for instance, *Google* placing ads in search engine results or *Amazon* using data generated by its customer businesses to compete with them.[299] Online platforms are also obliged to offer application developers fair and non-discriminatory conditions of access to the data they hold. The proposed DMA also contains obligations concerning data use and management which are of significant relevance to data contracts.

The DMA proposal has a strong focus on services that intermediate between businesses and consumers. But there are some provisions that, if adopted, may impact data sharing (which happens primarily in a business-to-business and business-to-government setting). Gatekeepers will have to:

a) Refrain from using competitors' data to compete with them (i.e. data generated through the activities of business users).
b) Provide business users with continuous and real-time data portability (i.e. for data generated by both business and end-users in the context of the use of the core platform services) and real-time access of aggregated or non-aggregated data;

---

[298] The Commission considered that Article 102 of TFEU was not sufficient to deal with all the problems associated with gatekeepers, given that a gatekeeper may not necessarily be a dominant player, and its practices may not be captured by Article 102 TFEU if there is no demonstrable effect on competition within clearly defined relevant markets.

[299] In the Google Shopping case, the European Commission fined Google for abusing its market dominance as a search engine by giving an illegal advantage to another Google product, its comparison-shopping service. European Commission, 'Press Release: Antitrust: Commission Fines Google €2.42 Billion' (27 June 2017) https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 accessed 14 January 2022; Also see the pending Amazon Marketplace (17.07.2019) and Amazon Buy Box (10.11.2020) investigations. The Commission inquires whether Amazon's use of non-public business data of independent sellers who sell on its marketplace amounts to an abuse of dominant position. The Commission has stated that the preliminary findings showed that very large quantities of non-public seller data were available to employees of Amazon's retail business. This allows Amazon to focus its offers in the best-selling products across product categories and to adjust its offers in view of non-public data of competing sellers. European Commission, 'Press Release: Antitrust: EC Opens Formal Investigation against Amazon' (17 July 2019) https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291 accessed 14 January 2022; European Commission, 'Press Release: Antitrust: Amazon' (10 November 2020) https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077 accessed 14 January 2022.

Funded by the European Union

c) Implement interoperability (i.e. allow business users and providers of ancillary services, e.g. payment services, to access and interoperate with the gatekeeper);
d) Provide third-party providers of online search engines with access on Fair, Reasonable and Non-discriminatory (FRAND) terms to ranking, query, click and view data concerning search generated by end-users on online search engines of the gatekeeper.[300]

Obligations a) – d) seek to reduce gatekeepers' exclusive control over the data they collect. Especially b) and c) aim to allow business users to access and re-use data that they or end-users generate on the platform. However, it has been argued that the exact scope and implementation of the rules on data portability, data sharing and interoperability could be further specified.[301] Others have argued that this "revolutionary" provision allowing business users to access data may prove moot in practice as gatekeepers may invoke their intellectual property rights or personal data protection to prevent data re-use.[302]

Data portability under the DMA proposal seems to have a broader scope than the GDPR's right to data portability and it would ensure additional forms of portability, including portability of non-personal data for business users and real-time and continuous portability. However, the implementation of data portability runs into several technical, legal and economic obstacles (e.g. loss of context once data assets are ported from the original platform, need to obtain consent from natural persons to port personal data).[303]

Some scholars have stressed that the scope of the data-sharing obligation under the draft DMA proposal does not provide a structural solution to the lack of data sharing because the scope of this obligation is restricted to search data and to a few large online platforms acting as gatekeepers. They call on EU policymakers to adopt a more detailed institutional framework to enforce the data-sharing obligation possibly with the creation of a European data-sharing agency or a data-sharing cooperation network.[304]

Finally, on interoperability, the European Data Protection Supervisor ("EDPS") recommends introducing minimum interoperability requirements to be imposed on gatekeepers and the implementation of technical standards drawn up at the EU level.[305]

---

[300] European Parliament, European Parliamentary Research Service (EPRS) briefing, 'Digital markets act: EU legislation in Progress', May 2021, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690589/EPRS_BRI(2021)690589_EN.pdf, accessed 14 January 2022.
[301] *Ibid*, p.9.
[302] Björn Lundqvist, 'The Proposed Digital Markets Act and Access to Data: A Revolution, or Not?' (2021) IIC 52**,** 239–241. https://doi.org/10.1007/s40319-021-01026-0, accessed 14 January 2022.
[303]EPRS briefing (n 300), p.9.
[304] *Ibid*
[305] EDPS, 'Opinion 02/2021 on the Proposal for a Digital Markets Act', 10 February 2021, https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf, accessed 14 January 2022.

Funded by the European Union

3.6.4. Short assessment of impact for MobiDataLab

The abovementioned legislation provides (and applies to) different categories of online services: “intermediaries”, “hosting services”, “online intermediation services”, “very large online platforms”, “core platform services”. This creates a difficulty to evaluate in which exact category (or categories) each service might belong, and consequently, the obligations that it needs to follow.

The most recent legislation (P2B, DSA proposal, DMA proposal) was conceived having in mind big technology platforms. Therefore, it is not clear to what extent they would apply to online platforms that seek to facilitate data transactions, which are still in their infancy. It should also be taken into consideration that the Commission seeks to create a European single market for data, which means that data transactions should be facilitated, rather than hindered by onerous obligations and uncertainty on which legal regime applies. The fact that the Commission tabled a proposal targeting exactly data intermediaries (the Data Governance Act, see further below under 3.7) unfortunately complicates things even more. Hopefully, there will be some further clarity in the future on this subject.

3.7. The Proposal for a Data Governance Act (“DGA proposal”)[306]

In November 2020, the European Commission adopted the Proposal for a Data Governance Act (“DGA proposal”).[307] It is the first legislative initiative under the Commission’s 2020 European Data Strategy that aims to reinforce the single market for data. The objective of the DGA proposal is to set the conditions for enhancing the development of the common European data spaces, as identified in the strategy document[308], by bringing trust in data sharing and data intermediaries.[309] In that respect, the DGA proposal lays down an overarching framework comprising horizontal measures relevant for all common European data spaces while leaving room for the application of sector-specific rules.

This section analyses the initial Commission proposal and does not take into account proposals tabled by the European Parliament and the Council of the EU.

[306] This section is based on and includes extracts from CITIP’s White Paper on the DGA proposal; Baloup J., Bayamlıoğlu E., Benmayor A., Ducuing C., Dutkiewicz L., Lalova T., Miadzvetskaya Y., Peeters B., White Paper on the Data Governance Act - CiTiP Working Paper. 23 Jun 2021. CiTiP KU Leuven, available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703, accessed 14 January 2022.
[307] European Commission, Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act), COM (2020) 767 final.
[308] A European Strategy for Data (n 10).
[309] European Commission Staff Working Document, ‘Impact Assessment Report accompanying the DGA proposal’, SWD (2020) 295 final, Section 1.2.

Funded by the European Union

During the time of drafting, the European Parliament and Council reached a provisional agreement.[310] But the informal agreement still needs to be formally endorsed by the Parliament and Council, and the final text agreed is not yet available.

3.7.1. Re-use of certain categories of protected data held by public sector bodies[311]

Chapter II of the DGA proposal concerns public sector bodies, defined as the State, regional or local authorities, bodies governed by public law, or associations formed by one or more such authorities, or one or more such bodies governed by public law.[312] It pursues, *inter alia*, to unlock the potential of re-use of the 'data' deemed to be outside the scope of the Open Data Directive (see section 3.6 above) —those subject to third party rights, covering data protected on the ground of commercial confidentiality, statistical confidentiality, intellectual property rights of third parties, and protection of personal data.[313] Data covered by the rights of third parties, allegedly excluded from the scope of the Open Data Directive, is therefore not subject to obligations for PSBs to make them available for re-use to the benefit of third parties, for both commercial or non-commercial purposes under that Directive. This objective of providing access to data that is not accessible as 'open data' may be seen as indicative of the emergence of a distinct regime for the data held by PSBs.

In contrast, the DGA proposal aims to find ways to make such data available for re-use to the extent possible. The Open Data Directive generally mandates PSBs to share the documents that they hold following the 'open data' approach, namely data in an open format that can be freely used, re-used, and shared by anyone for any purpose.[314] In contrast, the ambition of the EC with the DGA proposal is to find a middle ground by doing the following. First, allowing the re-use of data covered by the rights of third parties under more granular schemes compared to the open data approach of the Open Data Directive and, second, supporting PSBs in setting out the appropriate legal and technical arrangements to do so.

The DGA proposal does not create an obligation (*a fortiori* of result) for PSBs to make data covered by the rights of third parties available for re-use by potential data re-users, but there are some obligations (of means), namely to take some measures in order to facilitate such re-use.

However, there seems to be a risk of overlap and inconsistency in the scope of application of the DGA proposal with the Open Data Directive which results in a lack of clarity on which obligation(s) is(are) concretely applicable to PSBs **[Identified Gap 9].**[315] The DGA proposal is based on the

[310] European Parliament, 'Press Release: Data governance: deal on new rules to boost data sharing across the EU' (30 November 2021), https://www.europarl.europa.eu/news/en/press-room/20211129IPR18316/data-governance-deal-on-new-rules-to-boost-data-sharing-across-the-eu, accessed 14 January 2022.
[311] For the entire commentary on this section of the DGA proposal, please see CiTiP's Working Paper on the DGA proposal (n 306).
[312] DGA proposal, Article 2(11).
[313] DGA proposal, Article 3(1) and (2). Defence and security-related secret data remain outside of the scope.
[314] Open Data Directive, recital 16.
[315] CiTiP's Working Paper on the DGA proposal (n 306).

Funded by the European Union

assumption of a 'black or white' legal situation, where data would either be in the scope of the Open Data Directive or outside the scope. In the latter case, data may fall under the scope of the DGA. In reality, there is an obvious grey zone where 'documents' (in the parlance of the Open Data Directive) are adapted by PSBs to be accessed and re-used, according to the Open Data Directive, without infringing the rights of third parties (i.e. by deleting or anonymising sensitive parts of a document).

The risk of overlap between the Open Data Directive and the DGA proposal is reinforced by the reference to 'data' as a subject matter regulated in the DGA proposal. The 2003 PSI Directive applied to "documents", defined as "*any content whatever its medium [...]; any part of such content*." In contrast, the DGA proposal applies to 'data'. The question is, therefore, whether the term 'data' has replaced this of 'document' *mutatis mutandis*, or whether the two terms refer to different subject matters.

3.7.2. Data sharing services

This section will focus on the rules relating to "data sharing services" ("DSS"). The DGA proposal does not provide a definition for those services, but only defines "data sharing" as "*the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary*".[316] It follows from that definition that "data sharing services" are the intermediaries that facilitate the sharing of data between a data holder and a data user.

Article 9 of the DGA proposal describes which categories of intermediaries would qualify as "data sharing services providers" ("DSSP"):

- "Intermediation services" between data holders which are legal persons and potential data users;
- "Intermediation services" between data subjects and potential data users; and
- Services of "data cooperatives".[317]

"Intermediation services" between data holders (legal persons) and data users include:

- Bilateral or multilateral exchanges of data;
- The creation of platforms or databases enabling the exchange or joint exploitation of data; and
- The establishment of a specific infrastructure for the interconnection of data holders and data users.[318]

[316] DGA proposal, Article 2(7).
[317] DGA proposal, Article 9. Data cooperatives a form of data governance will be analysed under D2.7.
[318] DGA proposal, Article 9(1)(a).

Funded by the European Union

It should be noted that the DGA Proposal does not provide a set of criteria allowing to precisely identify 'intermediation services' considered as 'data sharing services. Rather, it provides examples of 'intermediation services' that shall be considered as 'data sharing services' such as bilateral or multilateral exchanges of data. It could be argued that this creates a futureproof regime that may allow different business models to flourish.

Rec. 22 of the DGA proposal intends to provide some guidance to identify what services or activities qualify as DSS. It is stated that the DGA proposal should only cover services that have as a "*main objective the establishment of a business, a legal and potentially technical relation*" between data holders (including data subjects on the one hand, and potential users on the other) and that aim to mediate data transactions. As the recital provides, these services should be aiming to intermediate between an indefinite number of data holders and data users. Those who collect data from external sources to offer services — without establishing a direct relationship between data holders and data users, e.g., advertisement or data brokers, data consultancies — are excluded.

In addition, making available the technical or other means to enable 'intermediation services' is also considered as 'data sharing services'. The DGA Proposal thus adopts a wide approach, arguably in line with its objective of regulating the activities of a broad range of service providers to bring trust in the data sharing ecosystem.

Providers of DSS are subject to several requirements under the DGA proposal, from a notification procedure as a pre-condition to provide data sharing services to conditions to comply with during the provision of such services.

a) Notification of data sharing services providers

Any entity who intends to provide "data sharing services" will be expected to submit a notification to the competent authority designated in the relevant Member State.[319] Thus, before being able to offer DSS, service providers have to notify the competent national authority in charge of monitoring and supervising compliance with this legal regime. Through this notification procedure, all data intermediaries operating in EU will be listed on a register kept by the Commission.

b) Conditions for providing data sharing services

To provide "data sharing services", entities will need to respect several strict conditions, notably the principle of (i) neutrality, (ii) the obligation to provide fair, transparent, and non-discriminatory access to the service, and (iii) the obligation to ensure a continuity of provision of the service.

[319] DGA proposal, Article 10.

Funded by the European Union

i) The principle of neutrality

The principle of neutrality is the cornerstone of the DSS regime to foster trust in data intermediaries and data sharing mechanisms. This principle translates into the following conditions:

- **Cross-usage of data prohibition:** data intermediaries are not allowed to use the data exchanged for other purposes.[320]
- **Limited intervention on the data exchanged**: data intermediaries have to facilitate the exchange of data in the format in which they receive it from the data holder. The conversion of the data into specific formats must be limited, for instance, to ensure interoperability.[321]
- **Limited use of metadata:** the metadata collected from the provision of the data-sharing service may be used only for the development of that service.[322]
- **Obligation to place the data sharing services in a separate legal entity**.[323] This entails that the provider of DSS shall be established as a legal entity and shall not provide other types of services through this entity.

ii) Obligation to provide fair, transparent, and non-discriminatory access to the service

The provider of DSS shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data holders and data users, including as regards prices.[324] This obligation also aims to ensure the neutrality of services, from the perspective of data holders and users. Obligations to ensure fair, transparent, and non-discriminatory access to the service usually constitute obligations for utility providers in sector-specific regulation. For instance, to ensure a smooth transition of the liberalisation of railway services, namely from legal monopoly to market conditions, railway infrastructure managers are bound by similar obligations vis-à-vis railway undertakings.[325]

iii) Obligation to ensure a continuity of provision of the service

The provider shall ensure reasonable continuity of provision of its services.[326] Such an obligation constitutes a principle of public law and a cornerstone of public service. The continuity of public services is recognised by the French Constitutional Court as vested with constitutional value, based

[320] DGA proposal, Article 11(1).
[321] DGA proposal, Article 11(4).
[322] DGA proposal, Article 11(2).
[323] DGA proposal, Article 11(1).
[324] DGA proposal, Article 11(3).
[325] See Directive 2012/34/EU of 21 November 2012 establishing a single European railway area (recast), OJ L 343/32, especially Chapter II, Section 4.
[326] DGA proposal, Article 11(6).

Funded by the European Union

on the 'continuity of the State's argument.[327] The principle of continuity of service is based on the exceptional character of public service activities as opposed to traditional economic ones conducted by profit-driven private entities. The DGA proposal thus imposes a principle of public law on DSS providers, although these are not identified as public service providers.

3.7.3. Short assessment of impact for MobiDataLab

The DGA proposal lays down the ground rules for heavy-handed regulation of data sharing services. This can be explained by the need to increase trust in data sharing and data intermediaries. At the same time, the Commission aims to create a model for data sharing through the emergence of data intermediaries acting as neutral market facilitators. The neutrality obligation concerns the data exchanged and ensuring fair, transparent and non-discriminatory access to their services. To some extent, the DGA proposal might lean towards the creation of 'data/digital utilities', carrying out a data intermediation activity for the general interest.

As noted in CiTiP's White Paper on the Data Governance Act,[328] similar initiatives can be found at the national level. One illustration is the Flemish plan for the economic post-Covid relaunch, which includes the creation of a data utility company ('data nutsbedrijf'). This data utility company will act as a neutral third party to support data sharing by public and private entities in the data economy.[329]

The new business model for data intermediation that the DGA proposal introduces may also capture the MobiDataLab cloud prototype. Theoretically, the new legislative framework should facilitate data sharing via the cloud. However, it remains to be seen in practice whether the obligations imposed on such intermediary services hinder that aim.

3.8. Intelligent Transport Systems Directive

The objective of the Intelligent Transport Systems Directive ("ITS Directive"[330]) was to put in place the necessary mechanisms to foster the uptake of ITS services and applications for road transport

[327] Constitutional Court (Conseil Constitutionnel), Decision 79-105 DC, 25th July 1979.
[328] CiTiP's Working Paper on the DGA proposal (n 306).
[329] Vlaamse Veerkracht, Relanceplan Vlaamse Regering, 2020: https://www.vlaanderen.be/publicaties/relanceplan-vlaamse-regering-vlaamse-veerkracht
[330] 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 mode of transport, OJ L 207, 6.8.2010, p. 1–13.

and their interconnections with other modes of transport.[331] This, in turn, was to reduce the air polluting and CO2 emissions from road transport, relieve congestion and improve road safety.[332]

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".[333] ITS applications and services are varied and include journey planners, travel information services, intelligent traffic lights, real-time traffic information, traffic management as well as vehicle safety applications such as the automatic 112 call and advanced cruise control.

3.8.1. Priority areas & Priority actions

The ITS Directive sets a legal framework for a coordinated deployment of ITS in the EU. The Directive identifies four priority areas:

I. Optimal use of road, traffic and travel data;
II. Continuity of traffic and freight management ITS services;
III. ITS road safety and security applications and
IV. Linking the vehicle with the transport infrastructure,[334]

as well as six priority actions[335]:

a) the provision of EU-wide multimodal travel information services,
b) the provision of EU-wide real-time traffic information services,
c) data and procedure for the provision, where possible, of road safety related minimum universal traffic information free of charge for users,
d) the harmonised provision for an interoperable EU-wide eCall,
e) the provision of information services for safe and secure parking places for trucks and commercial vehicles,
f) the provision of reservation services for safe and secure parking places for trucks and commercial vehicles.

Annex I of the Directive provides the specifications and standards for the priority areas and priority actions. Ensuring availability of data and facilitating data sharing holds a prominent position. For example, for the optimal use of road, traffic and travel data (priority area I), the Annex defines the actions that are to be taken to achieve the provision of EU-wide multimodal and real-time traffic

[331] European Commission, 'Support study for the ex-post evaluation of the ITS Directive 2010/40/EU, Final report', July 2019, p.11 https://op.europa.eu/en/publication-detail/-/publication/61597d8c-e99e-11e9-9c4e-01aa75ed71a1, accessed 14 January 2022.
[332] European Parliament, legislative train, https://www.europarl.europa.eu/legislative-train/theme-a-european-green-deal/file-intelligent-transport-systems-directive-review, accessed 14 January 2022.
[333] ITS Directive, Article 4(1).
[334] ITS Directive, Article 2.
[335] ITS Directive, Article 3.

Funded by the European Union

information services and free road safety related minimum universal traffic information, as defined by priority actions a, b and c. Such actions include: 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; and b) the facilitation of cross-border electronic data exchange between the relevant public authorities and stakeholders and the relevant ITS service providers and c) the timely updating of available road and traffic data by the relevant public authorities, stakeholders and service providers.

Similarly, to ensure the continuity of traffic and freight management ITS services (priority area II), the Annex holds that an EU ITS framework architecture needs to be adopted, which would ensure interoperability, continuity of services and multimodality aspects. Cross-border electronic traffic data exchange using standardised information flows or traffic interfaces between different parties will need to be facilitated for the management of passenger and freight transport. The urban ITS architecture and the European ITS architecture need to be made interoperable, integrating information in a single structure and facilitating electronic data exchange.

3.8.2. Proposal for an updated ITS Directive

In its work programme for 2021[336], the Commission announced the revision of the ITS Directive, including a multimodal ticketing initiative. In the inception impact assessment for the revision of the ITS Directive, the Commission has identified three key problem drivers: (a) a lack of interoperability and continuity of applications, systems and services (b) a lack of concertation and effective cooperation among stakeholders and (c) unresolved issues related to the availability and sharing of data supporting ITS services.[337]

The Commission has categorised the issues to be tackled with the revision of the ITS Directive under two broad themes: (i) the need to tackle shortcomings of the current regulatory framework for ITS and (ii) the need to future-proof the ITS Directive to maximise the benefits of emerging ITS solutions, including in the fields of Cooperative ITS (C-ITS), Cooperative, connected and automated mobility (CCAM) and Mobility-as-a-Service (MaaS).[338]

The specific objectives are to (1) increase interoperability and cross-border continuity of ITS applications, systems and services (2) establish effective coordination and monitoring mechanisms

[336] European Commission, Annexes to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2021, 19 October 2021, COM (2020) 690 final.
[337] European Commission, Inception Impact Assessment for the revision of the ITS Directive, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12534-Revision-of-the-Intelligent-Transport-Systems-Directive-_en, accessed 14 January 2022.
[338] For further information, see here a state of play presentation by DG Move (September 2021): https://uvarbox.eu/wp-content/uploads/2021/09/UVARBox_WS3_Presentation-on-revision-of-ITS-Directive-and-DR2015-962.pdf.

between all ITS stakeholders and (3) solve issues related to the availability and sharing of data that support ITS services.[339]

In December 2021, the European Commission issued a proposal for the revision of the ITS Directive.[340] The revision includes an extension in the Directive's scope to better encompass emerging services, such as multimodal information, booking and ticketing services (such as apps to find and book journeys that combine public transport, shared car or bike services), communication between vehicles and infrastructure (to increase safety) and automated mobility. It also mandates the collection of crucial data and the provision of essential services such as real-time information services informing the driver about accidents or obstacles on the road.[341]

The proposal suggests amending the priority areas into the following ones:

I. Information and mobility ITS services;
II. Travel, transport and traffic management ITS services;
III. Road safety and security ITS services;
IV. Cooperative, connected and automated mobility services.

Similarly, to the current ITS Directive, Annex I provides the specifications for the priority areas. Again, reference is made to the availability, accessibility and exchange of data. For example, the specifications for EU-wide multimodal digital mobility services is based, inter alia, on i) the availability and accessibility of existing and accurate multimodal traffic and travel data, used for multimodal digital mobility services to ITS service providers and ii) the facilitation of the electronic data exchange between the relevant public authorities and stakeholders and the relevant ITS service providers across borders.[342] Similarly, the definition of the necessary requirements to make EU-wide road traffic information and navigation services accurate and available across borders to ITS users is based, amongst others, on the availability and accessibility of existing and accurate road and traffic data, including real-time data, used for real-time traffic information to ITS service providers and others stakeholders, and for use in digital maps.[343]

3.8.3. Delegated Regulations

[339] Inception Impact Assessment (n 337).
[340] European Commission, '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', 14 December 2021, 2021/0419 (COD).
[341] European Commission 'Q&A: Intelligent Transport Systems' (14 December 2021), https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6727, accessed 14 January 2022.
[342] Proposal for an updated ITS Directive (n 340), Annex I, section 1.1.1 and 1.1.2.
[343] *Ibid*, Annex I, section 1.2.1.

Based on the ITS Directive, the Commission has introduced legally binding specifications for interoperability and continuity through delegated acts and developed certain necessary standards.

The following specifications have been adopted:

- Delegated Regulation (EU) No 305/2013 on the harmonised provision for an interoperable EU-wide eCall[344] (Priority action (d));
- Delegated Regulation (EU) No 886/2013 supplementing the ITS Directive with regard to data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users[345] (Priority action (c));
- Delegated Regulation (EU) No 885/2013 supplementing the ITS Directive with regard to the provision of information services for safe and secure parking places for trucks and commercial vehicles[346] (Priority action (e));
- Delegated Regulation (EU) 2015/962 supplementing the ITS Directive with regard to the provision of EU-wide real-time traffic information services. The specifications are intended to ensure the accessibility, exchange, re-use and update of road and traffic data by road authorities, road operators for the provision of EU-wide real-time traffic information services. (Priority action (b)) ;
- Delegated Regulation (EU) 2017/1926 supplementing the ITS Directive with regard to the provision of EU-wide multimodal travel information services.[347] The adopted specifications address both enabling conditions, such as accessibility of data, and services and provisions for linking travel information services. (Priority action (a));
- Delegated Regulation on common EU specifications for connected intelligent transport systems (C-ITS) to improve road safety by enabling vehicles to communicate with each other and with the infrastructure. This Regulation did not enter into force because the Council of the European Union objected.

It should be noted however that the actual implementation of the Delegated acts has started only recently and there has only been limited deployment of ITS services.[348]

The present analysis will focus on Delegated Regulation (EU) 2015/962 (“RTTI”) and Delegated Regulation (EU) 2017/1926 (“MMTIS”), as most relevant to the MobiDataLab project. Another

[344] Commission Delegated Regulation (EU) No 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall, OJ L 91, 3.4.2013, p. 1–4.
[345] Commission Delegated Regulation (EU) No 886/2013 of 15 May 2013 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users, OJ L 247, 18.9.2013, p. 6–10.
[346] Commission Delegated Regulation (EU) No 885/2013 of 15 May 2013 supplementing ITS Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of information services for safe and secure parking places for trucks and commercial vehicles, OJ L 247, 18.9.2013, p. 1–5.
[347] 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, 21.10.2017, p. 1–13.
[348] Support study for the ex-post evaluation of the ITS Directive (n 331), p.12.

Funded by the European Union

domain for adoption of specifications is related to open access for ITS services (open in-vehicle platform) through access to in-vehicle data and resources. In its Communication *On the road to automated mobility: An EU strategy for mobility of the future* published on 17 May 2018[349], the Commission announced that it would consider the need for specifications under the ITS Directive for access to (personal and/or non-personal) vehicle data for public authorities' needs, in particular traffic management (which was eventually proposed in the updated specification on EU-wide real-time traffic information services, see further below).[350]

This was confirmed in the updated working programme of the ITS Directive adopted on 11 December 2018[351], which lists also additional activities for 2018-2022. These may lead to new delegated acts (or revision of existing acts) under the ITS Directive covering:

- The possible geographical extension of existing specifications on EU-wide real-time traffic information services including possible additional data types (e.g. urban access restrictions, recharging/refuelling points);
- The possible extension of eCall to other vehicle categories (such as heavy goods vehicles, buses and coaches, powered two-wheelers, and agricultural tractors);
- Interoperable multimodal payment/ticketing; and
- The continuity of traffic and freight management services

In October 2021, the Commission published the draft act (for feedback) for an updated RTTI Delegated Regulation.[352] The proposed act confirms the direction that the Commission wanted to take in its 2018 Communication on an EU strategy for mobility of the future and the updated working programme of the ITS Directive.

Some of the proposed changes that may lead to increased data sharing include:

- Renaming the data categories within the scope of the Delegated Regulation (static data, dynamic road status data and traffic data) to align them better with the data characteristics and specific requirements. Also, new data categories are added: data on infrastructure (e.g. location of recharging and refuelling points and stations), data on regulations and restrictions (e.g. weight/length/width/height restrictions) and data on real-time use of the network (e.g. availability of refuelling points and stations for alternative fuel types);
- Extending the geographical scope of the Delegated Regulation to cover the entire road network, excluding private roads identified by Member States (applicable from January

[349] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'On the road to automated mobility: An EU strategy for mobility of the future', COM/2018/283 final.
[350] Report from the Commission to the European Parliament and the Council, 'Implementation of 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', 8 October 2019, COM(2019) 464 final, p.5.
[351] Commission Decision of 11 December 2018 updating the Working Programme in relation to the actions under Article 6(3) of Directive 2010/40/EU, C (2018) 8264 final and Annex to the Commission Decision.
[352] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12337-Road-traffic-information-services-revised-specifications_en, accessed 14 January 2022.

2028). An intermediate step has been introduced to allow Member States to gradually increase access to data, by asking them to determine a network of primary roads, defined as roads that connect major cities or regions, or both, that are not classified as part of the comprehensive trans-European road network or as a motorway (further information is provided under section 3.8.4.2 below);
- Strengthening the provisions on the re-use of specific data types (further information is provided under section3.8.6 below);
- Improving the re-use of in-vehicle generated data by allowing public authorities to request holders of in-vehicle generated data and service providers to share relevant data types under FRAND conditions. If personal data are used, then their processing will require that the public authorities can point to a lawful basis in line with Article 6(1) of the GDPR.

3.8.4. Data sharing & exchange via National Access Points ("NAPS")

3.8.4.1. Development and deployment of NAPs

In order to facilitate the exchange and re-use of data, Member States are required to set up NAPs. The implementation of NAPs is important to allow data to be shared and is a prerequisite to facilitate the wider development of ITS services.

NAPs have been established in many Member States since the adoption of the Delegated Regulations and although implementation is not yet complete, compared to the baseline scenario (where it was envisaged that only some countries would have set up NAPs), the developments represent significant progress.[353] NAPs may take various forms, such as a database, data warehouse, data marketplace, repository, register, web portal or similar depending on the type of data.[354]

In February 2021, the European ITS Platform published a comprehensive report on NAPs (covering the EU Member States, Norway and the United Kingdom).[355] The report sets out that real-time traffic information is the most implemented NAP.[356] Indeed, currently, 23 countries have a (partly) operational NAP for real-time traffic information. Four other countries are implementing or have concrete plans to implement a NAP. Conversely, the report suggests that the number of NAPs implemented for multimodal travel information services is significantly lower.[357] Sixteen Member

[353] A graphical overview of all active NAPs in Europe can be found here: https://andnet.ro/nap_eueip/.
[354] Delegated Regulation 2017/1926, recital 10.
[355] EU EIP - Annual NAP Report 2020, 26 February 2021, https://its-platform.eu/wp-content/uploads/ITS-Platform/AchievementsDocuments/NAP/EU%20EIP%20-%20National%20Access%20Points%20-%20annual%20report%202020.pdf, accessed 14 January 2022.
[356] *Ibid*, p.27.
[357] *Ibid*, p. 21.

Funded by the European Union

States report a NAP for multi-modal travel information services, either fully or partially operational. In eight other Member States, the NAPs are in progress or there are concrete plans to implement them.

For all NAPs, it is generally the public authorities (including concessionaires) that provide the data. Data from private parties, either as actual data or as weblinks or metadata, are rather limited so far. Although there seems to be an increase in the number of organisations that use the data from the NAP, NAP operators seem to pay little attention to monitoring the use of NAPs. Thus, it is not clear to what extent the Delegated Regulations have resulted in a wider (re)use of the various data sources.

The final report for the support study for the ex-post evaluation of the ITS Directive suggests that there has only been limited usage of the data provided by NAPs, with the possible exception of the services related to the exchange of static road attribute data used for updating digital maps.[358]

Finally, the European ITS Platform report also points out that there is a lack of harmonisation amongst EU Member States regarding the NAPs format[359], the datasets shared as well as the different possibilities for re-use (e.g. free or under a license)[360]. As the state of play of NAPs is not the focus of this analysis, we won't expand further on this here.

3.8.4.2. Data sharing obligations via the NAPs under the Delegated Regulations

The RTTI Delegated Regulation provides that road authorities[361], road operators[362] and real-time traffic information service providers[363] should make the road and traffic data (including data updates),

[358] Support study for the ex-post evaluation of the ITS Directive (n 331), p.8.
[359] EU EIP report (n 359), p. 85.
[360] See the different examples provided by the EU ITS report, pp. 57-73.
[361] Defined as 'any public authority responsible for the planning, control or management of roads falling within its territorial competence'. RTTI Delegated Regulation, Article 2(12).
[362] Defined as 'any public or private entity that is responsible for the maintenance and management of the road'. RTTI Delegated Regulation, Article 2(13).
[363] Defined as 'any public or private provider of a real-time traffic information service, excluding a mere conveyer of information, to users and end-users'. RTTI Delegated Regulation, Article 2(14).

corresponding metadata and information on the quality of the data accessible to other road authorities, road operators, real-time traffic information service providers and digital map producers through a national or common access point.[364] The type of data to be made available are detailed in Annex I. The access point can take the form of a repository, registry, web portal or similar depending on the type of data.[365]

Member States should regroup the existing public and private access points in a single point enabling access to all the types of relevant available data that fall within the scope of these specifications. Member States are free to decide to use the access points established under other delegated acts adopted under the ITS Directive as the national access points for the data falling within the scope of this Regulation.[366]

In order to allow road authorities, road operators, service providers and digital map producers to successfully and cost-efficiently discover and use the relevant data, it is necessary to properly describe the content and structure of this data using appropriate metadata.[367]

Road authorities or road operators and service providers are not obliged to start collecting any data that they are not already collecting or to digitise any data that is not already available in machine readable format.[368] At the same time, the Regulation provides that service providers are not obliged to share any of their data with other service providers, but are free to conclude commercial agreements between themselves for the re-use of relevant data.[369] We understand this provision as justified for data generated by private providers, as in that case, data sharing is primarily driven by bilateral agreements. However, service providers can also be of public nature, subject to the re-use obligations of the Open Data Directive. It is therefore not clear how this provision interacts with the obligations under the Open Data Directive that apply for PSBs and public undertakings **[Identified Gap 10].**

Even more confusingly, the Delegated Regulation provides that the specific terms and conditions applicable for the use or re-use of road and traffic data and real-time traffic information services generated by private service providers are left to the parties concerned, without prejudice to the provisions of Directive 2003/98/EC [i.e. the PSI Directive].[370] The purpose of the reference to the (now called) Open Data Directive is not evident.

A similar reference to the PSI Directive is made with regard to static road data, dynamic road status data and traffic data collected by road authorities and road operators. Indeed, recital 20 of the Delegated Regulation provides "*Private service providers may use static road data, dynamic road status data and traffic data collected by road authorities and road operators as input data for their own real-time traffic information services. The specific terms and conditions applicable for such re-use of these data should be left to the parties concerned without prejudice to the provisions of*

[364] RTTI Delegated Regulation, recital 14, Article 3.
[365] *Ibid*, recital 14.
[366] *Ibid*, recital 14.
[367] *Ibid*, recital 15.
[368] *Ibid*, recital 16.
[369] *Ibid*, recital 17.
[370] *Ibid*, recital 19.

Directive 2003/98/EC" **[Identified Gap 11].** However, road operators are defined as of both public and private nature. Again, the purpose of the reference to the (now called) Open Data Directive is not evident.

Static road data, dynamic road status data and traffic data (and the corresponding metadata, including information on the quality thereof) must be accessible for exchange and re-use by any service provider in the EU on a non-discriminatory basis.[371]

As mentioned above, the proposed act for an updated Delegated Regulation suggests the introduction of some new provisions. In particular, regarding the expansion of the geographical scope of the Delegated Regulation, all the data types listed in the Delegated Regulation on the TEN-T network, other motorways and primary roads must be accessible via the NAPs by 1 January 2025.[372]

Regarding re-use of data in traffic information services, the proposal provides that when a Member State makes traffic regulations, traffic circulation plans or temporary traffic management measures accessible via a NAP, service providers will be obliged to re-use this data in their services to road users, so the information provided via these services is coherent with the data that has been made accessible.[373]

The MMTIS Delegated Regulation follows the same approach about travel data. Transport authorities[374], transport operators[375], infrastructure managers and transport on-demand service providers[376] should make the (static and historic) travel and traffic data, corresponding metadata and information on the quality of the data, including data updates, accessible to users through a NAP.[377]

The type of data to be made accessible through the NAPs are detailed in Annex I of the Delegated Regulation. Static travel and traffic data are deemed essential information for planning purposes during the pre-trip phase, hence the sharing obligation. But for dynamic travel and traffic data, Member States are only encouraged to include these types of data (listed in the Annex) though the NAP **[Identified Gap 12]**.[378] The specific requirements regarding the static and dynamic travel and traffic data of different transport modes should only apply to the data that is actually collected and available in machine-readable format.[379]

The use of static and dynamic data for the purpose of travel information services involves data from different actors across the value chain. In many cases the original data from transport authorities,

---

[371] *Ibid*, Articles 4 (2)(a), 5(2)(a) and 6(2)(a).
[372] Draft act (n 352), section 5.2.
[373] *Ibid*, section 5.3.
[374] Defined as 'any public authority responsible for the traffic management or the planning, control or management of a given transport network or modes of transport, or both, falling within its territorial competence'. MMTIS Delegated Regulation, Article 2(9).
[375] Defined as 'any public or private entity that is responsible for the maintenance and management of the transport service'. MMTIS Delegated Regulation, Article 2(10).
[376] Defined as 'any public or private provider of transport on demand service to users and end-users, including travel and traffic information thereof;'. MMTIS Delegated Regulation, Article 2(18).
[377] MMTIS Delegated Regulation, recital 10, Article 3.
[378] *Ibid*, recital 12.
[379] *Ibid*, recital 14.

Funded by the European Union

transport operators, infrastructure managers or transport on-demand service providers will be used by a travel information service provider. In this instance, the original source, the date and time of the last static update are indicated when used.[380]

The travel and traffic data listed in Annex I and the corresponding metadata including information on the quality must be accessible for exchange and re-use on a non-discriminatory basis and within a time frame that ensures the timely provision of travel information services. They must also be accurate and up to date.[381] The data must be re-used in a neutral manner and without discrimination or bias.[382] Where reusing the static and dynamic travel or traffic data, the source of those data must be indicated. The date and time of the last update of the static data must also be indicated.[383]

The terms and conditions for the use of the traffic and travel data provided through the NAP can be determined through a licence agreement. The Delegated Regulation provides that such conditions must not "*unnecessarily restrict possibilities for re-use or be used to restrict competition*", but impose as few restrictions on re-use as possible.[384] Travel information service providers can also contractually agree the terms and conditions of linking travel information services.[385]

3.8.5. Rules on data protection and privacy

The ITS Directive does not contain specific rules on data protection and privacy. Conversely, it simply indicates that legislation on privacy and data protection must be complied with. In particular, the processing of personal data in the operation of ITS applications and services needs to comply with fundamental rights and freedoms and needs to be in conformity with Directive 95/46/EC35 (also known as the Data Protection Directive, the predecessor of the GDPR) and Directive 2002/58/EC (e-Privacy Directive).[386] Member States need to particularly ensure that personal data are protected against misuse, including unlawful access, alteration or loss, while the use of anonymous data is encouraged to prevent incidents regarding personal data.[387]

Interestingly, similar wording is provided in the proposal for an updated ITS. The proposal suggests that when the specifications adopted concern the processing of traffic, travel or road data that are personal data under the GDPR, the categories of those data need to be laid down and appropriate

[380] *Ibid*, recital 21.
[381] *Ibid*, Article 8(1).
[382] *Ibid*, Article 8(2).
[383] *Ibid*, Article 8(3).
[384] *Ibid*, Article 8(4).
[385] *Ibid*, Article 8(5).
[386] ITS Directive, Article 10(1).
[387] *Ibid*, Article 10(2) and 10(3).

personal data protection needs to be provided. Where appropriate, the use of anonymous data is encouraged.[388]

The protection of personal data was an important consideration when preparing the specifications on C-ITS, as several C-ITS services rely on the transmission of personal data.[389] It was clarified that for C-ITS, the specifications cannot constitute a legal basis for the lawful processing of data. This notwithstanding, the C-ITS specifications set requirements for the pseudonymisation of messages as well as considerations in the recitals that support the protection of personal data.[390]

3.8.5.1. The interface of the ITS Directive & the GDPR

It has been argued that by including provisions on the Data Protection Directive in the ITS Directive, the EU simply wanted to express specific concerns with regard to privacy and data protection in ITS solutions.[391] As will be analysed further below in the opinion of the EDPS, the provisions are however rather superficial and do not seem sufficient to tackle specific concerns arising in ITS solutions **[Identified Gap 13]**.

EDPS Opinion on the ITS Directive

The EDPS had provided an opinion on the original proposal for the Directive back in 2009.[392] The Opinion confirmed that ITS are based on the collection, processing and exchange of a wide variety of data, from public and private sources. The deployment of ITS will rely to a large extent on geo-localisation technologies, such as satellite positioning and contact-less technologies, such as RFID, which will facilitate the provision of a variety of public and/or commercial location-based services (e.g. real-time traffic information, eFreight, eCall, eToll, parking reservation, etc.). Some of the information that will be processed through ITS will be aggregated — such as on traffic, accidents, and opportunities — and does not relate to any individual, while other information will be related to identified or identifiable individuals and therefore qualifies as personal data.[393]

---

[388] Proposal for an updated ITS Directive (n 340), Article 10.
[389] Report from the Commission on the implementation of the ITS Directive (n 350), p.9.
[389] Katleen Janssen, 'The ITS Directive: More Than a Timeframe with Privacy Concerns and a Means for Access to Public Data for Digital Road Maps?'(2012), Comp. Law & Sec. Rev. 28.4, p.423.
[390] Report from the Commission on the implementation of the ITS Directive (n 350), p.9.
[391] *Janssen* (n 400), p.423.
[392] EDPS, 'Opinion of 22 July 2009 on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes', 2010/C 47/02, OJ C 47 of 25 February 2010, 6-15, https://edps.europa.eu/sites/default/files/publication/09-07-22_intelligent_transport_systems_en_0.pdf accessed 14 January 2022.
[393] *Ibid*, para.7.

The EDPS considered as essential that the actions planned for ITS deployment are consistent with the existing legal framework as cited in the Proposal, in particular Directive 95/46/EC on data protection (which was the then applicable framework – now GDPR) and Directive 2002/58/EC on e-privacy.

The EDPS noted that the proposed legal framework is too broad and general to adequately address the privacy and data protection concerns raised by ITS deployment in the Member States. In particular, it was not clear when the performance of ITS services will lead to the collection and processing of personal data, what are the specific purposes for which a data processing occurs, nor what is the legal basis that justifies such processing **[Identified Gap 13a].** Furthermore, the EDPS underlines that the use of location technologies for ITS deployment raises the risk of developing services that are intrusive from a privacy viewpoint if they entail the collection and exchange of personal data. Moreover, the Directive does not clearly set out the roles and responsibilities of the various operators intervening in the chain of ITS deployment, and it is thus difficult to know which operators will be data controllers and will therefore be responsible for compliance with data protection obligations **[Identified Gap 13b]**.[394] This role definition needs to be established prior to any data processing.

The EDPS further stressed the risk that the lack of clarity of the proposed legal framework will create diversity in the implementation of ITS in Europe and that, instead of reducing divergences amongst Member States it will, on the contrary, lead to considerable uncertainty, fragmentation and inconsistencies, due to different levels of data protection in Europe.[395]

While the EU data protection framework changed since 2009 with the adoption of the GDPR to ensure uniform application of data protection rules across Europe, the same concerns can be raised today.

In terms of anonymisation, the EDPS notes that there are concerns on how to make personal data anonymous.[396]

Privacy and data protection & ITS[397]

Many ITS solutions may include the ability to track vehicles.[398] This means that the whereabouts of drivers can be monitored. Such tracking can be perceived as an infringement on the privacy of the driver. Also, ITS solutions rely on the exchange of data between vehicles, infrastructures and the bodies - public or private - operating those. As such data may include specific information regarding the driver of the vehicle, certain data may be considered as personal data under the EU legal framework on data protection. As a result, the collection and processing of such personal data will have to comply with the GDPR.

[394] *Ibid*, para.14.
[395] *Ibid*, para.15.
[396] *Ibid*, para.26.
[397] *Janssen* (n 400), p.420.
[398] This could be as part of calculating the ETA as mentioned in section 3.1.5 or not.

The EDPS Opinion also specifically addressed the issue of location-based services in ITS solutions.[399] The Opinion stated that location technologies are particularly privacy-intrusive as they allow for the tracking of drivers and the collection of a wide variety of data relating to their driving habits. It stressed that the freedom to move around anonymously should be guaranteed and that specific safeguards should be implemented to prevent surveillance of individuals and misuse of such data.

Furthermore, the location data must therefore be collected for explicit and legitimate purposes, on a proper legal ground and must be proportionate to the purposes of those location-based services.[400]To ensure that only the location data necessary for the purposes of their collection are processed, such data should not be collected constantly, but only when necessary for the specified purposes. When the location data is not processed strictly anonymously, the data subject's informed consent should be obtained, thus requiring the data subject to be informed of the purposes of the processing, its duration, possible data transfers, etc.[401]

Furthermore, the processing of location data relating to users of public communications networks or publicly available electronic communication services is strictly regulated in Article 9 of the e-Privacy Directive. It notably requires that processing of location data should be carried out on an anonymous basis, or otherwise upon informed consent of the user. This means that users (data subjects) must, prior to agreeing to the use of a location tool, be provided with appropriate information, including the type of location data processed, the purposes and duration of the processing, and whether the data will be transmitted to a third party.

There must be a simple means, free of charge, for users to temporarily refuse the processing of location data for each connection to the network or for each transmission of a communication. The processing of location data should be strictly limited to persons acting under the authority of the provider of the public communications network or publicly available communication service or of the third party providing the value-added service.[402]

Delegated Regulations

The RTTI Delegated Regulation provides further clarifications in respect of personal data protection. The Delegated Regulation suggests that if personal data are processed, it should be, where possible, irreversibly anonymised and processing should comply with the principles of purpose limitation and data minimisation.[403]

Furthermore, where the information service relies on data collection, including geo-location, data directly from the end-users or through cooperative systems to be established in the future, the end-users should be clearly informed about the collection of such data, the arrangements for data collection and potential tracking, and the periods for which such data will be retained. Appropriate technical measures should be deployed by public and private data collectors such as road operators,

[399] EDPS Opinion on an Action Plan for the Deployment of ITS in Europe (n 403), para. 45.
[400] *Ibid*, para. 46.
[401] *Ibid*, para. 47.
[402] *Ibid*
[403] RTTI Delegated Regulation, recital 9.

service providers and automotive industries to ensure the anonymity of the data received from end-users or their vehicles.[404]

Road authorities, road operators and digital service providers are requested to regularly update their (static road) data and timely correct any inaccuracies in their data, either detected by them or signalled to them by any user and end-users.[405] The specifications of the Delegated Regulation apply regardless of the source of data.[406]

In its opinion on the Delegated Regulation delivered on 17 June 2015, the EDPS endorsed the above provisions.[407] However, in a later opinion, the EDPS stressed its disagreement regarding a change in the Annex. Annex I provide a list of data categories. In its initial draft, the Delegated Regulation used the term "namely" when providing the categories of data. In a corrigendum, the term was changed to "in particular". According to the EDPS, the change of words introduced, changed the meaning of the relevant provisions, which could be interpreted as setting forth an open list of data, thereby allowing the Member States to add new data to the minimum lists outlined in the Delegated Regulation. The EDPS stressed that any new data to be added must comply with the principles of data protection, including the respect of the principle of data minimisation.[408]

The MMTIS Delegated Regulation contains largely similar provisions as the RTTI Delegated Regulation. However, it seems to set different standards in terms of (i) data protection principles[409] and (ii) whether anonymisation is required, or other privacy-preserving mechanisms would suffice[410] **[Identified Gap 14]**. Most importantly, the MMTIS Delegated Regulation deviation from the principle that individuals should not be identified or identifiable if it hinders the purpose of the Regulation.[411]

The differences are indicated in the table below:

Issue	RTTI Delegated Regulation	MMTIS Delegated Regulation 2017/1926
Respect relevant privacy Regulations	Personal data should be processed in accordance with the Union law, as set out, in	The processing of personal data shall be carried out in accordance with EU law on the

[404] *Ibid*, recital 10.
[405] *Ibid*, recital 13, Article 7.
[406] *Ibid*, recital 8.
[407] EDPS, Letter of Giovanni Buttarelli to Ms Violeta Buc, 21 January 2015 regarding the Delegated Regulation to the provision of EU-wide real-time information services, https://edps.europa.eu/sites/default/files/publication/15-01-21_real_time_traffic_information_services_en_1.pdf, accessed 14 January 2022.
[408] EDPS, Letter of Wojciech Rafal Wiewiorowski to Mr Michael Cramer, 17 June 2015 regarding the corrigendum to the Delegated Regulation to the provision of EU-wide real-time traffic information services, https://edps.europa.eu/sites/default/files/publication/15-06-17_its_comments_en.pdf, accessed 14 January 2022.
[409] MMTIS Delegated Regulation, recital 5.
[410] *Ibid*, recitals 5 and 6.
[411] *Ibid*, recital 5, last sentence.

	particular, in Directive 95/46/EC of the European Parliament and of the Council (3) and in Directive 2002/58/EC of the European Parliament and of the Council (4), and with the national legislations thereto.	protection of personal data, in particular Directive 95/46/EC of the European Parliament and of the Council (1) and Directive 2002/58/EC of the European Parliament and of the Council (2), as well as the national implementing measures thereto.
Complying with data protection principles	Processing should comply with the principles of purpose limitation and data minimisation.	Information relating to an identified or identifiable natural person should be processed in ***strict*** compliance with the data minimisation principle and only for the purposes of this Regulation and as long as necessary.
	If the information service is to rely on the collection of data, including geo-location, from the end-users themselves or through cooperative systems in the future, then end-users should be clearly informed about the collection of such data, the arrangements for data collection and potential tracking, and the periods for which such data are kept (transparency principle).	Where the information service relies on the collection of data, including geo-location, end users should be clearly informed about the collection of such data, the arrangements for data collection and potential tracking, and the periods for which such data are kept (transparency principle).
Anonymisation (or other privacy-preserving techniques)	In case the personal data would happen to be processed, it should be, where possible, irreversibly anonymised.	Such data should not allow for the identification of an individual or make an individual identifiable whenever possible ***and when it does not hinder the purpose of this Regulation.***
	Appropriate technical measures should be deployed by public and private data collectors such as road operators, service providers and automotive industries to ensure anonymity	Appropriate technical measures (***including privacy by design and data protection by design features***) should be deployed by public and private data collectors such as transport operators, transport authorities, travel information service providers

	of the data received from end-users or their vehicles.	and digital map producers to ensure ***pseudonymisation*** of the data received from end users.

Table 2: Privacy related provisions of the RTTI and MMTIS Delegated Regulations

In its opinion on the Delegated Regulation delivered on 22 August 2017, the EDPS welcomed the references to the principles of privacy by design and privacy by default but stressed that these principles do not only include technical measures but also organisational ones.

The same remark applies regarding pseudonymisation, which also implies technical and organisational measures.[412] The final text, however, does not include references to organisational measures. Furthermore, the EDPS clarified that the use of pseudonymisation is merely a means to achieve some of the obligations of the data controller under the GDPR. Since pseudonymised data are still considered as personal data because they remain identifiable, data protection principles apply to them as well (contrary to anonymous data). The EDPS suggested clarifying that the mere use of pseudonymised data does not exempt the controller from respecting the provisions of data protection law.[413] But this was not added to the final text.

Transport authorities, transport operators, infrastructure managers and transport on-demand service providers are requested to regularly update their (travel and traffic) data and timely correct any inaccuracies in their data, either detected by them or signalled to them by any user and end-users.[414] The specifications of the Delegated Regulation apply to all transport modes, including transport on-demand (e.g. car-share, bike-hire) and personal based (e.g. car, bicycle).[415]

3.8.6. Rules on the re-use of information

Similarly, to the privacy provisions, the ITS Directive does not introduce new rules on the re-use of information, but simply refers to the PSI Directive. Recital 14 to the Directive provides that the "*deployment and use of ITS applications and services, and notably traffic and travel information services, will entail the processing and use of road, traffic and travel data forming part of documents*

[412] EDPS, Letter of Leonardo Cervera-Navas to Mr Herald Ruijters with regard to the provision of EU-wide multimodal travel information services, https://edps.europa.eu/sites/default/files/publication/17-08-22_travel_information_services_en_0.pdf accessed 14 January 2022.
[413] *Ibid*
[414] MMTIS Delegated Regulation, recital 18, Article 6.
[415] *Ibid*, recital 8.

held by public sector bodies of the Member States" and should therefore comply with the principles on the re-use of public sector information.[416]

In terms of definitions, road data is defined as "data on road infrastructure characteristics, including fixed traffic signs or their regulatory safety attributes"[417], traffic data as "historic and real-time data on road traffic characteristics"[418] and travel data as "basic data such as public transport timetables and tariffs, necessary to provide multimodal travel information before and during the trip to facilitate travel planning, booking and adaptation"[419].

3.8.6.1. The interface of the ITS & Open Data Directive

Annex I of the ITS Directive requires that specifications for Priority area I (optimal use of road, traffic and travel data) are based on the availability and accessibility of existing and accurate road and real-time traffic data to ITS service providers for a number of purposes, for example, use in multimodal travel information, for real-time information or for digital maps.

As mentioned above, the RTTI Delegated Regulation provides that road authorities, road operators and real-time traffic information service providers should make the road and traffic data (including data updates), corresponding metadata and information on the quality of the data accessible to other road authorities, road operators, real-time traffic information service providers and digital map producers through a NAP.

The MMTIS Delegated Regulation follows the same approach about travel data. Transport authorities, transport operators, infrastructure managers and transport on-demand service providers should make the (static and historic) travel and traffic data, corresponding metadata and information on the quality of the data, including data updates, accessible to users through a NAP.

It seems that the ITS Directive, by requiring to make all road, traffic and travel data accessible has a broader scope than the Open Data Directive, which does not contain obligations on availability or exchange of data, but only on re-use.[420] Under the Open Data Directive, accessibility is governed by national law. While the two pieces of legislation have different aims – the ITS Directive primarily targeting accessibility of data, whereas the Open Data Directive being primarily a legislation on open data, the exact relationship between the two is not entirely clear **[Identified Gap 15].** The terms used such as '*availability*', '*accessibility*' and '*re-use*' – that may seem like similar or complementary notions, but each have their own distinct meaning – may contribute to the confusion about what is in fact required under each legislation.

[416] ITS Directive, Article 10(5).
[417] *Ibid*, Article 4(14).
[418] *Ibid*, Article 4(15).
[419] *Ibid*, Article 4(16).
[420] *Janssen* (n 400), p.426.

Funded by the European Union

3.8.7. Liability

Provisions related to liability have been included in specifications as relevant, in accordance with Article 11 of the ITS Directive.

Liability being also an important element for C-ITS, due consideration has been given to reference provisions for Community harmonisation legislation for products set out in Annex I of Decision No 768/2008/EC37 when preparing the specifications. These are not strictly related to liability, but they detail the obligations and responsibilities of C-ITS station manufacturers.[421]

3.8.8. Short assessment of impact for MobiDataLab

The ITS Directive and its Delegated Regulations are considered as the cornerstone for the deployment of ITS systems in the EU. However, the scope of the ITS Directive and part of the Delegated Regulations as presented above are still evolving, meaning that certain gaps identified at the time of drafting may be remedied with the revision of the framework.

In terms of the interface of the ITS Directive with the GDPR, it should be noted that the RTTI Delegated Regulation predates the entry into force of the GDPR. Since 2018, the GDPR has set a uniform (and high) standard for personal data protection, so even if the rules in the ITS Directive and the Delegated Regulations are contradictory or not clear enough, transport providers should be able to rely on the GDPR itself for guidance. However, the GDPR rules are rather generic and there is no guidance on the application of the GDPR for ITS applications or within the mobility context. So far the only guidance available at the EU level is i) the Article 29 Working Party Opinion on the Recent Developments on the Internet of Things[422], which however focuses on issues unrelated to mobility (wearable computing, applications carried by individuals who want to record information about their own habits and lifestyles and home automation applications) and ii) the EDPB Guidance in the context of connected vehicles and mobility-related applications[423] which also analyses three case studies (“pay as you drive” insurance contracts, the eCall, accidentology studies and tackling automotive theft).

Concerning the interface of the ITS and the Open Data Directive, the Open Data Directive particularly focuses on high-value datasets, which include mobility data (to be defined further through an implementing Act). In an impact assessment study on the list of high-value datasets to be made available by the Member States under the Open Data Directive, Deloitte sets out the datasets

[421] Report from the Commission on the implementation of the ITS Directive (n 350), p.9
[422] Article 29 Data Protection Working Party, ‘Opinion 8/2014 on the Recent Developments on the Internet of Things’, 16 September 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, accessed 14 January 2022.
[423] EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications (n 35).

Funded by the European Union

covered by the ITS Directive and the datasets in scope for the analysis for the PSI mobility thematic area.[424]

A significant number of the datasets covered by the ITS Delegated Regulations are expected to be considered as public sector information and are already covered in NAPs.[425] Article 9 of the new Open Data Directive sets out practical arrangements to facilitate finding data. Examples include the development of tools and online portals that make it easier for users to find and re-use data and appropriately licensed metadata. Existing EU policies and NAP funded projects have made progress in portals, increasing data discoverability, metadata mapping and harmonised metadata catalogues, and it is anticipated this new directive will build from these.[426]

[424] Deloitte study (n 226), pages 76-79.
[425] EU EIP report (n 359), p.4.
[426] *Ibid*

4. Legal and regulatory data sharing gap analysis case study: Mobility as a Service

This section is inspired by MobiDataLab's use case on Mobility as a Service as analysed in deliverable D2.9. As mentioned in D2.9, mobility takes new forms, with new behaviours and new services –especially in urban areas. Mobility becomes a mixture of different modes of transport, both individual transport solutions (either cars, bicycles, e-scooters, etc.) and new forms of public transport like ride pooling and ridesharing. In order to motivate users to use and mix these different modes of transport, it is important to offer them a complete end to end solution that will not only allow them to plan their journey, but also to book and pay their ticket for the complete journey. Given the importance of this use case, we have decided to also examine it from a legal perspective.

4.1. What is Mobility as a Service?

Mobility as a Service ("MaaS") allows users to plan, book and pay for multiple types of transport services using a single interface (typically a mobile application). The objective is to offer to MaaS users mobility solutions that are ideally suited to their individual needs, while letting the MaaS operator the opportunity to promote alternative transport modes that users may not have considered otherwise.

Core components of a MaaS platform are:

- **Multi-modal / multi-criteria journey planning**: all available transport modes within the considered area shall be taken into account (bus, train, tram, car, taxi, bike, ride sharing, free floating, walking …) to propose the best journeys, depending on several criteria (time to destination, number of changes, accessibility, cost …) and taking into account real time information (car traffic, network disruptions, equipment availability …);
- **Booking and payment**: once a user has selected his/her preferred journey, he/she will be able to book and pay for the whole journey using a centralised account, even when using different transport modes. How the user will pay depends of the payment models set by the MaaS operator (pay-as-you-go or monthly subscription fee);
- **Ticketing**: once the journey has been paid, the user will receive tickets valid for his/her whole journey. Typically, the user's smartphone will store a m-ticket, to be used with all considered transport modes. Alternatively, a transport card could be used in the case of monthly subscription fee payment models.

From the user's point of view, MaaS serves as a facilitator to go from point A to point B, using a single interface that will present the best options available (even ones the user may not be aware of), door to door, and without having the burden to book and pay for different transport services using different interfaces.

Funded by the European Union

The MaaS Alliance describes MaaS as: "*the integration of various forms of transport services into a single mobility service accessible on demand. To meet a customer's request, a MaaS operator facilitates a diverse menu of transport options, be they public transport, ride-, car-, or bike-sharing, taxi or car rental/lease, or a combination thereof. For the user, MaaS can offer added value through use of a single application to provide access to mobility, with a single payment channel instead of multiple ticketing and payment operations. For its users, MaaS should be the best value proposition by helping them meet their mobility needs and solve the inconvenient parts of individual journeys and the entire system of mobility services*".[427]

From a legal perspective, the only legal definition of integrated mobility services currently available at EU level can be found in the 2017 Finnish Act on Transport Services (see below for further information), which deals specifically with MaaS platform providers. According to the Act, integrated mobility services refer to the "*formation of travel chains and other service packages in return for remuneration by combining the mobility services offered by different service providers, excluding travel packages or combined travel arrangements falling within the scope of the Act on Travel Service Combinations*".[428] Adopting an EU-wide definition of MaaS that sets out the characteristics of the service would allow for coherence in the deployment of the service across the EU and more predictability on the legal issues that need to be tackled to make MaaS a reality **[Identified Gap 1].**

4.2. The main actors involved

The MaaS main operator could be a public transport operator ("PTO"), offering services under the governance of a public transport authority ("PTA"), or a private company. In both cases, the main operator needs to enter into an agreement with every transport operator (public or private) as they choose to be integrated into the MaaS platform.

When the MaaS platform is operated by PTOs, it will usually be seen as a way to promote the options for public transport or alternative transport modes, compared to an individual car. In addition, the MaaS operator may improve its own operations by leveraging on data collected under the MaaS platform.

The MobiDataLab Transport Cloud may play a very important role to help MaaS platforms to achieve these goals. First of all, MaaS operators could connect to the Transport Cloud to retrieve some or all datasets that would allow them to compute multi-modal and multi-criteria journeys within the considered area. Alternatively, the future Transport Cloud may propose its own journey planning system.

[427] MaaS Alliance, "What is MaaS?", https://maas-alliance.eu/homepage/what-is-maas/. Accessed 14 January 2022.
[428] Björn Lundqvist and Erion Murati, 'Collaborative Platforms and Data Pools for Smart Urban Societies and Mobility as a Service from a Competition Law Perspective' in Michèle Finck, Matthias Lamping, Valentina Moscon, Heiko Richter (eds) *Smart Urban Mobility, Law, Regulation and Policy* (Springer 2020), p.192.

In such case, MaaS operators could use the Transport Cloud journey planning capability or combine it with their own journey planning system. In addition, MaaS operators could upload their own datasets to the Transport Cloud, and use Transport Cloud services to enrich, consolidate and analyse these datasets. For example: what are the most common journeys within a particular area, and at which times, what are the most popular transport modes, how many journeys are actually booked and paid for, etc. Using this information, prediction models could be devised, for example to understand which areas may be difficult to reach or which transport services may be overcrowded at a certain time.

4.3. The data types used in MaaS

While offering services, MaaS gathers data from hundreds of billions of public and private transport journeys per year. There are multiple sources of data coming into play, including private, passive, community and self-quantification data. These data are typically held by governments, governmental organisations and local communities and include sensor, transport data and energy use figures. Private data may include proprietary information held by private firms or individuals.[429]

Looking at the different data categories in more detail:

a) Public transport data (provided by PTOs)*:*
- Static network description (lines, stop points etc): although static, the network description may be updated frequently***;***
- Real-time data (network disruptions, next departures, vehicle occupancy, vehicle position …): this information is updated continuously and will be refreshed very frequently (e.g. every 30 seconds)***;***
- Road traffic: when made available by PTO or PTA.

b) Geographical data*:*
- Cartography: could be provided by Open Street Map or other actors (e.g. Google Maps)***;***
- Addresses: national addresses databases are usually openly available (e.g. BANO in France)***;***
- Points of interests: could be provided by Open Street Map (user contributions), by MaaS main operator or by MaaS integrated transport operators***.***

c) Other transport data (provided by private transport operators)*:*
- Free floating, ride sharing and road traffic data***.***

d) Booking and payment data:
- Static fares: a fare table provided by transport operators, or by the MaaS main operator if it has an agreement with transport operators to sell transport tickets to a different price. The price of each transport section should be displayed;

[429] *Finck, Lamping, Moscon, Richter* (n 440).

Funded by the European Union

- Dynamic fares: the fare is calculated by the MaaS operator, eventually using transport operators own fare systems, depending on various parameters (departure date, expected occupancy …). The price could be displayed only for the whole journey.

e) Ticketing data:

- e-Tickets: provided by transport operators to the MaaS operator, that in turn will create a single e-ticket or m-ticket for MaaS user.

f) User input data:

- User location: provided by the MaaS user, if he/she accepts to share his current location;
- Journey planning: preferred departures and arrivals, preferred transport modes, etc.;
- Personal details such as name, email, postal address (required for registration, booking and/or payment).

An illustration of the MaaS ecosystem can be found in the figure below:

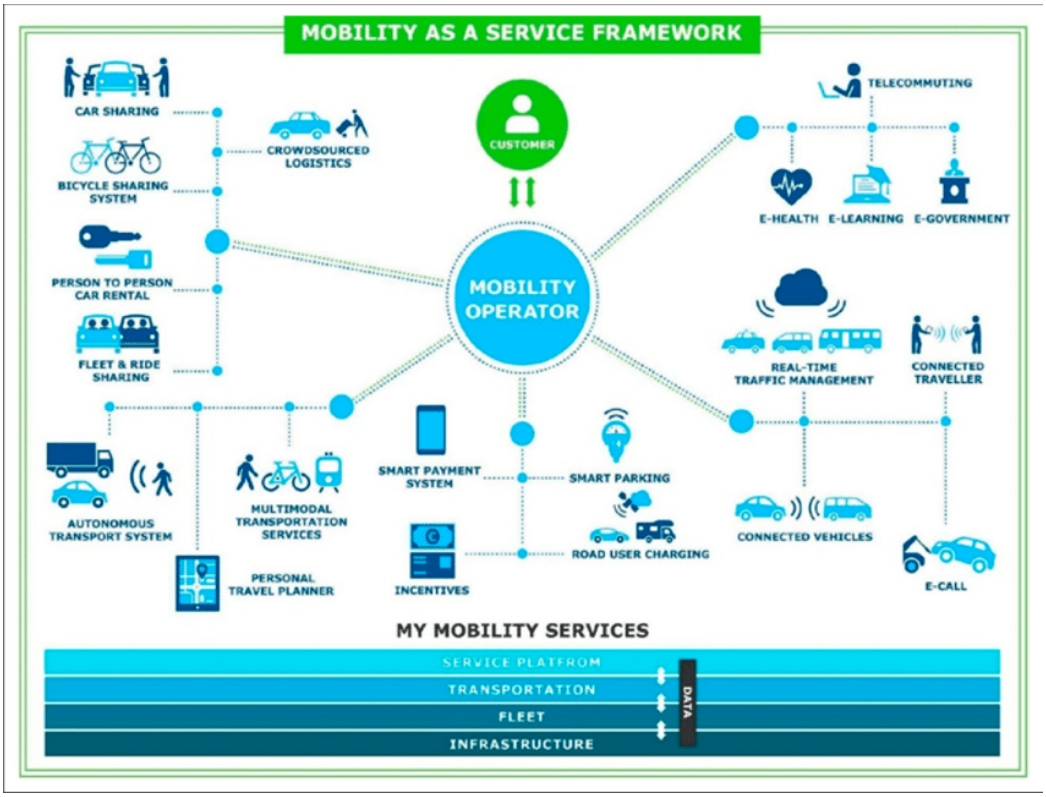

Figure 6: The Mobility as a Service framework (Reproduced from Kivimäki et al.)[430]

[430] https://www.researchgate.net/publication/338156972_State_of_the_Art_of_Mobility_as_a_Service_MaaS_Ecosystems_and_Architectures-

4.4. Legal and regulatory gap analysis

4.4.1. GDPR

User data that are collected by the MaaS operator, while critical to the development of MaaS, may raise privacy concerns as they could allow individuals to be identified by creating detailed traces of their mobility behaviour. Such data is regarded as personal data under the GDPR while the collection will qualify as processing. Consequently, the actions of MaaS operators would fall within the material scope of the GDPR and MaaS operators (assuming they determine the means and purposes of processing) would need to abide by the GDPR provisions as analysed under section 3.1. This constitutes a barrier to data sharing.

There is further a lack of understanding of the different actors that participate in a MaaS ecosystem and their precise role. This is crucial so as to define their obligations under the GDPR and ensure lawful data sharing **[Identified Gap 2].**

4.4.2. Competition Law

4.4.2.1. Article 101 TFEU considerations

MaaS is a concept akin to a data pool. As mentioned in section 3.5.1.2 above, data pooling can raise anticompetitive concerns by facilitating collusion and anticompetitive foreclosure through information exchange. Indeed, the combination of data in the MaaS pool – strategic competitive information such as routes, timetables, stops, customer preferences and history and fares, might be questionable from a competition law perspective.[431]

In their report "*Competition policy for the digital era*", Cremer and others suggest that the following factors will be relevant for the assessment of data sharing and data pooling agreements:[432]

- The type of data that is being pooled, e.g. whether it is aggregated or individual-level data;
- In the case where individual-level data is being pooled, even if the data provider remains anonymous, whether the data coming from two different firms is grouped under the same pseudonym;
- Whether the individual-level data are being pooled but used anonymously;
- Whether technical measures are taken to limit and/or control the use of data.

An_Overview_of_and_a_Definition_Ecosystem_and_System_Architecture_for_Electric_Mobility_as_a_Service_eMaaS, accessed 14 January 2022.

[431] *Lundqvist, Murati* (n 440), p.206.

[432] Cremer, Montjoye (n 129), p. 93.

Funded by the European Union

The case of *Eturas*, also mentioned in the same section, highlights that collusion can take place not necessarily via human coordination, but via automated means. Applying the facts of the case to the mobility scenario, a message by the MaaS platform operator to the "participating" transport operators to set or cap ticket fare prices could turn out to be problematic from a competition law perspective (assuming the transport operators are actual or potential competitors), if they did not distance themselves from it by objecting to the communications or systematically setting prices that disregard the rule.

Platform operators and administrators should therefore take particular care not to include anticompetitive restrictions in their terms and conditions to reduce the risk of liability for facilitating collusion between users. Indeed, in a MaaS collaboration, different transport providers should preferably set their own prices unilaterally while the system administrator (the MaaS platform provider) should provide the algorithm for calculating the joint price.[433]

However, a platform that is able to provide services which the individual providers cannot provide by themselves may fall outside the scope of Article 101 (1) TFEU or at least be available for an exemption under Article 101(3) TFEU. Indeed, pools containing information for the development of new transport services could be regarded as 'harmless' technical development cooperation's and considered as an analogy of R&D collaborations, standard-setting efforts, or to some extent, patent pools. The MaaS concept can lead to innovations for smart city transport.[434]

4.4.2.2. Article 102 TFEU considerations

Dominance of the MaaS operator

The MaaS model is designed on pooling of data and as a data-driven business model it can trigger network effects (i.e. the more users make use of one application providing the MaaS service the more value it gains) and potentially cause the market to tip in favour of one dominant platform.[435] The dominant MaaS platform may exclude competition by denying entry to the platform for suppliers, or its provider can use the platform to vertically integrate or exclude specific suppliers of transport services on the downstream transport markets.[436]

Refusal to supply

One aspect more pertinent to data sharing is the case where the MaaS operator would like to access and use data of another transport operator. Normally the two companies would enter into negotiations privately, but it may be the case that the (private) transport operator refuses to provide the data. Competition law could provide a solution by imposing a data access obligation, if it could be considered that the transport operator – who must hold a dominant position in the relevant market

[433] *Lundqvist, Murati* (n 440), p.213.
[434] *Ibid*, p.206.
[435] *Ibid*, p.205.
[436] *Ibid*, p.207.

– abused that dominant position by refusing to share data that is 'essential' or 'indispensable' for the other operator to develop the MaaS service.

In principle, companies are free to choose their contractual counterparties (generally known as contractual freedom). However, a dominant undertaking may be prohibited, in the absence of objective justification, to refuse to grant access to 'essential facilities' on a non-discriminatory basis to new customers, at least in circumstances where a refusal would eliminate effective competition on the downstream market.[437]

The meaning of *essential facility* or *indispensability* is a fact-specific issue that depends upon the presence of technical, legal or even economic obstacles preventing the would-be user of the 'facilities' from competing on the relevant market.[438] The Advocate General Jacobs has provided an explanation of what could constitute an essential facility in *Bronner*[439]:

"*An essential facility can be a product such as a raw material or a service, including provision of access to a place such as a harbour or airport or to a distribution system such as a telecommunications network. In many cases the relationship is vertical in the sense that the dominant undertaking reserves the product or service to, or discriminates in favour of, its own downstream operation at the expense of competitors on the downstream market. It may however also be horizontal in the sense of tying sales of related but distinct products or service*".

Under EU competition law, the 'essential facilities doctrine' has been developed in a long line of cases dealing with access to physical infrastructure as well as licensing of intellectual property rights. However, to our knowledge, there is no case at EU level (yet) that has led to the obligation to provide access to data.[440] Several cases at the EU level can, however, be interpreted as relating to information assets more broadly. In *Magill*[441], the ECJ concluded that the refusal by three Irish broadcasting companies to provide the publishing company Magill with a copyright license for the weekly listings of their television programmes was abusive. In *IMS Health*, the ECJ found an abuse in the context of a refusal of IMS, a company active in providing data on regional sales of pharmaceutical products in Germany, to grant a license to its competitor NDC for the use of the copyrighted brick structure that IMS had developed and that had become a de facto standard. In *Microsoft*, the General Court held Microsoft's refusal to provide rivals with interoperability information necessary for non-Microsoft work group server operating systems to communicate with Microsoft's dominant client PC operating system Windows to be abusive.[442]

But the CJEU in its case law (*Magill, Bronner, IMS Health, Microsoft*) has set strict criteria for refusal to supply to be considered an abuse of a dominant position:

- The input or assets is indispensable for producing the downstream service (where the dominant firm is also active);
- The denial of access leads to exclusion of effective competition in the downstream market,

[437] *Bellamy & Child* (n 145), para. 10.149.
[438] *Ibid*
[439] Case C-7/97, *Bronner*, Opinion of Advocate General Jacobs, 28 May 1998, para.50.
[440] *Van Gorp N., de Bijl P., Graef I., Molnar G., Peeters R. & Regeczi D.* (n 139), p. 38.
[441] Joined cases C-241/91 and C-242/91, *Magill* [1995], ECLI:EU:C:1995:98.
[442] *Van Gorp N., de Bijl P., Graef I., Molnar G., Peeters R. & Regeczi D.* (n 139), p. 38.

Funded by the European Union

- And the dominant firm does not have an objective justification for denying access.[443]

Given the high threshold set by the CJEU, it becomes challenging for the MaaS operator to find recourse to competition law so as to oblige a transport operator to share their data. At the same time, it's not clear if the essential facilities doctrine and the subsequent obligation to share data could apply in a MaaS context (or any other data intensive activity) and if so, how **[Identified Gap 3]**.[444]

4.5. National examples

Finnish legislation on MaaS[445]

Finland is the first country to use legislation in such a way as to mesh together all different transport modes from taxis and city trams to long-distance trains and bike shares so that users can get around and transport goods from A to B as frictionlessly as possible. The Finnish Act on Transport Services regards the entire transport system as a single entity.

It requires all transport service providers to open up their essential data, such as information on routes, stops, timetables, prices, availability and accessibility in a machine-readable form via open interfaces. By sharing data, service providers can use their transportation fleet more effectively in moving goods and passengers.

The Act also requires transport service providers to have compatible systems and grant each other access to their ticket and payment system interfaces. The government has given service providers an incentive to do this by making interoperability a criterion for public procurement. Service providers can sell customers tickets for other transport modes—a train vendor can sell you a train as well as the bus ticket you need to get to your destination from the train station, for instance. This makes going from A to B as easy and user-friendly as possible.

In keeping with the data regulation in the Act, mobility service providers have opened up a large number of interfaces for exchanging essential data and the opening of sales interfaces has also started.

The French mobility orientation law (La loi d'orientation des mobilités – "LOM")[446]

[443] *Ibid*
[444] *Ibid*, p.39-41.
[445] When the going gets easier, Harri Pursiainen, Permanent Secretary, Ministry of Transport and Communications of Finland, 2 March 2020, OECD library, https://www.oecd-ilibrary.org/docserver/34521141-en.pdf?expires=1637682530&id=id&accname=guest&checksum=B181F99FB3D2F7BF81AA6B2EF93A3852 , accessed 14 January 2022.
[446] https://futuramobility.org/en/lets-talk-lom-french-mobility-orientation-law/, accessed 14 January 2022.

France also adopted a new legal framework to enhance the use of new mobility means. The LOM aims, amongst others, to accelerate the opening up of data and development of digital services. The LOM affirms, steps up, and facilitates the move towards open data. All the organising authorities ("AOs") ('métropoles', community municipalities or intermunicipalities) are required to open up data on all existing modes.

The Regions are charged with coordinating the opening up of data and the transport regulatory authority (ART) with monitoring and settling disputes. Data must be disseminated either statically (a file) or dynamically via an API on the NAP, transport.data.gouv.fr. This NAP collects the data and shares it with re-users.

Moreover, with the LOM, *AO*s must now ensure MaaS exists to facilitate intermodality across all transport modes. They are also required to provide a digital interface accessible to parties offering MaaS services. Also new in the *LOM* is the definition of two legal categories of digital services for information, reservations and selling mobility services:
– the 'contact platform', which simply allows parties to deliver their own fare products;
– the 'distributor', which can, if the AO agrees, set the price a) for selling its own fare products and b) for reselling those of the transport operator. This means the 'distributor' could even create a different price.

SNCF announced the operation of SNCF Connect as of January 2022, an application which will not only be a real-time travel information services provider, journey planner and ticketing platform, but will also integrate intermodal door-to-door journey comparison including the companies' own services (train) but also green (bicycle, kick-scooter) and shared (taxi, ride-sharing, carpooling) mobility offerings. CO2 emissions of the suggested journeys will also be included.[447]

The obligation stipulated in the Finnish and French Acts to share or make data accessible originates from the ITS Delegated Regulation 1926/2017 on multimodal travel information services. As mentioned under section 3.10.3, the Regulation requires private and public transport operators to make travel and traffic data accessible for re-use through the NAP. However, access to fare data, as granted by the Finnish and French mobility laws is not envisioned by the Delegated Regulation **[Identified Gap 4].** Finally, it should be noted that the Commission has announced a "Multimodal Digital Mobility Services" initiative which aims at tackling the current legal and market fragmentation and ensure an increase in the deployment and operational use of digital mobility services within and across passenger transport modes, with the intention to significantly improve multimodality. The proposal seeks in particular to establish frameworks for commercial agreements for services re-selling mobility products as well as for agreements on journey continuation.[448] Consequently, gaps n.1 and 4 identified above may be addressed in this initiative.

[447] https://www.sncf.com/sites/default/files/press_release/CP_NR_SNCF_Connect_19112021.pdf, accessed 14 January 2022.
[448] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13133-Multimodal-digital-mobility-services_en, accessed 14 January 2022.

5. Conclusions and next steps

Data sharing relies on the existence and availability of data. Data are heterogenous, even in the mobility sector. For example, we have referred in our analysis to (real-time and historic) traffic data, passenger data, geolocation data or machine generated data (in the context of connected cars). This heterogeneity can also be reflected in the legal environment, as there is not one legislation governing data. Conversely, our analysis has demonstrated the existence of a complex and fragmented legal landscape regulating data, and by extension, data sharing. This is mainly caused by the lack of, firstly, a uniform legal definition of data and secondly, of a commonly accepted legal status of data. Indeed, a significant part of the data do not have a default legal status as intangible assets.

Most of the legal regimes analysed in Sections 3 and 4 were not designed with the needs of the data economy or the specificities of data sharing in mind. This legal gap is often bridged through contractual arrangements imposed by the party which has physical control over the data. In the current situation, the lack of a general status or access regime for data significantly limits data sharing and further shifts the balance of power in favour of those who develop or operate the systems and thus control data. At the same time, given the many potentially applicable frameworks, ensuring the legal validity of data contracts can be a challenge. It is usually difficult, costly and time-consuming to know in advance whether any data contract could survive the legal challenges stemming for example, from the application of personal data protection legislation.

The DGA proposal proposed by the Commission in 2020 is the first attempt towards creating a data-specific law. Data governance mechanisms proposed by the EC are expected to enable both individuals and companies to enter the data economy and share 'their' data without being unfairly treated (*i.e.* by the Big Tech companies). The variety of data governance mechanisms is expected to adapt to the various contexts and expectations of stakeholders concerning data. By providing them with a legal framework, the DGA proposal recognizes the long-standing need for laws to support (data) resource exchange, and especially to support data markets.

Despite the Commission's push on data-specific legislation, the reality remains that several regulatory gaps exist today, imposing barriers on data sharing. Our analysis has shown that legislative provisions are not streamlined to ensure consistency and particular challenges arise when we look at the interface of two different pieces of legislation, for example, the GDPR and the ITS Directive, or the Open Data and the ITS Directive.

The picture becomes even more complicated if we consider that during the time of drafting of this report, a wave of legislative interventions has taken place (e.g. the DSA, DMA proposal, the updated ITS Directive), while a number of others are foreseen for 2022 or later (e.g. initiative on Multimodal Digital Mobility Services, introduction of new or update of current delegated acts under the ITS Directive, guidance on high-value datasets under the Open Data Directive). This means that the current legal landscape on data sharing is constantly changing, which in turn makes providing guidance for legal aspects arising in the MobiDataLab project equally challenging. KU Leuven will continue its research as well as monitoring the legislative developments. A more targeted and in-depth analysis on the legislative gaps identified will follow in 2023.

6. Annexes

GDPR	Competition Law	Open Data and Public Sector Information Directive	Regulation on the free flow of non-personal data	Proposal for a Data Governance Act	ITS Directive & Delegated Regulations
How to ensure compatibility with the GDPR while benefiting from the information data can provide (e.g. when identified or pseudonymous data may be necessary to understand mobility patterns) [Gap n.1]	Defining 'data markets' to assess dominance (and establish potential abuses) [Gap n.5]	Lack of guidance on the aspect of protection of personal data under PSI (e.g. in terms of limits to anonymisation, opportunity to carry out data protection impact assessments). [Gap n.6]	Difficulty to qualify data as 'non-personal' (which may result in an unnecessary application of the GDPR) [Gap n.8].	Risk of overlap in the scope of application of the DGA proposal with the Open Data Directive which results in a lack of clarity on which obligation(s) is(are) concretely applicable to Public Sector Bodies [Gap n.9]	Lack of clarity on the interface with the Open Data and Public Sector Directive, particularly following the 2019 revision [Gaps n.10, 11, 15]
Identifying the legal basis under which data processing can take place if consent is withdrawn or rendered invalid [Gap n.2]		Divergence of implementation of the 2013 PSI Directive in EU Member States which may also lead to divergence of the 2019 Open Data Directive [Gap n.7]			No obligation under the Delegated Regulation 2017/1926 on multimodal travel information services to make dynamic travel and traffic data accessible though the National Access Point [Gap 12]
Potential difficulty in distinguishing between what constitutes personal and what non-personal data [Gap n.3]					Lack of clarity on the application of the GDPR [Gap n. 13] • Unclear when the performance of ITS services will lead to the collection and processing of personal data, what are the specific purposes for which a data processing occurs, nor what is the legal basis that justifies such processing [Gap n.13a]

					• The Directive does not clearly set out the roles and responsibilities of the various operators intervening in the chain of ITS deployment, and it is thus difficult to know which operators will be data controllers and will therefore be responsible for compliance with data protection obligations [Gap n.13b]
Characterising the role of actors in the data stakeholder framework under the GDPR [Gap n.4]					Different standards set by Delegated Regulation 2017/1926 on the provision of EU-wide multimodal travel information services and Delegated Regulation 2015/962 the provision of EU-wide real-time traffic information services in terms of (i) data protection principles and (ii) whether anonymisation is required, or other privacy preserving mechanisms would suffice [Gap n.14]

Table 3: Horizontal legal and regulatory gaps matrix

MaaS – Legal and regulatory gaps matrix
Lack of EU wide definition of MaaS that sets out the characteristics of the service. A uniform definition would allow for coherence in the deployment of the service across the EU and more predictability on the legal issues that need to be tackled to make MaaS a reality [Gap n.1]
Lack of understanding of the different actors that participate in a MaaS ecosystem and their precise role. This is crucial to define their obligations under the GDPR and ensure lawful data sharing/pooling [Gap n.2]
Lack of clarity on whether the “essential facilities doctrine” under competition law could be to applicable to oblige private operators to share data – and if so, how [Gap n.3].
The ITS Delegated Regulations do not include in the scope of data that need to be made available via NAPs fare data [Gap n.4]

Table 4: Maas – Legal and regulatory gaps matrix

MOBIDATALAB

Labs for prototyping future mobility data sharing solutions in the cloud

MobiDataLab consortium

The consortium of MobiDataLab consists of 10 partners with multidisciplinary and complementary competencies. This includes leading universities, networks and industry sector specialists.

@MobiDataLab
#MobiDataLab

https://www.linkedin.com/company/mobidatalab

For further information please visit **www.mobidatalab.eu**

MobiDataLab is co-funded by the EU under the H2020 Research and Innovation Programme (grant agreement No 101006879).