MOBILITY SERVICES ENHANCED BY GALILEO & BLOCKCHAIN

D.6.5 Ethical and Regulatory Aspects

Work Package No.	6
Work Package Title	Business and Regulatory Aspects
Task No.	
Task Title	
Dissemination level[1]	PU
Main Author(s)	Laurens Dauwe (Osborne Clarke) Benjamin Docquir (Osborne Clarke) Margo Cornette (Osborne Clarke)
File Name	*Molière – D6.5 – Legal and Ethics Report_v0.1.docx*
Online resource	

European Global Navigation Satellite Systems Agency

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004275

[1] PU = Public | CO = Confidential, only for members of the consortium (including the Commission) | CL = Classified, information as referred to in Commission Decision 2001/844/EC

Revision and history sheet

Version history			
Version	***Date***	***Main author(s)***	***Summary of changes***
v0.1	31/01/2021	Laurens Dauwe (Osborne Clarke) Benjamin Docquir (Osborne Clarke) Margo Cornette (Osborne Clarke)	
	Name		***Date***
Prepared	Laurens Dauwe (Osborne Clarke) Benjamin Docquir (Osborne Clarke) Margo Cornette (Osborne Clarke)		January 2021
Reviewed	Laurens Dauwe (Osborne Clarke) Benjamin Docquir (Osborne Clarke) Margo Cornette (Osborne Clarke)		31 March 2021
Revised	Laurens Dauwe (Osborne Clarke) Benjamin Docquir (Osborne Clarke) Margo Cornette (Osborne Clarke)		31 March 2021
Reviewed	Isaac Pozo		10 April 2021
Circulation			
Recipient		***Date of submission***	
European Commission		10 April 2021	
Consortium		10 April 2021	

Authors (full list)
Laurens Dauwe (Osborne Clarke)
Benjamin Docquir (Osborne Clarke)
Margo Cornette (Osborne Clarke)

Project Coordinator
Josep Laborda
(Managing Partner)
Factual Consulting SL / 08195 – Sant Cugat del Vallès (Barcelona)
Mobile: +34-622854528
E-mail: josep@factual-consulting.com

Legal Disclaimer

Table of Contents

Glossary

BCR	Binding Corporate Rules.
CJEU	The Court of Justice of the European Union.
CNIL	National Commission on Informatics and Liberty. The CNIL is designated to operate as Data Protection Authority in France.
Database Directive	Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20, 27.3.1996, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML (last consulted 31 March 2021).
DLT	Distributed Ledger Technology
DMA	Digital Markets Acts - Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM (2020) 824, https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf (last consulted 31 March 2021).
DSA	Digital Services Act - Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM (2020) 825, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72148 (last consulted 31 March 2021).
DPIA	Data Protection Impact Assessment pursuant to Article 35 of the GDPR.
DPO	Data Protection Officer pursuant to Article 37 of the GDPR.
e-Commerce Directive	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN (last consulted 31 March 2021).

EDPB	European Data Protection Board pursuant to article 68 of the GDPR.
EEA	European Economic Area.
End-Users	A natural or legal person using the MDM.
ESA	European Space Agency.
GALILEO	Galileo is a global navigation satellite system (GNSS) created by the European Union through the European Space Agency (ESA), operated by the European GNSS Agency (GSA).
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj (last consulted 31 March 2021).
GNSS	Global Navigation Satellite System.
GSA	European GNSS Agency.
InfoSoc Directive	Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0029 (last consulted 31 March 2021).
IoT	Refers to the Internet of Things (IoT), a network of physical objects that are equipped with sensors, software and other technologies with the aim of connecting and exchanging data with other devices and systems over the Internet.
LBS	Location based services.
MaaS	Mobility as a Service.
MDM Operator	The person offering the Mobile Data Marketplace to End-Users and Service Providers.

Mobile Data Marketplace	The mobile platform pursuant to which mobility services and, as the case may be, other services may be offered to End-Users and Service Providers.
Mobility Services Providers	A Service Provider offering mobility services or MaaS services through the Mobile Data Marketplace.
MOLIÈRE	MOBILITY SERVICES ENHANCED BY GALILEO & BLOCKCHAIN.
Service Provider	Means a person offering services to other Service Providers or End-Users through the MDM.
WP	Work Package.
WP 29	Article 29 Working Party.

1. Executive Summary

This report provides a high level overview of the key legal and ethical challenges when operating a Mobility Data Marketplace (MDM) based on geolocation and blockchain. Section 3 of this report clarifies the MDM ecosystem and the roles of the different participants to such ecosystem.

When operating an MDM, there are a number of key legal challenges that need to be taken into account. Such key challenges relate among others to (a) privacy and data protection (see point (a) below), (b) intellectual property rights (see point (b) below) and (c) the validity and enforceability of smart contracts (see point (c) below). In addition to such legal challenges, the deployment of an MDM also brings certain ethical challenges with it (see point (d) below).

(a) *Data Protection*

As part of the MDM, a vast set of data, including personal data, will be used and exchanged by the different participants of the MDM. Consequently, different participants of the MDM, including the MDM Operator and (Mobility) Service Providers, will need to comply with the GDPR when using or exchanging such personal data. Although compliance with the GDPR is not straightforward in the context of an MDM, such compliance can be facilitated by (i) properly mapping the different types of data and data sets that will be used and exchanged as part of the MDM and (ii) implementing the proper business processes and contracting mechanisms, as further clarified in Section 4.1 and, in particular, Section 4.1.8 below.

(b) *Intellectual property rights*

Since the MDM aims at exchanging data between its participants, question arise around the ownership in data. To answer such questions, one needs to distinguish between (i) the *type of data* and (ii) the *type of protection mechanism*. With regard to the *type of data*, one needs to make the distinction between, (i) the *raw data* such as coordinates and (ii) *derivate data* which is essentially data generated further to the analysis (through Artificial Intelligence or other methodology) of different sets of raw data.

In principle, raw data will not enjoy the benefit of copyright protection as such data lack originality. However, as set forth in Section 4.2.2 below, sets of raw data may enjoy (i) the protection under the Database Directive if the structuring of such database would be original and/or (ii) the so-called *sui generis* protection if a substantial investment was made in obtaining, verifying and creating the database.

Derivative data on the other hand, can enjoy the benefit of copyright protection if such data are original. In addition, sets of derivative data could equally enjoy the benefit of database protection or *sui generis* protection if the criteria for such protection, as set forth in the preceding paragraph, are met.

(c) Smart contracts

As part of the MDM, different participants will enter into contracts with each other. One way to enter into such contracts is to use so-called *smart contracts*. Smart contracts are contracts which are based on computer language and, in some cases, use *Distributed Ledger Technology* or *blockchain*. Although such smart contracts facilitate the transactional process within the MDM ecosystem, their use also raises specific legal questions as regards their validity and enforceability.

The answer to the question on whether smart contracts are legally binding, is not straightforward. Whether or not a smart contract is legally binding, largely depends on the applicable contract law under which such smart contract is concluded (see Section 4.3). Consequently, when (a) an MDM Operator would decide to commence the offering of its services in a specific jurisdiction and (b) provided that such MDM Operator would aim to use smart contracts for its operations, it would need to first assess the legal validity of such contracts in jurisdiction in which it aims to operate (see Section 4.3).

(d) Ethical challenges

When operating an MDM, the different participants will obtain, use and exchange a significant set of personal data. When such data are collected on a massive scale, the use of AI technology and Big Data can enable new business opportunities. At the same time, the use of these technologies might also enable companies to profile End-Users and link certain conclusions to such profiles.

Aside from the privacy concerns regarding profiling, the profiling of individuals and the possibility to link automatic decisions to such profiles, also creates significant ethical risks. As further clarified in Sections 5 and 6, profiling could lead to inadvertent discrimination on the basis of gender, race or social background. In the context of an MDM, such discrimination might result among others in an unequal access to mobility solutions for certain groups of End-Users or a higher cost for such End-Users. As to accommodate for these concerns, Section 5.1.3 provides some general guidelines on how to apply Big Data and AI in the context of an MDM.

2. About Molière

Urban mobility is becoming an issue of great importance in today's society due to the increasing population movements towards big cities and the exponential growth of cities in developing countries. Today, urban mobility schemes are evolving faster than ever mainly due to social, economic and technological changes. The traditional choice between walking, taking public transport or buying a car is being extended with a wide range of new flexible mobility services, such as vehicle sharing and ride-hailing.

In this context, a new mobility paradigm is needed - from disconnected to complementing. Promoting more sustainable, affordable, equitable, and accessible mobility is crucial, where micromobility and shared mobility services increasingly complement public transport. The ultimate goal is to reduce dependence on single occupancy private vehicles.

MOLIERE aims to build the world's best open data commons for mobility services, the "Wikipedia of public transport and new mobility data", a Mobility Data Marketplace (MDM) underpinned by blockchain technology, raising the profile, visibility, availability, and utility of geo-location data from GALILEO, and will test it to fuel and demonstrate a diverse set of concrete, highly relevant mobility scenarios and use cases where geo-location data is key, addressing the needs of cities, public transport authorities, mobility service providers, and end-users.

3. Introduction

3.1. Data as a driver for new business models

Information technology has significantly changed our perception on data. Whereas data were traditionally used to support business decisions, it has now become an asset by itself as it often creates opportunities for new business models. In industries such as the financial industry and telecommunications industry, vast sets of financial transaction data and communication data are now being used for the creation of value added services such as, to name just one example, fraud detection.[2]

Also in the context of urban mobility, the use of data is invaluable for the creation of new and smart mobility solutions. Over the last years, there is an increasing trend for the deployment of alternative modes of transportation. These alternative modes of transportation are offered in various cities through micromobility solutions such as e-scooters, e-bikes and various other electrically powered micro-vehicles. Such mico-mobility solutions are either privately used or shared by its users.[3] In addition, traditional modes of transportation such as cars, busses and trains have become *smart* in the sense that such vehicles have become connected to the Internet.

As a common denominator, such modes of transport are becoming part of the so-called *Internet of Things* as they are equipped with *IoT devices* such as digital sensors and communication technologies. These IoT devices enable mobility solutions to generate a significant set of data on a variety of aspects including a vehicle's trajectory, fuel consumption, times of arrival etc.

Although the data generated by a single device might only have limited value, the combination of data from many vehicles and the subsequent analysis and interpretation thereof through Big Data, might create additional value. If data sets are combined, one might, depending on the data available, predict potential traffic congestion issues, propose (i) routes with lower fuel consumption, (ii) a lower overall cost, (iii) more environmentally friendly modes of transportation or routes, (iv) adapted vehicle insurance solutions etc.

Consequently, the use of MDMs could, depending on the use cases and the data at hand, enable companies to propose alternative business models and generate additional value whereas public authorities could use such data to further define urban mobility policies.

3.2. MDMs and the MDM ecosystem

Since many different Mobility Services Providers operating in cities have their own data sets and their own data platform, added value might be created if the data of these

[2] EBA Report in Big Data and advanced analytics, EBA/REP/2020/01, January 2020 p. 11, https://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf (last consulted on 22 March 2021); Becker, Richard & Volinsky, Chris & Wilks, Allan. (2010), Fraud Detection in Telecommunications: History and Lessons Learned, Technometrics, 52, 10, 1198/TECH, 2009, 08136.

[3] G. Oeschgera, P. Carrolla, B. Caulfield, "*Micromobility and public transport integration: The current state of knowledge*", Transportation Research Part D: Transport and Environment, 89, December 2020, 102628, https://doi.org/10.1016/j.trd.2020.102628 (last consulted on 23 March 2021).

Mobility Services Providers are combined and exchanged.

An MDM plays a crucial role in this setup as it can act as a central hub for the collection and exchange of these data. The MDM would not only *collect* the data from the different Mobility Services Providers, it would also allow for the *exchange* of such data with other Mobility Services Providers, End-Users or even third parties or Service Providers who aim to use the MDM to offer their services.

Consequently, a basic MDM ecosystem is composed primarily out of the following participants:

- **Mobility Data Marketplace Operator**: The MDM Operator is the person who operates and manages the Mobility Data Marketplace. It will in principle operate as a central hub for the collection and exchange of data between the different participants of the MDM. In the context of the Moliere Project, Moliere aims to operate as an MDM Operator.
- **Mobility Services Provider**: The Mobility Services Provider is a person offering mobility services such as MaaS Services to End-Users.
- **Service Provider**: A Service Provider is a person offering additional services to either the End-User, the Mobility Services Provider or the MDM Operator. Depending on the envisaged use case, a Service Provider could offer a variety of additional services such as (i) insurance services to End-Users or Mobility Services Providers, (ii) services relating to environmentally friendly modes of transportation, (iii) data analytics or the provision of specific derivative data etc.
- **End-User**: Is the person using the services offered by the MDM Operator and the modes of transport and/or additional services provided through the MDM.

The MDM ecosystem can therefore be visualised as follows:

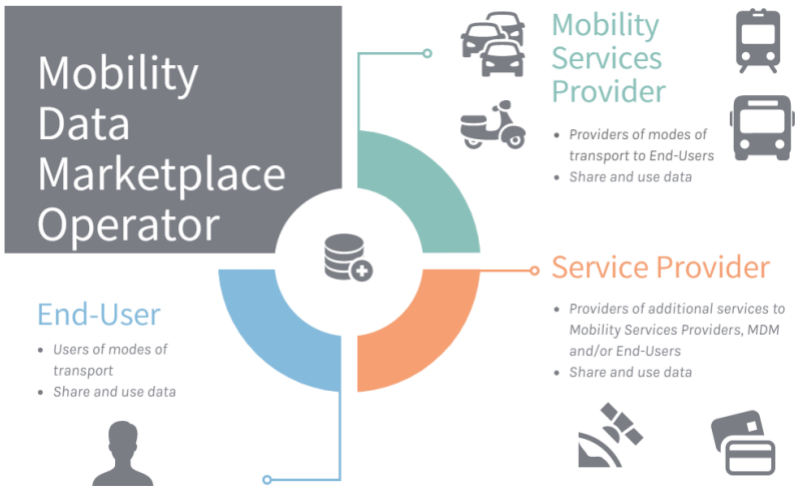

Image 1[4]

3.3. Key challenges

[4] Image created with VennGage Editor (https://infograph.venngage.com/)

Although an MDM can bring benefits, it also raises certain legal challenges. Since End-Users share substantial amounts of data, a significant part of these data might be personal data within the meaning of the General Data Protection Regulation.[5] As a result, participants to the MDM who receive these personal data may need to comply with the specific requirements set forth in the General Data Protection Regulation. These questions are fundamental for the operation of an MDM and are further analysed in Section 4.1 below.

In addition, the utilisation or sharing of the data also raises the question on the ownership hereof. If such data are enriched through the use of data analysis methodologies such as Big Data, it also raises the question on the ownership of these enriched or derivative data. These questions essentially relate to the topic of intellectual property rights in data, a topic that is further addressed in Section 4.2 below.

When becoming a participant to the MDM or ordering mobility services through an MDM, an End-User will enter into agreements with the MDM Operator and / or other participants. As to facilitate the integrity and non-repudiation of the agreements to be entered into and the underlying data, so-called *smart contracts* based on Distributed Ledger Technologies and blockchain could be used. Although the use of DLTs and blockchain has its merits, it also raises some legal questions as regards (i) the validity and enforceability of such of smart contracts and (ii) the compliance of such blockchain technology with the basic requirements under the GDPR. These issues are further analysed in Sections 4.1.7 and 4.3 below.

The use of digital marketplaces such as a Mobility Data Marketplace, is a relatively new concept. Even though the provision of digital marketplaces has been regulated to some extent by legal instruments such as the e-Commerce Directive (see Section 4.4.1(a) below), it has become clear that such regulation needed to be updated to tackle newly emerging issues. In this context, the European Commission recently issued a proposal for a Digital Services Act. Section 4.4 below aims to clarify some of the legal obligations that may be imposed upon operators of online marketplaces, which might include an MDM Operator, in the context of the upcoming legislation.

Lastly, the use of mobility data and the further analysis thereof on the basis of so-called Big Data or artificial intelligence algorithms, raises certain ethical concerns. This is particularly the case as some data sets may be misused for profiling End-Users and even discriminating certain users on the basis of certain characteristics such as race, gender, physical characteristics or social background. Section 5 below aims to identify some of these risks and provide some principles on how to avoid such ethical issues in the context of an MDM.

This report has by no means the intention of providing an exhaustive list of all relevant legal and ethical challenges that are relevant when operating an MDM nor does it intend to provide any legal advice in relation thereto. However, it does aim to provide some guidance on which key challenges one might face when operating an MDM and provide certain principles to tackle some of these challenges.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj (last consulted on 31 March 2021).

4. Legal challenges for MDM's

A key characteristic of an MDM is the exchange of data between its different participants. As part of an MDM, End-Users and Mobility Services Providers will consult the MDM's data or even share such data with the MDM or other End-Users or Mobility Services Providers.

This section aims to (i) identify certain key legal challenges when using and operating an MDM and (ii) provide practical guidance on how such challenges could be tackled.

4.1. Data Protection

4.1.1. *Introduction into the GDPR*

(a) *What is the GDPR*

On 25 May 2016, the General Data Protection Regulation or GDPR entered into force. This regulation specifically aims at creating a harmonised legal framework for the use of data relating to identified or identifiable natural persons by imposing a number of strict obligations to safeguard the privacy of the individual concerned (the "data subject").

(b) *Scope of the GDPR*

With regard to its material scope, the GDPR essentially applies to the "processing" of "personal data" wholly or partly by automated means and to manual processing if the personal data form part of a filing system or are intended to form part of a filing system.

In this context,

- **Personal Data**: are defined as "any information relating to an identified or identifiable natural person"[6] whereby an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"; whereas

- **Processing**[7]: covers a wide range of operations performed on personal data, whether or not by automated means, including the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

However, as the GDPR requires a processing of "personal data", it does not

[6] Article 4 (1) GDPR.
[7] Article 4 (2) GDPR - *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"*

apply to any processing operations of anonymous data, such as data that cannot be traced back to a specific individual.[8]

4.1.2. *Applicability of the GDPR in the context of MDMs*

A key business driver for MDMs is the collection, exchange and use of various types of data. In many cases and depending on the specific nature of the MDM concerned, such data may include data sets relating to (i) the specific location of a device or a vehicle and (ii) information concerning a specific End-User such as its access credentials, its unique identifier, device ID, etc.

(a) *Applicability of the GDPR on MDM Operators*

As part of an MDM, the MDM Operator will typically require its End-Users to enter into an agreement with the MDM Operator. To that end, the MDM Operator will typically request such End-User to provide specific personal details such as its name, (e-mail) address and potentially additional information.

Since such data can be used to identify a specific natural person, the GDPR is applicable to the MDM Operator.

(b) *Applicability of the GDPR on Mobility Service Providers*

(i) *GDPR and Mobility Service Providers*

When providing their mobility services, Mobility Service Providers may, depending on the setup of the MDM and the mobility service provided, acquire certain personal data of an End-User. Such personal data may include, as the case may be, geo-positioning data or even account information of the End-User concerned.

To the extent that such data can be used to identify a natural person, the GDPR will also apply to the Mobility Service Provider concerned.

(ii) *Applicability of the GDPR on MDM Service Providers*

Although it is unclear on whether it would be in scope of Moliere, certain actors such as Service Providers may also aim to use specific data from the MDM to provide value added services such as location based services ("**LBS**"), insurance services (vehicle insurance, travel insurance or other forms of insurance) or payment services to either other Service Providers or End-Users.

Should such Service Providers acquire personal data for the

[8] Please note however that the question on whether data is *anonymous*, is subject to discussion.

purpose of such additional services, the provision of such services would also imply that the GDPR would be applicable to such Service Providers. In such a case, the allocation of responsibilities and liabilities among the different operators should be addressed with caution and early on in order to avoid legal uncertainty or increased risks for the MDM Operator.

4.1.3. *Legal qualifications under the GDPR*

In terms of its obligations, the GDPR makes a distinction between so-called data *controllers* and data *processors*. Further to Article 4 (7) GDPR, a controller is defined as the person who defines the *means* and *purpose* of the processing[9], whereas the processor is typically defined as the person who *processes personal data on behalf of the controller*.[10]

The qualification as a controller or processor of the different actors involved has implications beyond the allocation of responsibility and liability. Therefore, it is important to understand and assess the respective roles of the MDM Operator, the Service Providers and the Mobility Service Providers under the GDPR.

The legal qualifications are driven by a factual analysis and do not depend upon contractual arrangements nor corporate structures. As a main rule, the more a party is involved in the decision-making process with respect to the processing of personal data, the more likely it will qualify as a (joint) controller.

Against this background, the entity that determines the *purpose* of the processing will in all cases be regarded as the data controller, whereas the entity determining the *means* of the processing will not, unless that determination concerns the essential elements of the processing operations. Various factors are listed below that should be taken into account when assessing the relevant data processing roles of the different parties in an individual case:

- Decisions to collect personal data and the legal ground thereof;
- Decisions on the purpose(s) for the collection of the data;
- Decisions on the categories of personal data to collect;
- Decisions on the methodology to be used and which individuals to collect data bout;
- Decisions on which (third) parties the data is disclosed to;
- Decisions on how long the personal data will be retained.

The collaboration with the MDM Operator, the Service Providers and the Mobility Service Providers can be implemented in various manners and hence

[9] Article 4 (7) GDPR – *"'controller' means the 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;"*

[10] Article 4 (8) GDPR – *"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"*

result in different legal qualifications. Given the various manners in which the MDM can be implemented, one cannot propose a one-size-fits-all solution as regards the legal qualifications under the GDPR. However, as the MDM Operator and the majority of Services Providers will also process the personal data for their own purposes, one might argue that the MDM Operator and the Service Providers would most likely be considered separate data controllers whereby each controller would have its own legal responsibilities.

(a) *Separate controllers*

If the MDM Operator and the (Mobility) Service Providers qualify as separate controllers, no agreement between them is legally required, as each controller has its own responsibilities under the GDPR for its own processing activities.

That being said, sharing the data through the MDM is a processing operation in itself, for which the MDM Operator will be accountable under the GDPR. Consequently, as to mitigate its own GDPR risks, the MDM Operator should impose terms and conditions upon other Service Providers in which some key roles and responsibilities of the parties are covered (see Section 4.1.8 below).

(b) *MDM (Mobility) Service Providers as processors*

If the MDM Operator qualifies as the sole controller and the (Mobility) Service Providers as processors, the parties have to enter into a Data Processing Agreement pursuant to Article 28 GDPR.

(c) *Joint Controllership*

The allocation of responsibilities between the parties depends on the circumstances of the relationship. Processing operations are often sequential and attributable to different legal entities, but in those situations the European Court of Justice tends to regard the various operators as *joint controllers* (even if not all entities have access to all of the data in the same time).

Such "joint control" does not necessarily mean that the responsibilities are equivalent between the parties. Where the MDM Operator and the (Mobility) Service Providers are joint controllers, a distribution of responsibilities between the parties is to be made in a written agreement, allocating the roles and duties to inform data subjects, reply to requests to access personal data, etc. (see Section 4.1.5 below). In other words, the joint controllers need to decide among others on who is the most appropriate party to e.g. inform the customers and respond to requests from customers exercising their rights under the GDPR (see Section 4.1.5(a) below).

The essence of the arrangement between the parties must be made available to the data subjects, including which of the parties serves as a point of contact. This information is generally made available via a privacy notice but can be provided to data subjects by any other means.

When operating as joint controllers, such joint controllership also results in a

joint liability at least vis-à-vis third parties. This implies that individuals can seek compensation from any of the joint controllers. Each joint controller will be liable for the entire damage caused by the processing, unless it can prove it is not in any way responsible for the event giving rise to the damage. The arrangement made as regards the allocation of liability between controllers is irrelevant as regards such third-party claims. In addition, joint controllers are also each fully accountable to data protection authorities for a failure to comply with their responsibilities.

4.1.4. *General Requirements under the GDPR*

(a) *Legal Basis – Legitimacy principle*

Under the GDPR, a person may only process personal data if such processing has a "legitimate basis" (the so-called *legitimacy principle*). Article 6 of the GDPR provides the following six legal bases: (i) consent, (ii) processing is necessary for the performance of a contract, (iii) processing is necessary for compliance with a legal obligation to which the controller is subject, (iv) processing is necessary in order to protect the vital interest of the data subject or another natural person, (v) processing is necessary for the performance of a task carried out in the public interest, and (vi) processing is necessary for the purpose of the legitimate interest pursued by the controller or by a third party.

In the context of an MDM, the legitimacy principle implies that each person who processes personal data as part of the MDM should determine:
(i) for which purposes it processes it processes such personal data; and
(ii) on which legal basis such personal data will be processed.

In addition, Article 9.2 of the GDPR sets out the circumstances in which the processing of sensitive personal data which is otherwise prohibited, may take place. Consequently, in order to lawfully process sensitive data, each participant must identify both a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9 (such as explicit consent or protection of vital interests).

With regard to the processing of personal data relating to criminal convictions and offences, it should be noted that the national rules for the processing of such data may differ per EU Member State.[11]

In practice, the MDM Operator and the (Mobility) Service Providers will most likely rely on one or more of the following legal grounds: (explicit) consent, performance of a contract, legitimate interest and / or the performance of a legal obligation.

Please note that if an MDM participant would prefer to rely on legitimate interest as a legal basis, it must perform a *balancing test* to justify any impact on individuals which must be made available to data subjects on request. The

[11] Please note that a comparative analysis of the legal regimes as regards the processing of personal data regarding criminal convictions within the different EU Member States, is outside the remit of this study.

balancing test implies an assessment on whether "the interest or fundamental rights and freedoms of the data subject which require the protection of personal data" outweighs the interests of the MDM participant concerned. In essence, this balancing test is an elementary risk assessment to check that any risks to individuals' interests are proportionate. In addition, the MDM participant should inform the End-Users that it is using their personal data on this lawful basis, explaining to them what the legitimate interests are, and also informing End-Users of their right to object to processing (see also Section 4.1.5(a) below).

When applied in the context of an MDM, one could foresee that different categories of personal data might be processed. The table below, which is provided **for illustrative purposes only** and based on a theoretical use case for car sharing services, provides an example of the different categories of personal data to be used as part of an MDM together with the legal basis on which such data might be processed.

Category of personal data	Reasons	Legal ground
1. *Sensitive data (e.g. health data)*	(i). Fulfilling (pre)contractual obligations (e.g. requests as regards prior medical conditions and the fitness to operate a specific vehicle as part of mobility sharing solutions);	Article 9 lists the conditions for processing special category data. In this case, the most appropriate ground might be: The data subject's **explicit consent**[12] - Article 9.1.(a) GDPR.
2. *Personal data relating to criminal convictions and offences*	Processing of personal data might be necessary in certain circumstances e.g. for: **car sharing services**: in order to assess the risk, it will be necessary to obtain information from the prospective End-User (via a questionnaire) about recent criminal convictions for drunkenness, alcoholism or revocation of driving licences.	Article 10.5. of the Belgian Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data: *"in cases where the data subject has given his **explicit consent** in writing that the personal data in question can be processed for one or more specific purposes and if the processing is strictly limited to those purposes;"*

[12] Where consent is necessary, it should be a freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify they agree to the processing of their personal data. The Article 29 Working Party has defined "explicit consent" as "all situations where individuals are presented with a proposal to agree or disagree to a particular use of disclosure of their personal information and they respond actively to the question, orally or in writing".

Category of personal data	Reasons	Legal ground
3. Other personal data	(i). own interest of the parties; (ii). obligations imposed by the law (e.g. to comply with anti-money laundering legislation, detection of payment fraud); (iii). e.g. Vehicle bookings and use of vehicle: when an End-User decides to book a vehicle of a Mobility Service Provider, he/she is required to share his/her location data so that the Mobility Service Provider can locate the End-User with respect to the vehicle. The End-User needs to be in a certain distance of the vehicle to be able to unlock it; (iv). The processing of personal data strictly necessary for the purposes of preventing fraud without their being a legal obligation; (v). The provision of payment services.	(i). legitimate interests of the controller and/or third parties - article 6.1.(f); (ii). legal obligation – article 6.1.(c) (iii). necessary for the performance of the contract – article 6.1.(b) (iv). Recital 47 GDPR: The processing of personal data strictly necessary for the purposes of preventing fraud could constitute a legitimate interest of the payment service provider concerned, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject – article 6.1.(f). (v). In principle, Article 6(1)(b), meaning that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract[13].

(b) *Proportionality principle*

When assessing the processing of personal data, proportionality requires that only that personal data which is *adequate* and *relevant* for the purposes of the processing is collected and processed. Furthermore, personal data that is

[13] European Data Protection Board, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, version 2.0., adopted 15 December 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf (last consulted on 31 March 2021).

processed **may not be kept longer than necessary**.[14]

In the context of an MDM, the proportionality principle implies that each person who processes personal data should determine:

(i) for which purposes it processes it processes such personal data;
(ii) whether such processing is necessary for the envisaged purpose;
(iii) how long such data needs to be retained; and
(iv) whether such retention period is proportionate in light of the purposes pursued.

On the basis of such analysis, the data controller can draft a data retention policy that is aligned with its specific needs and would comply with the proportionality principle of the GDPR.

(c) *Transparency principle*

The transparency principle, as set forth in Articles 12 - 14 of the GDPR, essentially implies that the individual concerned must understand (a) that her personal data are being processed, (b) who processes her personal data, (c) which personal data are being processed and for which purposes, (d) who may receive these personal data and for which purposes, (e) how long personal data will be stored and (f) that she has certain rights under the GDPR.

Prior to the processing of such personal data, the data controller must provide the information set forth above in a clear and unambiguous manner to the data subject.

In the context of an MDM, the transparency principle would imply that (i) the operator of the MDM and (ii) the Service Provider, are required to provide such information to the data subject prior to the processing of personal data. To comply with this requirement, the persons involved typically provide a privacy policy which needs to be accepted by the End-User when registering on the MDM or entering into an agreement with the Service Provider.

4.1.5. *Specific Requirements under the GDPR*

(a) *Data Subject Rights (Article 15 – 22 GDPR)*

The GDPR attributes certain rights to data subjects. Such rights include among others, the right (i) of access to personal data, (ii) to rectification of incorrect personal data (the so-called *right to rectification*), (iii) to erasure of personal data (the so-called *right to be forgotten*), (iv) to restrict the processing of personal data (*data minimisation*), (v) to data portability, (vi) to object to the processing of personal data for e.g. direct marketing purposes, (vii) to oppose to automated decision making or profiling. The conditions for exercising such rights by the data subject are further specified in the GDPR.

Controllers are obliged to give effect to the rights of data subjects within

[14] Article 5 (1) GDPR.

specified time periods. Depending on the assessment above as regards the legal qualifications (see Section 4.1.3 above), the parties need to decide who would be the most appropriate party to respond to requests from data subjects exercising their rights. The parties may choose to specify a central point of contact to which the data subjects can address their requests for the exercise of their rights. However, in case of joint controllership (see Section 4.1.3(c) above), data subjects must remain able to exercise their rights against each of the joint controllers.

If the MDM Operator qualifies as the sole controller, it is up to the MDM Operator to decide autonomously (and be transparent about) how it will comply with transparency obligations and individuals' rights.

In the context of an MDM, the MDM operator and Service Providers who operate as data controllers (be it separately or jointly) must ensure that their internal data protection processes are organised in such a manner as to allow data subjects to exercise these rights. This is explicitly provided in Recital 59 of the GDPR which emphasises that "modalities should be provided for facilitating the exercise of the data subject's rights, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object." In addition, the data controller should "also provide means for requests to be made electronically, especially where personal data are processed by electronic means".

The modality provided by a data controller for data subjects to exercise their rights should be appropriate to the context and the nature of the relationship and interactions between the controller and a data subject. To this end, a data controller in the framework of the MDM should consider designing a data subject's right form which individuals can complete and submit electronically.

However, even if such form has been provided to a data subject, it does not imply that a data subject right request submitted by any other means will be invalid. Therefore and although a data subject might be invited to use such a form, one should also make it clear that the data subject is not obliged to do so.

(b) *The right to oppose to "automate decision making"*

Article 22.1 GDPR introduces the concept of *automated decision making*, i.e. the processing by machine with no human intervention. More specifically, this provision includes a right for data subjects "not to be subject to a decision which is based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." It thus prohibits such automated decisions unless certain conditions as set forth in Article 22 GDPR are satisfied.

As further discussed in Section 5.1.1 below, the right to oppose to automated decision making is a substantial concern for companies that largely rely on

Big Data for their business model.

(c) *Requirements regarding the appointment of a DPO*

According to the GDPR, controllers and processors are free to determine on whether or not they appoint a Data Protection Officer or DPO. However, in the following cases, the appointment of a DPO is mandatory:

- When personal data is processed by public authorities;
- For organisations whose core activities require regular and systematic monitoring of data subjects on a large scale;
- For organisations whose core activities require large scale processing of special categories of data or criminal convictions and offences; and
- Organisations obligated to do so by national member state law.[15]

The GDPR sets out detailed requirements for the position and tasks of the DPO. Under Article 37.5 GDPR, the DPO must have expert knowledge of data protection law and practices to fulfil the tasks listed in Article 39 GDPR as a minimum.[16]

In addition, Article 38 GDPR requires the organisation to ensure that the DPO (i) is properly and in a timely manner involved in all issues which relate to the protection of personal data, (ii) performs his or her duties and tasks independently and (iii) does not receive any instructions as regards the exercise of the function. The GDPR specifies that a DPO may fulfil other tasks and duties but that the controller or processor must ensure that any such tasks and duties do not result in a conflict of interests. This is supported by WP29, which has further elaborated this principle in its Guidelines on Data Protection Officers (the "**Guidelines**"): "*A conflict of interest entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case*."[17]

In addition, as a rule of thumb, the Guidelines state that a conflict of interest occurs when a DPO also holds a senior position within an organisation - such as CEO, COO, CFO, CMO, Head of Marketing, Head of HR or Head of IT - but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing.

If a DPO is not mandatory but an organisation decides to appoint a DPO on a voluntary basis, the same requirements as set forth by the GDPR to mandatory DPOs, will apply to them.

[15] Article 37.1. GDPR.
[16] These tasks include: (i) informing and advising the organisation's employees of their data protection obligations, (ii) monitoring compliance with the Regulation and the organisation's policies, (iii) providing advice on data protection impact assessments and (iv) acting as the contact point for the supervisory authority and cooperating with the authority.
[17] Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev. 01.

Finally, unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends[18] that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly. This analysis is part of the documentation under the accountability principle[19].

In the context of the MDM, the question on whether or not the MDM Operator needs to appoint a DPO depends on the criteria as set forth above. However, as the MDM Operator will operate the data marketplace and as such marketplace might have as its core activity to store data, it is likely that the MDM Operator would be obliged to appoint a DPO.

(d) *Requirements regarding the performance of a DPIA*

Under the GDPR controllers must carry out a DPIA if the proposed processing is likely to entail a *high risk* for the individuals whose data are being processed. The DPIA should be conducted before the processing and should be considered as a living tool, not merely as a one-off exercise. Where there are residual risks that cannot be mitigated by the measures put in place, the competent Data Protection Authority must be consulted prior to the start of the processing[20].

(i) *General rule*

Article 35 of the GDPR states that a DPIA is mandatory in particular if the following takes place:

- Systematic and extensive evaluation of the personal aspects of an individual, including profiling;
- Processing of sensitive data on a large scale;
- Systematic monitoring of public areas on a large scale.

(ii) *Article 29 Working Party (currently the European Data Protection Board)*

The WP29 sets out nine criteria to be taken into account in order to determine whether a processing operation is likely to create a high level of risk.[21] If at least two criteria are met, the WP29 considers that the processing operation concerned requires a DPIA. These nine criteria are: (i) evaluation or scoring, (ii) automated decision making with significant legal or similar effect, (iii) systematic monitoring, (iv) sensitive data, (v) data processed on a large scale, (vi) matching or combination of data sets, (vii) data concerning vulnerable persons, (viii) innovative use or application of new technological or organizational solutions, (ix) processing operations in themselves that

[18] Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev. 01, p.5.
[19] Article 24.1 GDPR.
[20] Article 36 GDPR.
[21] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 October 2017, WP 248 rev. 01, p. 10.

prevent the data subjects from exercising a right or benefiting from a service or contract.

(iii) A mandatory DPIA

National Data Protection Authorities, in concertation with the European Data Protection Board, may provide lists of cases where a DPIA would be required. The following EU Members States have submitted their DPIA lists[22]: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Slovakia, Spain and Sweden.

In certain European Member States such as Belgium, the following data processing activities require companies to conduct a DPIA:[23]

- Processing of biometric data (e.g. fingerprints) of individuals in a public area or private area that is publicly accessible;
- Collecting personal data from third parties in order to use that information for making a decision to refuse or end a contract with an individual;
- Collecting health-related data by automated means through an active implantable medical device;
- Collecting personal data on a large scale by third parties in order to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of individuals;
- Systematic sharing of sensitive data or data of a very personal nature (e.g. related to poverty, unemployment, social work) between data controllers;
- Large-scale processing of data generated by devices with sensors that send data over the Internet or any other means (e.g. Internet of Things applications like smart TVs and smart energy systems) in order to analyse the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of individuals;
- Large-scale and/or systematic processing of telephony-, Internet- or other communication data, metadata or localization data of individuals (e.g. Wi-Fi tracking), when such processing is not strictly necessary for the service requested;
- Large-scale processing of personal data where behaviour of individuals is observed, collected, established or influenced in a systematic manner and by using automated means.

(iv) Conclusion

[22] Opinions European Data Protection Board on the draft list of the competent supervisory authority regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4. GDPR), https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.
[23] Belgian DPA (Gegevensbeschermingsautoriteit), DPIA list, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf (last consulted on 29 March 2021).

Given the fact that the processing of data via the MDM by the different participants might reasonably entail (i) the processing of behavioral data on a large scale, (ii) the systematic sharing of data of a very personal nature between data controllers and (iii) that the envisaged data processing activity meets already three criteria listed by the WP29 (innovative use or application of new technological or organizational solutions, data processed on a large scale and potentially sensitive data) it is likely that the MDM Operator and certain Service Providers who meet these criteria are required to perform a DPIA.

(e) *Retaining a Data Process Register*

In accordance with Article 30 of the GDPR, controllers and processors are required to maintain extensive and up-to-date internal records of their data processing activities.

A very limited exemption from this obligation applies to organisations employing fewer than 250 people, provided that the processing is "occasional", is unlikely to result in a risk to the rights and freedoms of data subjects and the processing does not involve special categories of data as referred to in Article 9(1) of the GDPR or personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR.

In light of the foregoing, the MDM Operator and the (Mobility) Service Providers are in principle required to create and maintain such a data processing register.

(f) *Data security and personal data breach notifications*

(i) *Data security requirements*

Pursuant to Articles 5.1.(f) (principle of integrity and confidentiality) and 32 of the GDPR, all parties involved in the processing should implement appropriate technical and organisational measures to ensure an appropriate level of security of the personal data gathered, taking into account in particular the nature, scope, context and purposes of the processing.

The table below provides an indication of specific technical and organisational measures that could be applied:

Examples of technical measures[24]	• Pseudonymisation and data encryption; • Two (or more) factor authentication; • Firewalls, virus and malware scanners, periodic backups, SSL certificates for websites.
Examples of organizational measures[25]	• Access management, based on need-to-know/need-to-use, enhanced protection of high-privilege accounts (e.g. privileged administrator account) and access monitoring (logs); • Physical security of office space; • Signature of a confidentiality and non-disclosure clause with all persons having access to personal data; • Educate employees about information security; • Clear protocols and procedures are in place for the rapid and effective detection and handling of information security incidents and vulnerabilities; • Promote a clean desk policy; • Password Policy.

If the MDM Operator qualifies as the sole controller, the MDM Operator should require its data processors to implement appropriate security measures.

(ii) Personal data breach notification

A security incident, leading to a data breach, can give rise to a number of notification duties:

- To the relevant supervisory authority without undue delay and, where feasible, not later than 72 hours of becoming aware of the breach, unless the breach is unlikely to put the data subjects' rights and freedoms at risk;
- To affected data subjects if the breach is likely to result in a high risk to the rights and freedoms of the data subjects.

[24] Information Commissioner's Office, Penalty Notice, Case ref. COM0804337, Marriott International Inc., https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf (last consulted on 31 March 2021); Information Commissioner's Office, Penalty Notice, Case ref. COM0783542, British Airways, https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf (last consulted on 31 March 2021).
[25] *Ibidem.*

- As a processor, to the controller without undue delay in all cases.

In light of the foregoing, the MDM Operator and Service Providers should (i) implement procedures to identify security incidents, respond and make the required notifications, (ii) allocate responsibility for personal data security, (iii) ensure that processors are obliged to report personal data breaches and (iv) maintain a register of all the facts relating to the personal data breaches, its effects and the remedial action taken (internal breach register).

Please note that in the case of a cross-border processing and notification is required, the data controller should notify, if it has a single or main establishment, the competent lead supervisory authority. This may not necessarily be where the affected data subjects are located or where the breach has taken place. When notifying the lead supervisory authority, the data controller should indicate whether the breach involves establishments located in other Member States and whether the breach affects data subjects in other Member States. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.[26]

(g) *International data flows*

(i) *General*

Article 44 of the GDPR prohibits transfers of personal data to a country outside the European Union and the European Economic Area which does not offer an adequate level of protection, unless adequate safeguards with respect to the protection of personal data and individuals' privacy are taken (see below "transfer tools"). This prohibition applies to transfers of "personal data which are undergoing processing or are intended for processing after transfer." In other words, the transfer of personal data to countries outside the EEA/EU may only take place if the third country in question ensures an adequate level of protection.

Before deciding which framework to use to enable data transfers, it is important to assess whether the accessibility of End-Users data to people in third countries constitutes a transfer of data to a third country within the meaning of the GDPR.

The term "data transfer" is not defined in the GDPR and its interpretation relies on the doctrine and jurisprudence.

If one relies on the doctrine developed in the *Lindqvist* CJEU case[27], it is arguable that the MDM does not entail international transfers of data. However, subject to the specifics of the IT infrastructure (e.g. in case the data is stored on US servers or accessed from outside the European Union), there

[26] Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, wp250 rev.01, p. 16 – 17.
[27] CJEU, C-101/01 (Lindqvist), Personal data which appear on the computer of a person in a third country, coming from a person who has loaded them onto an internet site, were not directly transferred between those two people but through the computer infrastructure of the hosting provider where the page is stored. Such transfers do no as such constitute a transfer of data to a third country.

is a risk that a competent judge would come to a different conclusion in the particular case as (i) there is little case law on the interpretation of a data transfer, (ii) the EDPB mentioned in its recent guidelines[28] that remote access by an entity from a third country to data located in the EEA is also considered a transfer and (iii) several legal scholars take the view that the safest interpretation of Lindqvist case is that making personal data available on the Internet must be considered a transfer of data, as it involves granting access to data about other parties (for example customers, etc.) on a large scale and for business purposes. Currently, national supervisory authorities tend to qualify the collaboration with cloud computing providers (IaaS, PaaS, SaaS) as a transfer of personal data, to the extent the data are stored on a server outside the EU/EEA or on a so-called "public cloud". National courts across Europe appear to follow that trend. As a result, and in spite of the relatively old Lindqvist decision, there is a major risk that the personal data processed in the context of the MDM will be found to be "transferred outside the EU/EEA" since such data is at least accessible from outside the European Union.

(ii) Transfer tools

In view of the above, from a risk mitigation perspective, the MDM Operator and (Mobility) Service Providers should implement adequate safeguards in order to secure the transfer of personal data in the context of the MDM. As stated above, a choice needs to be made on the joint controllership / sole controllership issue, and that will also influence the implementation of the adequate safeguards since those essentially rely on a specific form of contractual arrangement between the different actors involved.

That being said, at this stage, there are mainly two types of possible safeguards: (i) the so-called "transfer tools" under article 46 GDPR and (ii) the derogations under article 49 GDPR. Adequacy decisions are not a realistic possibility for an MDM given the potential global reach of an MDM.

Article 46 GDPR transfer tools include (i) the *standard contractual clauses*, (ii) *binding corporate rules* ("BCRs") or (iii) *ad hoc arrangements* that are either approved by the Commission or certified by an accreditation body.[29]

The *standard contractual clauses*, which is the most commonly used transfer tool, is a template contract drafted by the European Commission which sets forth the conditions under which personal data can be transferred to a country that does not provide an *adequate level of protection*.

Article 49 allows for the derogation of the principle on using a *transfer tool* as set forth in Article 46 GDPR. This derogation includes the option to (i) ask for the explicit consent of the data subjects for the transfer of personal data to

[28] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en (last consulted on 29 March 2021).

[29] As *Binding Corporate Rules* and *ad hoc decisions* are typically not the common mode to transfer personal data, both transfer modes have not been included in the remit of this study.

a country that does not provide an adequate level of protection or (ii) to rely on the fact that the making available of the data is necessary for the performance of a contract (it can also be a contract "in the interest of the data subject"). The general thinking of the EDPB is however that derogations under Article 49 of the GDPR should be limited to sporadic and temporary situations. Consequently, from a risk mitigation perspective, it is typically recommended to opt for the usage of one of the transfer tools as provided under Article 46 of the GDPR.

4.1.6. *Sanctions under the GDPR*

The GDPR imposes strict conditions on the processing of personal data. A failure to comply with such strict obligations can result in (i) civil, (ii) criminal and/or (iii) administrative liability.

In order to ensure effective compliance with the GDPR, Article 83 of the GDPR allows for national competent authorities to impose among others administrative fines up to the higher of EUR 20.000.000 or 4% of the total annual turnover of the undertaking concerned in the fiscal year preceding the infringement.

4.1.7. *GDPR in the context of Blockchain*

One of the key characteristics of the MDM as envisaged by Moliere, is that the MDM would be underpinned by the use of blockchain or Distributed Ledger Technology ("**DLT**"). At the moment, the precise impact of the use of blockchain is hard to anticipate, as it will depend on the specific use cases envisaged. As a consequence, the GDPR compliance of a specific implementation of blockchain technology for a specific use case, must ultimately be determined on a case-by-case basis.

This paragraph, however, will briefly discuss certain concepts relating to the use of blockchain technology such as (i) the blockchain technology itself, (ii) the concepts of pseudonimised, hashed and encrypted data and (iii) the tension between blockchain and the GDPR.

(a) *Introduction into blockchain technology*

Although blockchain is a commonly used term, it does not have an unambiguous definition as there is not one blockchain technology and blockchain technology as such can have many applications.

In the most general sense, blockchain can be defined as a decentralised technology where a network of servers or nodes, each with their own replicated registry, receive transactions together, approve them using a cryptographic exercise and compare the outcome to reach consensus.[30] In

[30] P-J. Aerts and F. Hoogendijk, "Smart contracts, een overzicht vanuit juridisch perspectief", Intersentia, Antwerpen, 2020, p. 13; EPRS, Panel for the Future of Science and Technlogy, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019; World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C.,

essence, it can be defined by the following properties:[31]

- **transparent**: all participants to the blockchain can view all data recorded;
- **decentralised database**: several copies of the blockchain coexist on different computers, thereby creating a distributed ledger;
- **often structured as a chain of blocks**: a single 'block' of information groups together multiple transactions and is then added to the existing chain of blocks through a hashing process;
- **hashing and encryption**: the common techniques in the context of blockchain are cryptographic hash functions and asymmetric encryption;
- **irreversible**: once data is recorded, it cannot be altered or removed and;
- **disintermediation**: while transactions normally require the intermediation of a third party, blockchain allows to cut out the 'middle man' and have all decisions taken by consensus between the participants.

In terms of the categories of blockchain technologies, there are typically two general categories that need to be discerned:

a) Public / permissionless blockchain network; and
b) Private / permissioned blockchain network.

In a public or permissionless blockchain network, anyone can read and submit transactions to the blockchain without authorisation. However, private blockchain networks limit the participation thereto to specific people or organisations.

(b) *Blockchain and GDPR*

(i) *Pseudonimised, hashed and encrypted data – The question on "personal data" and blockchain*

As described above, the GDPR applies to the processing of personal data. The notion of personal data is crucial as it determines whether an entity processing data is subject to the various obligations the GDPR imposes on data controllers.

In the framework of the MDM, it is important to assess whether the data stored via a blockchain technology should be considered personal data. In this respect, it is worth noting that the GDPR takes a broad approach to the definition of personal data in order to ensure the full and complete protection of data subjects under data protection laws. That anonymised data, i.e. data

http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-DistributedLedger-Technology-and-Blockchain-Fintech-Notes.pdf, https://responsiblefinanceforum.org/wp-content/uploads/2018/04/Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf (last consulted on 29 March 2021).

[31] CNIL and EPRS, Panel for the Future of Science and Technlogy, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019

that has been irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the controller alone or in collaboration with any other party, [32] will not fall within the scope of the GDPR, is beyond dispute.[33] However, there is an ongoing debate as to whether data that once was personal but no longer is (as linkage to a natural person has been removed), is to be considered as personal data.

The application of DLT will result in personal data being pseudonimised, hashed or encrypted. Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information. Encryption and hashing are examples of pseudonymisation.[34]

The legal test to differentiate between personal and non-personal data is integrated in recital 26 of the GDPR:

> […] *To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.* […]

According to the GDPR, data is personal when the controller or another person is able to identify the data subject by using the 'means reasonably likely to be used'. The test as provided under recital 26 of the GDPR can be considered a risk-based approach: when there is a reasonable risk of identification, data should be treated as personal data. When that risk is negligible, data may be treated as non-personal data, even if identification cannot be excluded with absolute certainty.[35]

The European Court of Justice (CJEU) has adopted a broad approach to identifiability in the *Breyer* case, as it considered that the possibility to combine a dynamic IP address with the additional data held by an internet service provider, constitutes a means likely reasonably to be used to identify the data subject.[36] In addition, the Advocate General pointed out in his opinion which was followed by the Court, that it is also important to consider whether identification is reasonable.[37] As a result, data is not considered personal data if the identification of the data subject would be very costly in human and economic terms, or practically impossible or prohibited by law,

[32] ISO 29100:2011; Recital 26 GDPR, Article 29 Working Party, Opinion 05/2014 on Anonymization Techniques, WP 216; CJEU, C 582/14, Breyer v. Bundesrepublik Deutschland, 19 October 2016, nr. 42 – 43.
[33] Recital 26 GDPR.
[34] Recital 26 GDPR, Article 29 Working Party, Opinion 05/2014 on Anonymization Techniques, WP 216, 23.
[35] M. Finck and F. Pallas, They who must not be identified—distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, Volume 10, Issue 1, February 2020, 11 – 36.
[36] CJEU, C-582/14, Breyer v. Bundesrepublik Deutschland, 19 October 2016.
[37] Opinion of Advocate General, CJEU, C-582/14, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CC0582&from=EN (last consulted 29 March 2021).

resulting in an insignificant risk of identification.

Encrypted data cannot be connected to a specific individual without a decryption key. For the holder of the key, however, decrypting the data and identifying each data subject remains a rather simple task, given that the personal data is still present in the dataset that has been encrypted. As a result, encrypted data that can be used to re-identify someone, remain personal data and falls within the scope of the GDPR. This is also the view of the WP29: *'encryption may significantly contribute to the confidentiality of personal data if implemented correctly, although it does not render personal data irreversibly anonymous'.*[38]

In addition, identification will in most cases still be possible when using a cryptographic hash function, as the initial input for a particular record can be retrieved by applying the function repeatedly to random input values, especially when the input range is known.[39]

Nonetheless, as already emphasised above, whether pseudonimised data always remains personal data under the GDPR, is a matter of ongoing debate. Taken into account the above and the *Breyer* case as cited above, **whether encrypted, hashed or pseudonimised data are considered personal data will depend on many factors, such as whether it is possible to get access to the key, how good the encryption is, if additional privacy measures have been adopted or if the key has been removed** as this may reduce the reasonable likelihood of identification.[40] All in all, according to the Court of Justice, there is no personal data in situations where the identification is prohibited by law, or requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant (Breyer, par. 46). That being said, when data qualifies as personal data, even if the data controller does not himself have access to such data, all obligations under the GDPR apply.

It follows that it is necessary to determine, on a case-by-case analysis, whether specific data qualifies as personal data.

(ii) The qualification as controller or processor when processing data on a blockchain

As stated above, the question on whether a person acts as a data controller is to be determined on a factual basis, e.g. which person/entity is responsible for deciding how the data is processed, in particular the purposes and the means of processing. The CJEU has opted for a broad notion of the data controller to ensure effective and full protection for data subjects, any deviating contractual arrangements in this regard will not be decisive and can easily be

[38] Article 29 Working Party, Opinion 05/2021 on Cloud Computing, WP 196, 2012, p. 15.
[39] S. Bennis, "Consumentenbescherming bij blockchain en smart contracts", Intersentia, p. 30.
[40] EPRS, Panel for the Future of Science and Technology, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019.

overturned by a court.[41] Consequently and given (i) the decentralised data governance model used by DLT and (ii) the large number of actors involved in the processing of data, it is complex to discern the roles of data controller and data processor in the context of blockchain technology.

Whenever a person decides to use blockchain instead of any other form of database, it has made a decision on how to process personal data and thus on the means to be used. Such decision creates a strong indication that the person concerned would qualify as the data controller under the GDPR. [42] For example: a notary that records his or her client's property deed on a blockchain or a consortium that relies on blockchain to manage its accounts are likely data controllers as they have made the decision regarding the means as well as the purposes for the processing operations.[43]

A. The legal qualification of the MDM Operator

In the framework of the MDM, it can be argued that, if the MDM Operator would decide to set up a private blockchain for the MDM, whatever the purpose may be, the MDM Operator would qualify as the data controller for the processing of personal data that are taking place. This is particularly the case as the MDM Operator will be the one determining the means and the purpose for the global set of processing operations in the context of the MDM.

Should the MDM Operator be established as a consortium, such consortium would essentially be an association of several legal entities. If the legal entities in the consortium would jointly decide on the use of blockchain and purposes for its use, it would imply that all the participating legal entities could be considered joint controllers, as provided by Article 26 of the GDPR. Consequently, all such joint controllers must determine, in a transparent way, their respective responsibilities to ensure compliance with the GDPR.

However, should the participants decide to delegate the decision as regards to the use and purposes of blockchain to one entity of the consortium, arguably only the legal entity that has been mandated thereto, and in practice exercises the decision-making powers in an autonomous way, will be considered as a data controller under the GDPR.[44]

B. The legal qualification of the (MDM) Service Providers

When determining whether an (MDM) Service Provider acts as a data controller, the analysis must be done in relation to each personal data processing operation at stake. Consequently, (Mobility) Services Providers that have joined the MDM and are subsequently using the infrastructure for their own commercial purposes (thus enabling the DLT to process new

[41] CJEU, C-210/16, Wirtschaftsakademie Schelswigholstein, nr. 28.
[42] EPRS, Panel for the Future of Science and Technlogy, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019, p. 39.
[43] CNIL, "Blockchain et RGDP: quelles solutions pour un usage responsable en présence de données personnelles?" and EPRS, Panel for the Future of Science and Technlogy, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019, p. 39.
[44] CNIL, "Blockchain et RGDP: quelles solutions pour un usage responsable en présence de données personnelles?".

personal data) will in all likelihood also qualify as data controllers[45], the question being whether a qualification as joint controller with the MDM Operator also applies in parallel.

To summarize, when blockchain is applied in the specific context of an MDM, one might argue that:

- **Software developers of the DLT** are most likely to qualify as data processors. They have a limited role in determining the means of the processing and/or the purposes of a specific personal data processing operation. They simply provide an infrastructure that others can use to realize their own purposes.[46]
- **Miners, merely validating transactions** based on the software protocol, will not qualify as data controllers but will likely be processors or sub-processors. This view has also been confirmed by the French Data Protection Authority (the "**CNIL**").[47]
- **Nodes**: according to some legal scholars, the mere operation of a node is sufficient to qualify as a data controller. However, as certain other legal scholars already take the view, the mere operation of a node implies adding information to one's own copy of the chain, based on the underlying software protocol, and thus does not imply a choice of purpose or means of processing.[48]
- **Consumers/data subjects who put personal data on a blockchain**: will in at least some circumstances be considered as data controllers under the GDPR (for example, when a transaction is made directly by the user, the user undertaking the transaction will be the one determining the purposes and means of data processing), albeit they might be regarded as acting within the boundaries of personal or household activities, to which the GDPR does not apply.[49]
- **(Mobility) Service Providers** who subsequently use the infrastructure for their own commercial purposes (thus enabling the DLT to process new personal data), could also be considered data controllers;
- **MDM Operators:** who decide on the use and purposes of blockchain can be qualified as data controllers. If the MDM Operator consists of a consortium whereby the decision to use blockchain is taken jointly, the participants will be considered joint controllers unless in case the decision to use blockchain is delegated to a single member of the consortium.

(iii) GDPR challenges in the context of blockchains

[45] S. Bennis, "Consumentenbescherming bij blockchain en smart contracts, Intersentia, p. 30; CNIL, "Blockchain et RGDP: quelles solutions pour un usage responsable en présence de données personnelles?".
[46] EPRS, Panel for the Future of Science and Technlogy, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019, p. 46 – 47.
[47] EPRS, Panel for the Future of Science and Technlogy, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019, p. 46 – 47; CNIL, "Blockchain et RGDP: quelles solutions pour un usage responsable en présence de données personnelles?".
[48] Similar to users of social networks, who also do not, through their mere participation, become co-responsible for the processing of personal data taking place on that network. S. Bennis, "Consumentenbescherming bij blockchain en smart contracts", Intersentia, p. 254 – 255.
[49] EPRS, Panel for the Future of Science and Technlogy, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019, 47.

As set forth above, the GDPR imposes a number of obligations when processing personal data. When processing personal data through a blockchain, compliance with the legal obligations is sometimes challenging. This Section aims to address some of these legal challenges

A. Lawfulness, transparency, data portability and access rights

In principle, it appears that there are no specific technical limitations for data controllers using blockchain solutions to comply with transparency requirements, the right to data portability, the access right, as well as the principle of lawfulness. Consequently, the use of blockchain technology should in principle not preclude a data controller's compliance with these specific legal obligations.

B. Purpose limitation

Personal data on a blockchain are in principle accessible by any participant to the blockchain. The availability of such data to all participants on the blockchain might entail certain difficulties under the GDPR as it is difficult to reconcile with the purpose limitation principle as set forth under the GDPR.[50]

When personal data is made available to all participants on a blockchain,

i. it makes it difficult to anticipate all future uses of personal data; and
ii. one can hardly avoid that personal data on the blockchain ends up being processed in a way that was not envisaged by the controller and notified to data subjects.[51]

With these concerns in mind, personal data stored and made publicly available on the blockchain should be limited as far as possible. The data controller(s) will also need to implement contractual and possibly technical or organisational measures to ensure that the data available on the blockchain cannot be used for totally different purposes. The permissions and protocols to be decided upon by the members of the blockchain could indeed make it possible to prevent at least to some extent any reutilization of the personal data for other purposes.

C. The *right to be forgotten* and the *right to rectification*

In addition to the concerns regarding the purpose limitation, the use of blockchain also raises concerns as regards the *right to be forgotten* and the *right to rectification* (see Section 4.1.5(a) above).

The immutable nature of blockchains to ensure secure data integrity of the records in the chain and trust in the network, is a core idea within DLT. As a

[50] Article 5.1.(b) GDPR: The principle of purpose limitation requires that personal data be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
[51] CNIL, "Blockchain et RGDP: quelles solutions pour un usage responsable en présence de données personnelles?"

result, any (personal) data contained on the blockchain cannot be modified or deleted to meet GDPR requirements. Even if a new block is entered onto the chain with the correct information, the previous block (containing the incorrect data) remains. It is argued, however, that the essence of this right could be respected by alternative technical means. For example, the destruction of the private key, or the application of encryption measures similar to those used to "erase" personal data to the inaccurate block.[52]

D. Data minimisation

Another fundamental question arising in the context of blockchain is how to adhere to the principle of *data minimisation*, which requires that only data that is necessary for the processing operation is to be processed. Given that data and possibly personal data is continuously added to the blockchain often without a possibility of deletion or editing of such data, it raises the question as to what extent this is in line with the data minimisation principle under the GDPR. Given the ambiguity in this regard, further regulatory guidance on this topic more than welcome. In the meantime, it is strongly recommended that data controller(s) define upfront and in a precise manner the type and categories of personal data likely to be used in the context of the blockchain.

E. Appropriate security measures

Under the GDPR, the data controller and data processor must define and apply appropriate security measures (see Section 4.1.5(f) above). In the context of blockchain the French Data Protection Authority has opined that at least the following security measures should be implemented when processing personal data via DLT:

- Use strong, state-of-art encryption technologies (including hashing, digitisation and anonymization techniques) are to be used;
- Implement strong contingency plans to ensure that adequate operational and technical procedures to ensure the protection of personal data. In particular, blockchain operators should document any upgrade to the software used for conducting transactions and mining operations; and
- Ensure the security of secret keys when using DLT.

4.1.8. *Mitigating data protection challenges in the context of an MDM: some practical recommendations to be followed in the early stage*

As stated above, the GDPR imposes various legal obligations when processing personal data. Given the different roles of the participants in an MDM and the complexity of the technology used, such as blockchain technology, GDPR compliance of an MDM is not straightforward.

[52] EPRS, Panel for the Future of Science and Technology, "Study Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", July 2019, p. 46 – 47; CNIL, "Blockchain et RGDP: quelles solutions pour un usage responsable en présence de données personnelles?".

In light of the analysis set forth above, and in spite of there being a need to further define the various use cases of the MDM and to review these recommendations accordingly, an MDM Operator and essentially all other MDM participants could minimize legal risks under the GDPR by adhering to the following key principles:

1. **Data inventory / data mapping**: MDM Operators and (Mobility) Service Providers should conduct a data inventory/mapping to better understand which data will be processed in the framework of the MDM and whether sensitive data will be processed. The data inventory and mapping exercise should imply that:
    - MDM Operators and (Mobility) Service Providers should determine (i) which personal data they aim to process and (ii) on which legal basis such personal data will be processed.

    - MDM Operators and (Mobility) Service Providers should each determine and disclose to the other members of the MDM: (i) for which purposes they process such personal data, (ii) whether such processing is necessary for the envisaged purpose, (iii) how long such data needs to be retained and (iv) whether such retention period is proportionate in light of the purposes pursued. On the basis of such analysis, such MDM participants should draft their own data retention policy.

2. **Roles and responsibilities**: The MDM Operator must understand and assess the respective roles of the different participants to the MDM such as, its own role and the roles of the Service Providers and End-Users.

3. **Data Processing Agreements and terms and conditions:** The MDM Operator should draft terms and conditions for the MDM which impose limitations, commitments and liability obligations on the part of the (Mobility) Service Providers in order to provide further legal certainty to the MDM Operator with respect to the processing of personal data in particular but also other legal or contractual issues identified in this report.

4. **Data Protection Policies**: MDM Operators and (Mobility) Service Providers should comply with the transparency obligation and draft appropriate data protection policies;

5. **Data Subject Rights**: Based on the assessment of their legal qualification under the GDPR, MDM Operators and (Mobility) Service Providers need to decide who is the most appropriate party to respond to requests from data subjects exercising their rights and should implement appropriate procedures allowing for the effective exercise of such rights;

6. **Assignment of a DPO**: The MDM Operator and possibly each MDM participant should decide whether a DPO should be appointed for its

specific processing operations;

7. **Data Protection Impact Assessment:** The MDM Operator and possibly each MDM participant should determine if it needs to perform a Data Protection Impact Assessment;

8. **Data Register**: MDM Operators and (Mobility) Service Providers should have an appropriate data register in place;

9. **IT security**: MDM Operators and (Mobility) Service Providers must implement appropriate safeguards as regards IT security and confidentiality;

10. **Data Breach Notifications**: MDM Operators and (Mobility) Service Providers should put appropriate data breach notification procedures in place;

11. **Data Transfers**: MDM Operators and (Mobility) Service Providers should have appropriate data processing and data transfer agreements in place when engaging third parties for the processing of personal data;

12. **Blockchain:** When using blockchain, the MDM Operator using and/or proposing the blockchain should have the following security measures in place: (i) strong, state-of-art encryption technologies, (ii) contingency plans to ensure adequate operational and technical procedures to ensure the protection of personal data and (iii) ensure the security of secret keys.

13. **Data Minimisation**: MDM Operators and (Mobility) Service Providers should only process those personal data that are necessary and proportionate in light of the aim pursued. If appropriate and possible, it is highly recommended to store personal data off-chain as much as possible, to facilitate GDPR compliance.

4.2. Intellectual Property Rights

This Section aims to (i) clarify the different intellectual property rights that are relevant in the context of MDMs (see Section 4.2.1 below), (ii) assess to which extent such intellectual property rights can be applied in the context of an MDM (see Section 4.2.2 below) and (iii) provide guidance on how to tackle specific intellectual property rights issues in the context of MDMs (see Section 4.2.3 below).

4.2.1. *Introduction*

As part of the MDM, various data sources such as the MDM Operator, End-Users and the Service Providers including Mobility Service Providers will share significant sets of data with the MDM. Depending on the specific use cases for the MDM, these data can include among others geo-positioning data, data regarding means of transport, vehicle information and other types of data.

With regard to the protection of intellectual property rights in this "information system", the following types of intellectual property rights are particularly relevant (i) copyright protection, (ii) database rights and (iii) trade secrets.

(a) Copyright Protection

Within the European Union, the protection of copyright is granted by among others Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society[53]. Further thereto and further to established case-law of the European Court of Justice, copyright protection can be granted to "works" provided that such works are (i) *original* and (ii) *fixated or expressed in a tangible form*.

> *"29. The concept of 'work' that is the subject of all those provisions constitutes, as is clear from the Court's settled case-law, an autonomous concept of EU law which must be interpreted and applied uniformly, requiring two cumulative conditions to be satisfied. First, that concept entails that there exist an original subject matter, in the sense of being the author's own intellectual creation. Second, classification as a work is reserved to the elements that are the expression of such creation (see, to that effect, judgments of 16 July 2009, Infopaq International, C-5/08, EU:C:2009:465, paragraphs 37 and 39, and of 13 November 2018, Levola Hengelo, C-310/17, EU:C:2018:899, paragraphs 33 and 35 to 37 and the case-law cited)."* (Case C-683/17 Cofemel–Sociedade de Vestuário v. G-Star Raw) [54]

As clarified by the European Court of Justice in *Cofemel–Sociedade de*

[53] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0029 (hereinafter the "**InfoSoc Directive**") (last consulted 29 March 2021).
[54] Case C-683/17, Cofemel–Sociedade de Vestuário v. G-Star Raw, EU:C:2019:721.

Vestuário v. G-Star Raw (as cited above), the originality requirement implies that, in order to be eligible for copyright protection, the work concerned must be the result of the author's "*own intellectual creation*".

In addition thereto, the work concerned must also be *fixated or materialised*, in the sense that it must be an *expression*. Consequently, a mere idea that is not materialised, is not eligible for protection under copyright law.

When it comes to the copyright protection of data in itself, such data can only be protected by copyright to the extent that such data is "original". This originality requirement requires an intellectual human intervention and the consciousness of achieving a result.[55] As raw data such as numbers and / or factual data typically do not meet this requirement, it is in practice rather difficult to claim copyright protection on raw data.

Regarding software, however, the copyright protection will generally be available and cover the object and source code as well as the preparatory design materials. The choices made by the maker of the computer program will be deemed original, unless they are purely driven by technical considerations that exclude any margin of creativity, typically in situations where there is one single way of addressing a given functionality or business requirement. In other words, the MDM in itself and the software layer supporting the blockchain could be regarded as original works of authorship and be protected as software, subject of course to demonstrating that they have been newly created and not merely copied from an existing source. Even the implementation of existing instructions, standards or rules and procedures can give rise to a protected subject matter, to the extent it is an original computer program that results from the efforts and the choices made by the developer. Lastly, the graphical user interface of a computer program will generally be regarded as a separate work protected by general copyright.

(b) *Database Rights*

Aside from the question on whether (raw) data itself can be protected by copyright, one also needs to assess whether collections of data are eligible for protection. In this context, the European Union has adopted the Database Directive[56].

The Database Directive applies a dual protection mechanism. One the hand, the Database Directive applies copyright protection to databases that have an "*original structure*". On the other hand, the Database Directive also provides a *sui generis right* which aims to protect the rights of those who have made a *substantial investment* in obtaining or creating a database.

[55] Y. Benhamou, *Licensing Big Data: holistic analysis based on a three-step approach*. p. 6, https://www.researchgate.net/publication/339140374_Licensing_Big_Data_a_holistic_analysis_based_on_a_three-step_approach (last consulted 29 March 2021).

[56] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20, 27.3.1996, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML (hereinafter the "**Database Directive**") (last consulted 29 March 2021).

(i) Copyright protection of databases

Further to Article 3 (1) of the Database Directive, databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. Consequently, in order to be eligible for database protection, the author of a database must be able to demonstrate that the manner in which it has selected or arranged the individual data, is original.

In practice, the protection of "original" structures of databases will often be combined with the protection of software as copyrighted works.

(ii) Sui generis protection for investment in producing databases

To the extent that a database in itself would not be eligible for protection under copyright, the Database Directive also provides for a *sui generis* protection. The *sui generis* protection, which is set forth in Article 7 of the Database Directive, allows the maker of a database to oppose, under certain circumstances, to the extraction and/or re-utilization of the whole or of a substantial part of its database.

In order to benefit from the sui generis right, the maker of the database must demonstrate that there has been *qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents* of the database concerned.[57]

(c) Trade Secrets

Aside from potential copyright protection and database protection, data may be protected as a trade secret. In order to be eligible for protection as a trade secret, the data concerned must (i) be *secret*, (ii) *have commercial value* because of its secrecy and (iii) have been subject to reasonable *steps to protect its secrecy*.[58]

The regime on trade secrets differs from copyright protection and database protection. Whereas the copyright and database regimes aim to create an exclusivity and protect against the unlawful dissemination and use of the data, a trade secret primarily aims at protecting the secrecy of such data.[59] Consequently, the scope of the protection as a trade secret is fairly limited as it only protects against unlawful use or disclosure of confidential information by illegitimate means. Moreover, once the data set is disclosed, one can no

[57] Article 7 (1) Database Directive.
[58] Y. Benhamou, Licensing Big Data: holistic analysis based on a three-step approach. p. 8, https://www.researchgate.net/publication/339140374_Licensing_Big_Data_a_holistic_analysis_based_on_a_three-step_approach (last consulted 29 March 2021).
[59] *Ibidem.*

longer claim the protection under the trade secrets regime.[60]

4.2.2. *Intellectual Property Rights in the context of MDMs*

(a) Intellectual Property Rights in geolocation data

One of the main characteristics of the envisaged MDM is that there will be an exchange of *raw* geolocation data between different actors such as End-Users, (Mobility) Services Providers and MDM Operators. Such raw geolocation data will at least include geo-positioning information provided by the GALILEO GNSS further to the use of for instance trilateration, such as timestamps and geographical coordinates.

(i) Copyright protection

Although the GNSS technology as such might be eligible for the protection by copyright or other intellectual property rights (e.g. patents), the individual *raw* data they generate is not necessarily protectable under copyright. As the individual raw data such as geographic coordinates or timestamps of a signal are typically not the result of an author's own intellectual creation, such raw data are in principle not eligible for copyright protection.

(ii) Database protection & sui generis protection

Albeit that individual geolocation data might in principle not be eligible for copyright protection, it does not preclude the protection of the set of data (collection of data) as either (i) a protectable database or (ii) under the *sui generis* right.

As part of the MDM, a significant set of geo-positioning data will essentially be machine-generated data generated by the GNSS and individual IoT devices such as the on-board units of vehicles.

The creation of such IoT devices and on-board units typically requires a substantial investment. However, such investment is generally not considered to be relevant for the protection under the *sui generis* right as the European Court of Justice requires that an investment is made rather *in resources used to seek out existing independent materials and collect them in the database* as opposed to the resources used *for the creation of materials which make up the contents of a database*.[61]

Although this requirement impacts the possibility to claim for a sui generis protection of *raw* data generated, it does not preclude

[60] *Ibidem.*
[61] Case C-46/02 Fixtures Marketing Ltd v. Oy Veikkaus AB [2004] ECLI:EU:C:2004:694, http://curia.europa.eu/juris/document/document.jsf?text=&docid=49636&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1378242 (last consulted 29 March 2021).

such *sui generis* protection, to the extent that the participant to the MDM can, independent from the resources used to create the content, demonstrate that it has made a substantial investment (either qualitative and/or quantitative) in the obtaining, verification or presentation of the content. Consequently, if the person concerned such as, for instance the MDM Operator, is able to demonstrate that it has made a substantial investment in obtaining, verifying and/or structuring and presenting the underlying data, it could still claim a *sui generis* protection for such data. This is particularly the case in the context of so-called "non-sole-source databases" where the issue of exclusive access to the raw data is less apparent.

(iii) Trade secrets

As stated above, geolocation data might theoretically be eligible for the protection as a trade secret to the extent that the data (i) is kept secret, (ii) has commercial value and (iii) the data source has taken reasonable steps to keep such data secret. Not only the data in itself, but also the information on how best to process and use such data, can be protected as trade secrets.

(b) Intellectual Property Rights in data provided by data sources

Depending on the specific use cases of the MDM, Service Providers will provide and/or use sets of raw data other than geolocation data. Such raw data sets might relate to End-User personal data, financial information, transactional data (e.g. blockchain data) or other types of data. In this case, the question on whether or not such raw data is eligible for copyright protection or database protection primarily depends on whether such data or the structuring thereof (in case of databases), is *original* (see Section 4.2.1(a) above). In many cases however, raw data will not pass the originality test and are therefore not protectable by copyright.

Conversely, the question on whether or not such raw data are eligible for protection under the *sui generis* right, depends on the level of investment made for *the acquisition, verification and structuring* of such data (see Section 4.2.2(a)(ii) above).

(c) Intellectual Property Rights and Big Data

Although the MDM primarily relies on the exchange of raw data, one must not neglect the added value and alternative revenue streams that might be generated on the basis of data that is derived from such raw data (the "*derivative data*"). In the context of the MDM, it is possible that, on the basis of certain raw geolocation data, one could derive specific patterns and link specific conclusions to such patterns or generate additional derivative data on the basis thereof. Such process, whereby pre-existing data is analysed as to subsequently generate specific output data, is generally referred to as Big Data.

The use of Big Data in the mobility industry is a proven concept. Currently, there are a number of providers of mobility solutions, including for instance the mobile app Waze[62], who use Big Data as part of their business model.

Depending on the specific use cases defined, Service Providers may use Big Data to develop alternative data analysis methodologies and new data sets. If such analysis methodology and the derivative data created therewith are "original", such methodologies and data may be protected by copyright. Moreover, even if such data sets of derivative data are not original, it does not preclude that they might be eligible for protection under the database right or the *sui generis* right.

Lastly, if such data meet the requirements of a trade secret, they may also be protected under the trade secrets regime.

4.2.3. ***Tackling key issues with regard to intellectual property rights***

(a) *The monopoly created by intellectual property rights*

Intellectual property rights are essentially property rights that, subject to certain exceptions, allow the holder(s) thereof to exercise a monopoly on the use of a creation for a specific period.[63]

In the context of the MDM, the monopoly created by potential intellectual property rights on data sets, allows the owner hereof to license the same data sets and potentially impose additional obligations such as the application of specific protocols or constraints on the reutilization of the data. As the operation of the MDM essentially relies on the exchange of data between the participants in the MDM, it is imperative that specific usage rights for such data are granted to the participants of the MDM.

(b) *Trade secrets and MDMs*

As stated above, the trade secret protection implies that the data to which such trade secret would apply, are kept confidential. However, as part of an MDM, one of the key benefits is that data is exchanged between the different participants as to allow them to benefit from such data and offer alternative mobility solutions. Consequently, as part of an MDM, it would be appropriate to carefully assess which types of information and potentially which data sets are to be kept confidential and which are to be shared as part of the MDM, be it under a clear commitment to confidentiality and an "embargo" style obligation to prevent harming the legal protection attached to trade secrets.

(c) *How to tackle such key issues*

As to avoid that the monopoly rights created by intellectual property rights

[62] https://www.waze.com/
[63] R. S. Khemani and D. M. Shapiro, 'Glossary of Industrial Organisation Economics and Competition Law' (OECD 1993) http://www.oecd.org/regreform/sectors/2376087.pdf (last consulted 17 March 2021).

would interfere with the operation of the MDM, one could envisage either (a) a licensing model for the participants of the MDM or (b) a transfer of the intellectual property rights concerned to the MDM.

Although a transfer of intellectual property rights to the MDM would provide the most legal certainty for the MDM Operator and other participants in the MDM, such an approach might have an adverse consequence for the MDM from an operational perspective. As some Service Providers might have invested substantially in the creation or obtaining of specific data sets, they might be rather reluctant to transfer such rights to the MDM.

An alternative and typically more suitable solution would be to adopt an appropriate data licensing model for the MDM. This licensing model could imply that every MDM Service Provider who aims to use the MDM, either by offering services on the MDM or by using data of the MDM, agrees to grant the MDM and other Service Providers a broad license to use the data concerned for the purpose of the MDM. The specific modalities of such license, such as for instance the specific purposes for which such data can be used, the geographic scope and duration of the license, can be further defined once the specific use cases of the MDM are defined.

4.3. Smart contracts using MDMs

4.3.1. *What is a Smart contract*

Smart contracts are defined as 'contractual type arrangements', an incorporation of contractual clauses, through computer language, into computer software or protocols. They have the characteristic of executing themselves automatically on the basis of specific conditions predetermined by the parties.

In other words, the smart contract is based on a code that reads the clauses that have been agreed and the operational situations in which the agreed conditions must occur. The code executes itself automatically when the data referring to the actual situations match those referring to the agreed conditions and clauses. As a result, smart contracts are not a real contract. As its inventor, lawyer-computer scientist Nick SZABO explained in 1994[64], it is a "*computerized transaction protocol that executes the terms of a contract"*.

To illustrate the functioning of a smart contract, SZABO uses the simple vending machine example where the sale takes place at the moment when the user pays the price of the selected product. At that moment, the vending machine, which has been programmed to release the product upon payment of the relative price, releases the requested product, if the payment condition is fulfilled. Similarly, smart contracts automatically perform actions (or arrange for certain actions to be performed), according to the terms defined by the parties.

In essence, a smart contract can be described as a code or software program:[65]

- that is stored and executed in a decentralised manner, without intermediaries, on different nodes that are interconnected in a network and belong to different individuals (disintermediated peer-to-peer network);
- which independently executes "if this then that" commands, as a result of which agreements are automatically executed (self-executing);
- where (as a condition precedent) the transfer of value (e.g. payment from customer to supplier) can only take place when validated within the computer network;
- that conforms to the rule of code is law[66]; and
- which is immutable: once the smart contract has been validated and added to the blockchain, it can, in principle, no longer be retracted. In

[64] N. SZABO, "Smart Contracts", 1994, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (last consulted 17 March 2021).
[65] P-J. Aerts, F. Hoogendijk and N. Vandezande, "Smart contracts, een overzicht vanuit juridisch perspectief", Intersentia, Antwerpen, 2020, p. 59; T.J. DE GRAAF, "Van oud naar nieuw: van internet naar smart contracts en van mensen naar code (I), *WPNR* 2018, 494.
[66] This means that within a smart contact, the code or software replaces the law. Trust in the law would no longer be necessary now that one has the certainty of execution through the code. However, in legal terms, this means that the parties accept that smart contracts will self-implement themselves without the need for external enforcement mechanisms (e.g. a court injunction).

other words, once the triggering event occurs, no one can prevent the execution of the terms contained in the smart contract.[67]

The most common examples of smart contracts are associated with blockchain platforms such as Ethereum and Bitcoin.

4.3.2. *Legal implications of smart contracts - Validity and enforceability*

Smart contracts raise many questions, for example, if smart contracts can be considered as a legally binding contract? Currently, the answer will depend on a number of factors: (i) the applicable contract law[68], (ii) the characteristics of the smart contract concerned and (iii) the factual context.

Firstly, to determine whether a smart contract can give rise to a legally enforceable contract, it is important to emphasise that this cannot be answered in general but always requires an assessment whether each of the elements necessary for a legally binding contract are met under national law.

In Belgium, for example, a contract can be concluded verbally or digitally and, in our opinion, certainly also on the basis of a computer code in a smart contract, since Belgian law generally does not require any specific formalities for a contract to be formed (with a few specific exceptions for certain contracts which do require specific formalities). In the absence of such a formal requirement in the law, a contract concluded electronically is as valid as a written or oral contract. Of course, the general requirements for having a valid agreement must also be taken into account. For example, under Belgian law, the following cumulative and constitutive conditions must be fulfilled for an agreement to be valid: (i) the parties have freely consented to the contract, (ii) they have the capacity to enter into the agreement, (iii) the contract has a specific and legal object and (iv) there is a legitimate cause. In principle, these principles can be met equally well with smart contracts. However, a smart contract as a legally binding agreement may give raise to specific difficulties:

(i) *Consent*

Several legal scholars raise the question: How do we know that the contracting parties have actually understood the programming code and thus the content of the contract? For two programmers this will probably be the case, but for others, non-professionals, it is almost impossible to understand the computer code. In our opinion, a smart contract concluded electronically by means of a code rather than by means of a language immediately understandable to all participants, does not a priori affect the validity of the contract, as long as the parties agree (i) to record their legal relationship in computer language and (i) to the

[67] F. Lefèvre and N. Delwaide, "Resolving Smart Contracts' Disputes Through Arbitration: Thoughts and Perspectives", Kluwer, 223 – 237.
[68] Please note that a comparative analysis of the legal regimes as regards the enforceability of smart contracts within the different member states, is outside the remit of this study.

execution in the smart contract system. As mentioned, the principle is that a contract can be concluded without any formal requirements, unless the law provides otherwise. As long as the parties to the smart contract have sufficient knowledge to understand their commitments and the terms thereof, which are contained in lines of code, there should be no problem with regard to the requirement of freely given consent for a smart contract to be recognised as legally binding.[69]

(ii) Legal capacity to enter into a contractual relationship.

Another possible issue is the question of the identity of the parties. To assess – at a later time - whether the contracting parties freely consented and whether they had the capacity to do so, they must be identified or at least identifiable. Currently, this is not guaranteed under the current form of smart contracts, as parties are often not known under their true identity, but under a pseudonym. Nevertheless, a more nuanced view should be considered, as the essence is that a party is identifiable, which does not always require knowledge of one's true identity. For the sake of completeness, with regard to more complex contracts, knowledge of one's real identity is often essential (e.g. if further investigation of the parties is required or if the identity of the party is essential for the agreement and for the assessment of consent and legal capacity). Moreover, there may be regulatory or legal obligations that require knowledge of the identity. For instance, under Belgian Law, an information society service provider must provide the recipients of its services and the competent authorities with its name and business name.[70] Consequently, certain measures are required to ensure that the identity of parties to a smart contract can be established with sufficient certainty. This will be particularly relevant in the case of public smart contracts. Possible remedies include, for example, adapting the management rules of a smart contract so that parties to a particular contract can access the identity of the other contracting party or confirming the identity of the parties off-chain, for example, by using a trusted third party.[71]

(iii) The signature requirement

Another question affecting whether a smart contract is legally binding relates to the obligation in certain jurisdictions that a contract must have a valid signature in order to be binding. Without going into further details, it should be mentioned that an electronic signature has the same probative force as an ordinary

[69] P-J. Aerts, F. Hoogendijk and N. Vandezande, "Smart contracts, een overzicht vanuit juridisch perspectief", Intersentia, Antwerpen, 2020, p. 89, H. Jacquemin, A. Cotiga and Y. Poullet, Les blockchains et les smart contracts à l'épreuve du droit, Larcier, Namur, 2020, 161;
[70] Article XII. 6 Code of Economic Law.
[71] P-J. Aerts, F. Hoogendijk and N. Vandezande, "Smart contracts, een overzicht vanuit juridisch perspectief", Intersentia, Antwerpen, 2020, p. 91-92.

written signature, provided that (i) the signature complies with the requirements of Article 3(10), 3(11) and 3(12) of the Regulation on electronic identification and trust services for electronic transaction in the internal market (the "**eIDAS Regulation**")[72], (ii) the person from whom the writing originates can be identified and (iii) the writing has been made and preserved in conditions which ensure its integrity (i.e. guarantee that the statement was actually made by that party).

In this context, it is important to consider the question whether smart contracts can be considered as electronic contracts, and thus be treated in certain jurisdictions as equivalent to a traditional written contract on the basis of the functional equivalence approach. The rules for this vary from country to country. As far as Belgium is concerned, the following elements should be considered for the establishment of electronic contracts:

(a) the requirement of writing shall be complied with by a sequence of intelligible marks that are accessible to a later consultation, irrespective of the support or the methods of transmission thereof;
(b) the explicit or implicit requirement of a signature shall be complied with when the signature complies with the requirements of the qualified electronic signature (eIDAS Regulation);
(c) the requirement of handwritten wording by the party that binds itself may be complied with by any other means that warrants that the statement is effectively made by that party.

When analysing the functional equivalence under Belgian Law in the context of smart contracts, we note that the main issue relates to readability/intelligibility. The code used in smart contracts is not always directly understandable by humans, but only to the computer. To the extent that it is readable to some degree (e.g. source code), this is often difficult to understand for non-professionals (see above). From a Belgian point of view, in principle, smart contracts are not per se considered as an equivalent of a written instrument, but there is no objection to qualifying it as a written instrument if all the conditions are met.[73]

(iv) Evidence

Although, even when national law provides for a consensual approach and does not require a written document for the formation of a valid agreement, a written document can still be a

[72] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
OJ L 257, 28.8.2014, p. 73–114, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (last consulted 29 March 2021).
[73] P-J. Aerts, F. Hoogendijk and N. Vandezande, *Smart contracts, een overzicht vanuit juridisch perspectief*, Intersentia, Antwerpen, 2020, p. 100.

practical requirement for proving the existence of a smart contract and the intention to create a binding legal obligation. At the moment, there is uncertainty as to whether smart contracts can meet the legal requirements of the various EU jurisdiction in order to be considered a mode of proof. Under Belgian Law, there is no text recognising the blockchain or a smart contract as a method of proof. However, we believe that there is no contradiction between the existing principles in Belgian Law and the fact that evidence from the blockchain/smart contract could be legally produced in court: (i) there is no contradiction with the Belgian Civil Code rules to recognise blockchain or smart contracts as an admissible mode of proof in legal proceedings and (ii) the evidence is free between and against enterprises and between and against non-enterprises for legal acts under certain conditions. In addition, according to Article 25 of the eIDAS regulation, an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form (a smart contract via the blockchain may be considered an electronic contract in certain jurisdictions, based on the functional equivalent approach[74]). It should be noted that it may be possible for contracting parties to include deviating evidence clauses, insofar as the law of evidence is not of mandatory law or public policy (*ordre public).* Such deviating provisions may relate to the burden of proof, the subjective burden of proof, the means of evidence to be used, their probative value and/or the assessment of evidence by the court.[75]

4.3.3. *Smart contracts in the context of an MDM*

As part of an MDM, there are a number of use cases which would allow for the use of smart contracts and DLT. Although a technical analysis on how such smart contracts and DLT would be used as part of an MDM would fall outside the scope of this study, one could envisage that DLT and/or smart contracts could be used for the contracting process between different MDM participants.

In this context, one could envisage that an End-User would enter into an agreement with the MDM Operator and/or the Service Provider concerned on the basis of a smart contract.[76] In addition, one could also envisage a use case whereby financial transactions (e.g. remuneration for vehicle sharing or damages to vehicles etc.) between the End-User and the MDM Operator and/or Service Provider are based on smart contracts and/or DLT or blockchain technology.

[74] Article 15 of the Belgian Code of Economic Law foresees the rule of "functional equivalence" according to which a form requirement is not defined by reference to a specific process but with regard to the functions it allows fulfilling.
[75] P-J. Aerts, F. Hoogendijk and N. Vandezande, *Smart contracts, een overzicht vanuit juridisch perspectief*, Intersentia, Antwerpen, 2020, p. 112-113.
[76] In the context of smart mobility, there are blockchain and smart contracting implementations. An examples thereof is the BikeBlockchain project in the Netherlands (https://www.channelweb.nl/artikel/informatie/overheid/6017165/5412796/bikeblockchain-helpt-rdw-met-fietsregister.html) (last consulted 24 March 2021).

As stated above, the use of smart contracts and/or blockchain technology is not per definition precluded for demonstrating the validity and enforceability of such transactions. However, as the legal approach towards the use of smart contracts and their validity and enforceability under national law is not fully harmonised within the European Union, it is recommended that, if the MDM Operator aims to use smart contracts for a specific geographical market, it would assess the legal requirements and enforceability of such smart contract under the national laws of the geographical market concerned.

4.4. Upcoming legal challenges: MDM and the Digital Services Act

4.4.1. *The Digital Services Act as a game-changer for marketplaces*

On 15 December 2020, the European Commission published the first draft of the long-awaited Digital Services Act[77] ("**DSA**") and Digital Markets Act[78] ("**DMA**"). Both legal instruments form part of the European Commission's broader digital strategy, called *Shaping Europe's Digital Future*, and primarily aim to tackle certain shortcomings of the e-Commerce Directive and allow for more specific regulation for large online platforms.

(a) *Rationale – Why is there a need for a Digital Services Act?*

As (i) the digital economy, (ii) the use of online marketplaces and (iii) social networks has grown significantly over the last twenty years, the abuse of such new technologies, such as the dissemination of illegal content, has also increased significantly. Although the e-Commerce Directive[79] provides for mechanisms allowing to tackle certain abuses on online platforms, many European Member States considered such measures insufficient as to effectively tackle these issues.

In addition, since the majority of union citizens are now using online platforms and technologies that were inexistent in the year 2000 when the e-Commerce Directive was adopted, it became clear that certain consumer protection mechanisms of the e-Commerce Directive, were insufficient to tackle the challenges posed by such new technologies. This is particularly the case for the lack of transparency by many digital service providers when they apply *decision-making* and *content moderation algorithms* on their platforms and marketplaces.

Given these challenges, the European Commission felt a compelling need to provide for more and better regulation of digital services through the adoption of a Digital Services Act.

[77] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM (2020) 825, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72148 (last consulted 29 March 2021).
[78] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM (2020) 824, https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf (last consulted 29 March 2021).
[79] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN (last consulted 29 March 2021).

Although the published version of the Digital Services Act is only a first draft and it is unknown as to when the final text will be adopted, it is nevertheless relevant in the context of the MDM as it will most likely also apply to the MDM. In light thereof, this Section provides a brief summary of certain key aspects of the Digital Services Act.

(b) *Is the DSA applicable to MDMs?*

(i) *The applicability of the DSA on online marketplaces*

The DSA aims to apply to a broad range of online service providers. In that respect, it applies to providers of so-called "*intermediary services*", such as *caching*, *hosting* and *mere conduit* providers (Article 2 (f) DSA) and "*online platforms*" (Article 2 (h) DSA). Given the very broad notion of *intermediary services* and *online platforms*, the DSA will typically apply to a broad spectrum of digital operators including traditional hosting providers such as webhosting and cloud providers, providers offering consumer based platforms such as social media providers and online marketplaces.

As many providers of online marketplaces are established outside the European Union, the DSA aims to have an extra-territorial effect. Consequently, it applies not only to online marketplaces established in the European Union, but also to the online marketplaces established outside the European Union having a so-called *substantial connection* with the European Union whereby they offer their services in the European Union.

Although the DSA has a broad scope of application, it does clarify that certain obligations (including the obligations regarding compliant-handling and out-of-court dispute settlement – see below point 4.4.2(b)), will not apply to online platforms and marketplaces that are considered to be small and micro-enterprises further to Recommendation 2003/361/EC.[80] In this respect, online marketplaces that meet the criteria for a small enterprise, being an enterprise who employs less than 50 employees and has an annual turnover or total balance sheet of less than 10 million euro, would not be obliged to comply with these specific obligations. This exemption would also apply to online marketplaces who are considered microenterprises and therefore employ less than 10 employees and have an annual turnover or balance sheet of less than 2 million euro.

In addition, the DSA also states that online platforms for which the storage or dissemination of content is *purely an ancillary feature* of their service and for which their *service would not function without the storage and dissemination of content*, would not be considered an online platform under the DSA.

Lastly, the DSA imposes additional obligations on so-called *very large platforms*. Such very large platforms are defined as platforms with more than 45 million active users per month on average.[81]

[80] Article 16 DSA: "*This Section shall not apply to online platforms that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC.*"
[81] Article 25 DSA.

(ii) Illegal content under the DSA

As regards the subject matter of the DSA, it primarily relates to the dissemination of so-called *illegal content.* Further to Article 2 (g) of the DSA, illegal content means "*any information which, in itself or by reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law*".

4.4.2. ***Key obligations under the DSA***

The proposed DSA clearly indicates that it aims to impose a number of new obligations upon online marketplaces. Certain key obligations that are included in the current proposal are further specified in this Section.

As the DSA has not yet been adopted, this section does not intend to provide an exhaustive analysis of the DSA nor to provide an exhaustive of list all the relevant obligations under the DSA.

(a) *Liability and transparent notice and takedown*

In terms of liability for intermediary service providers, the DSA essentially confirms the regime of the e-Commerce Directive and the current case-law of the European Court of Justice in this regard. However, as to facilitate combatting the dissemination of illegal content, the DSA also imposes additional obligations on intermediary service providers such as marketplaces which go beyond the requirements that were imposed under the e-Commerce Directive.

One of the key obligations imposed upon hosting providers and online platforms such as marketplaces is to provide clear and user-friendly notice and takedown mechanisms allowing for the notification of illegal content.[82]

Should an online marketplace decide to remove or disable access to certain content, it is also required to inform the recipients concerned of its decision to delete or make such content unavailable. Such information should be provided at the latest upon the actual deletion or disabling of the illegal content and should provide a clear statement of reasons underlying the decision.[83]

(b) *Internal complaint-handling system and out-of-court dispute settlement*

The DSA obliges operators of online platforms, including online marketplaces, to provide for a compliant-handling system. This compliant-handling system enables individuals whose content has been removed or rendered inaccessible or for which the service has been suspended or terminated, to lodge, free of charge, an electronic complaint against such

[82] Article 14 DSA.
[83] Article 15 DSA.

decision. The online marketplace must further ensure that such complaint-handling system is easily accessible and user-friendly.[84] Moreover, the online platform shall handle such complaints in timely, diligent and objective manner.

Lastly, should a user of a service fail to agree with the decisions taken by the online marketplace as part of the compliant-handling system, it shall be entitled to select any out-of-court settlement procedure that will be certified further to the DSA.[85]

(c) *Measures and protection against misuse*

Under the DSA, operators of online marketplaces should also implement appropriate measures to protect against misuses on their platform. Should an End-User frequently disseminate illegal content via the online marketplace, the online marketplace operator is entitled to suspend access for a reasonable period after having issued a prior warning. Conversely, it shall equally suspend access to End-Users who frequently issue unfounded requests for the takedown of illegal content.[86]

(d) *Reporting obligations*

Online platforms are required to regularly report on a variety of topics including the number of disputes submitted to the out-of-court settlement, the number of suspensions imposed and the use of automated means as regards contents moderation.

(e) *Very large platforms*

In addition to the obligations set forth above, the DSA imposes specific obligations on so-called "very large online platforms". Very large online platforms are platforms that have on average more than 45 million active users per month. Given their overall importance in the information society, such very large platforms are among others required to:

- **Perform a risk assessment**: Very large platforms should perform risk assessments on the systemic risk resulting from the use of their online platform. In such risk assessment, they shall consider among others, the dissemination of illegal content through their platform, negative effects on the exercise of fundamental rights and the intentional manipulation of their services through for instance "fake news";
- **Provide transparency on recommender systems**: When using algorithms to recommend specific content to specific users, providers of very large platforms are required to clearly state the parameters used in their recommender systems and allow users to modify or influence such parameters;

[84] Article 17 DSA.
[85] Article 18 DSA.
[86] Article 20 DSA.

- **Appoint a Compliance Officer**: Very large platforms are also required to appoint an internal or external compliance officer to oversee the compliance with the DSA. Just as it is the case under the GDPR, compliance officers are required to have the proper qualifications to exercise this task.

(f) *Enforcement and sanctions*

The DSA strongly focusses on its enforcement. It requires European Member States to appoint a so-called Digital Services Coordinator who will oversee compliance on a national level and designate platforms as a "very large platform operator". In addition, the DSA also imposes strict sanctions as non-compliance with the DSA can lead to fines of up to 6% of the annual turnover of the provider.

4.4.3. *Implications for an MDM*

Although the DSA has not yet been adopted, it does provide some guidance on the new regulatory regime that will apply to providers of intermediary services.

As the MDM is essentially a marketplace whereby the MDM Operator would, as a core service, store data generated by users and devices, the MDM could in principle fall within the scope of the DSA and, in such case, should comply with the DSA's requirements, some of which are specified above.

Since the obligations of the DSA primarily aim at tackling the dissemination of *illegal content*, it is not, at this stage, entirely clear how such requirements would apply in the context of an MDM. Taking into account that the primary goal of the MDM would be to make available geolocation and related data to the End-Users and Service Providers, it is rather difficult to apply the obligations of the DSA in this specific context.

However, depending on the specific use cases for the MDM, one might envisage scenarios where End-Users and Service Providers could disseminate content other than raw geolocation and related data, or make an illegal use of the data rendered available by the MDM. In such situations, the risk that so-called illegal content would be shared by such End-Users or Service Providers, would evidently increase.

In any case, should the DSA in its current state become effective, the MDM Operator would most likely need to ascertain that its organisation and procedures comply with the requirements of the DSA, as further clarified above.

5. Ethical Challenges when operating MDMs

5.1.1. *Big Data, AI and profiling*

(a) *General*

The term Big Data is widely used and has a number of meanings. In practice, the term is associated with organisations manipulating large amounts of data via the use of artificial intelligence systems ("**AI systems**"). Big Data and AI systems open up new opportunities for organisations around the world to improve their services and develop new products. To illustrate, big data analytics can lead to a better understanding of customers behaviour and preferences, provide new information on mobility and economic activity, and reveal trends and correlations within and across large data sets that would otherwise be unknown. The value of such AI systems, therefore, lies not only in their ability to process the data elements in large data sets, it also lies in their ability to spot and correlate patterns in such data and learn from them.

In the framework of an MDM, Big Data can be of great value: data produced by End-Users and (Mobility) Service Providers at either end of the chain, can be shared among all MDM participants, allowing them to improve how they perform their roles. Moreover, the data can be exploited to improve services, deliver a better customer experience, and increase revenue. To make this possible, suitable infrastructure and frameworks both within the ecosystem and externally, must of course be implemented.

Not surprisingly, the use of Big Data and AI systems raises several concerns:

- **Privacy,** as the use of AI systems and Big Data means that large amounts of data about users are collected and used. Privacy is not only an ethical imperative but also an enforceable fundamental right in the EU. As privacy and data protection have already been extensively dealt with above (see Section 4.1 above), we will not address this in detail in this Section. However, it should be noted that the privacy and data protection concerns regarding Big Data will mainly relate to: (i) the basic principles of data minimisation, transparency, storage limitation and the strict necessity requirements of article 5 GDPR, (ii) having a legal basis under article 6 GDPR (if sensitive data also under article 9 GDPR), (iii) the information obligation under article 13 and 14 of the GDPR, (iv) facilitate data subjects' control over their data via the implementation of specific mechanisms and tools for the exercise of their rights, (v) the right not to be subject to a decision based solely on automated processing, including profiling, under article 22 GDPR (vi) the implementation of organisational and technical safeguards under article 32 GDPR, and (vii) the performance of a DPIA.
- **Fairness:** the use of Big Data and AI systems entails the risk of reinforcing and increasing inequality between individuals and groups in society. The use of AI systems could result in profiling and segmentation practices. As a result, (Mobility) Service Providers will therefore have the ability to differentiate between

individuals or groups of users. Meaning, there is a risk that individuals or groups of users will (i) receive unequal access to products or services, (ii) have discriminatory forms and quality of service, such as (de)reprioritisation or even denial of access to products and services in periods of high demand and (iii) be subject to discriminatory differential pricing strategies. Moreover, the black-box characteristics of certain AI systems, might make discriminatory practices difficult to identify and prove.[87] In addition, as mentioned by the European Commission in its Gender Equality Strategy, AI may intensify gender inequalities by repeating, amplifying or contributing to gender biases that programmers may not be aware of or that are the result of specific data selection.[88] This is why it is necessary that teams that design, develop, test and maintain, deploy and procure AI systems reflect the diversity of users and of society in general.

- **Explainability:** as already stated above, AI systems may operate as black-boxes, making it difficult for users to understand how (Mobility) Services providers using AI systems, have arrived at a particular output, or what input factors or a combination of input factors have contributed to the decision making process.
- **Safety and security:** risks of cybersecurity incidents, manipulating AI, incorrect advice on the most appropriate insurance to subscribe to, etc.

(b) *Ethics Guidelines*

On 8 April 2019, the High-Level Expert Group on Artificial Intelligence (AI) presented Ethics Guidelines for Trustworthy AI.[89] For this group, trustworthiness of AI means maximising the benefits of AI systems while preventing and minimising their risks. To reach this objective, three components need in their opinion to be met together during the entire life cycle of the system: (i) lawfulness, (ii) robustness and (iii) ethics.[90] Ethics must be considered a necessity, as laws are not always up to speed with technological developments and they can be inconsistent with ethical norms or simply inappropriate to address certain issues.[91] By way of illustration, the scope of some legal documents is geographically limited, such as the EU Charter that is limited to EU law areas or the European Convention on Human Rights that only binds State Parties.[92]

[87] European Commission, Ethics of connected and automated vehicles, https://ec.europa.eu/info/sites/info/files/research_and_innovation/ethics_of_connected_and_automated_vehicles_report.pdf, p. 43 (last consulted 29 March 2021).
[88] European Commission, A Union of Equality: Gender Equality Strategy 2020-2025, COM(2020) 152 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0152&from=EN, p. 6 (last consulted 29 March 2021).
[89] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai, p. 5 (last consulted 29 March 2021).
[90] *Ibidem.*
[91] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, p. 6-7.
[92] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, p. 10.

It should be noted that, though ethics are relevant as regards AI to complement the law, ethics may still rely on the law – especially fundamental rights – when identifying ethical criteria, which can be operationalised in the context of AI.[93] In this way, by relying on fundamental rights such as human dignity[94], freedom of the individual, respect for democracy, non-discrimination and equality[95],[96] four ethical principles were identified by the High-Level Expert Group on AI.

- **Respect for human autonomy**: means that humans interacting with AI systems must be able to maintain full and effective self-determination over themselves and be able to participate in the democratic process. In this way, this principle aims to ensure human oversight of the work processes in AI systems, so that these systems result in enhancing, complementing and strengthening human cognitive, social and cultural skills.[97]
- **Prevention of harm**: means that AI systems should neither cause nor aggravate harm or adversely affect human beings, either individually or collectively, including harm to the social, cultural and political environment as well as to the natural environment and living beings. If open to malicious use, AI systems can cause or increase adverse impacts due to asymmetries of power or information, such as MDM (Mobility) Service Providers and End-Users. In addition, one should also take into account the prevention of harm relating to gender since, as mentioned by the European Commission in its Gender Equality Strategy, AI may intensify gender inequalities by repeating, amplifying or contributing to gender biases that programmers may not be aware of or that are the result of specific data selection.[98] That is why, it is necessary that teams that design, develop, test and maintain, deploy and procure AI systems reflect the diversity of users and of society in general (see below).[99]
- **Fairness**: even though there are many different interpretations of fairness, the concept of fairness can be illustrated using two dimensions, one substantive and one procedural. From a **substantive perspective**, AI must ensure equal and just distribution of both benefits and costs, but also that individuals and groups are free from unfair bias, discrimination and stigmatisation. This includes equal opportunity in terms of access to goods and services. Nonetheless, fairness also has a **procedural dimension**, which entails the ability to challenge and seek effective redress against decisions made by AI systems and by the humans operating them. To achieve this second procedural dimension of fairness, it is important that the entity responsible

[93] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019, p. 9.
[94] Article 1 of the EU Charter.
[95] Title III of the EU Charter;
[96] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, p. 10 and 11.
[97] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, p. 12.
[98] European Commission, *A Union of Equality: Gender Equality Strategy 2020-2025*, COM(2020) 152 final, p. 6.
[99] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, p. 23.

for the decision is can be easily identified and the decision-making processes are explainable.[100] However, as discussed by the Commission in its *White Paper on Artificial Intelligence*, this procedural dimension may appear to be complex, as enforcement authorities and affected persons may not have the means to assess how a given decision involving AI was reached and, therefore, whether the applicable rules were respected.[101]

- **Explicability**: to maintain users' trust in them, AI systems processes need to be transparent, which mean that the capabilities and purpose of AI systems should be openly communicated, and decisions must be explained to those directly and indirectly affected. Otherwise, a decision involving AI systems could not be properly challenged.[102] However, the extent to which decisions must be explained is based on a case-by-case assessment, depending on the context and the severity of the consequences. For example, there will be few ethical objections to inaccurate recommendations on which mobility services to use. On the other hand, AI systems that evaluate whether or not an individual with a certain behavioural pattern is entitled to insurance, may have to pay more to use a certain mobility service, or may even be denied access to certain mobility services, will have serious consequences and thus require a higher degree of transparency. A principle of transparency should be ensured, which can be implemented with either complete technical transparency or explanation in clear and familiar language by communicating, for example, the nature of the services offered, the tools developed, their performance and the risks of error.[103]

However, as these ethical principles are fairly abstract, the Guidelines describe seven essential requirements that AI systems must meet to be trustworthy: (i) human agency and oversight, (ii) technical robustness and security, (iii) privacy and data governance, (iv) transparency, (v) diversity, non-discrimination and fairness, (vi) environmental and social well-being, and (vii) accountability. These requirements apply to all stakeholders involved in the lifecycle of AI systems.

5.1.2. *Application in the context of an MDM*

In the context of the MDM, the requirements set forth above imply that not only the MDM operator, the MDM and the (Mobility) Service Providers are responsible for ensuring that the obligations are met, but also the developers, installers and end-users, as well as society at large. To operationalise these requirements, the Ethics Guidelines provide a non-exhaustive checklist that formulates concrete questions to verify compliance with the seven requirements.

[100] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, p. 12- 13.
[101] European Commission, *White Paper on Artificial Intelligence*, COM(2020) 65 final, p. 12 (last consulted 29 March 2021).
[102] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, p. 13.
[103] European Commission for the Efficiency of Justice, *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, 2018, https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, p. 11 (last consulted 29 March 2021).

The table below briefly addresses each of the seven requirements and gives practical examples (questions) based on the checklist for MDM actors to consider when using AI systems:

	Principle	Brief explanation	Practical examples
1.	*Human agency and oversight*	Human autonomy must not be restricted or abused and the AI systems as such must always be under the influence and supervision of humans. AI systems should support people in making better, more informed choices that are in line with their goals. Moreover, users of public AI systems should always receive the necessary knowledge and tools to understand and interact with AI systems and their limitations.	- Is there a risk that the AI system could affect human autonomy by influencing the MDM actor's decision-making process in an unintended way? - Did the relevant MDM actor take safeguards to prevent overconfidence in or overreliance on the AI system? - Who is the "human in control" and what are the moments or tools for human intervention?
2.	*Technical robustness and security*	The algorithms used must be safe, accurate, reproducible and reliable. Any errors in the AI systems must be detectable and repairable. Also, the system must be sufficiently accurate or indicate the likelihood of errors.	- Did the relevant MDM actor assess potential forms of attacks to which the AI system could be vulnerable? - Did the relevant MDM actor consider the level of risk raised by the AI system in this specific use case? - Did the relevant MDM actor assess whether there is a probable chance that the AI system may cause damage or harm to End-users or third parties? Did you assess the likelihood, potential damage, impacted audience and severity?
3.	*Privacy and data governance*	End-users must have control over the data they provide, as well as over the information generated in the course of their interaction with the AI system (and the MDM actors). In addition, the data must not be misused and the quality and integrity of the data must be ensured. Inaccuracies, errors and socially constructed biases must be removed from the data sets before training the system.	- Did the relevant MDM actor consider ways to develop the AI system or train the model without or with minimal use of potentially sensitive or personal data? - Did the relevant MDM actor take measures to enhance privacy, such as via encryption, anonymization and aggregation? - Did the relevant MDM actor align your system with relevant standards (for example ISO, IEEE) or widely adopted protocols for daily data management and governance? - Did the relevant MDM actor assess who can access users' data, and under what circumstances? - Did the relevant MDM actor ensure that these persons are qualified and required to access the data, and that they have the necessary competences to understand the details of data protection policy
4.	*Transparency*	The data sets and processes must be traceable, verifiable and explainable.[104]	- Traceability: does the relevant MDM actor have documentation of (i) the methods

[104] Traceability means that the data sets and processes from which decisions of AI systems originate must be documented as well as possible. Explainability relates to the ability to explain both the technical processes of a AI

	Principle	Brief explanation	Practical examples
			used to design and develop the AI system, (ii) the methods used to test and validate the AI system and (iii) the results of the AI system? - Explainability: To what extent can the decision taken by the AI system and thus the result be understood? To what extent do the decisions of the system influence the decision-making process? What is the reason for using this particular system in this particular area? - Communication: Have the reasons and criteria behind the results of the AI system been communicated to the End-users? Have the characteristics, limitations and potential shortcomings of the AI system been clearly communicated to the End user?
5.	*Diversity, non-discrimination and fairness*	AI-systems may not create or reinforce unfair biases.	- Did the relevant MDM actor consider diversity and representativeness of users in the data? Did the MDM actor test for specific populations or problematic use cases? - Did the relevant MDM actor put in place processes to test and monitor for potential biases during the development, deployment and use phase of the system? - Depending on the use case, is there a mechanism that allows others to flag issues related to bias, discrimination or poor performance of the AI system? - Did the relevant MDM actor assess whether there is any possible decision variability that can occur under the same conditions?
6.	*Environmental and social well-being*	AI systems must contribute to social and ecological well-being.	- Did the relevant MDM actor assess the broader societal impact of the AI system's use beyond the individual (End-)user, such as potentially indirectly affected stakeholders?
7.	*Accountability*	First of all, it must be clear who is responsible for the AI system and the results, and it must always be possible to control the algorithms, data and design processes. In addition, negative consequences must be minimised and there must always be an appropriate weighing up of the various interests[105]. This must also always be adequately	- Did the relevant MDM actor carry out a risk or impact assessment of the AI system, which takes into account different stakeholders that are (in)directly affected? - Did the relevant MDM actor establish processes for third parties (e.g. suppliers, consumers, distributors/vendors) or

system and the related human decisions. It must be possible to obtain an explanation of the system's decision-making process. People must also always have the right to be informed that they are dealing with a AI-system. In addition, users must also be made aware of the limitations and capabilities of AI systems in order to create appropriate expectations of the system.

[105] E.g. when using AI systems for the purpose of predicting crime, the individual freedom and privacy of the person concerned is affected. The balancing act in such cases should be approached in a rational and methodological way, by recording, evaluating and documenting the relevant interests and values at stake. The person making the final decision must be accountable for the way in which the assessment is made.

Principle	Brief explanation	Practical examples
	documented so that the use of AI systems is always verifiable.	workers to report potential vulnerabilities, risks or biases in the AI system? - Did the relevant MDM actor establish a mechanism to identify relevant interests and values implicated by the AI system and potential trade-offs between them? - Did the relevant MDM actor put mechanisms in place both to provide information to End-users/third parties about opportunities for redress?

(a) *Guidance on explaining decisions made with AI – ICO and the Alan Turing Institute*

As mentioned above, the relevant MDM actor should take appropriate measure to inform End-Users of the intended use of the AI system. For this purpose, the MDM participant can use various means: the platform, privacy policy, etc. The risk associated in not explaining AI decisions include regulatory actions, reputational damage and disengaged End-Users.

Therefore, in addition to the ethical guidelines, we consider it useful to refer to guidelines published by the UK Information Commissioner's Office ("ICO") and The Alan Turing Institute.[106] The guidance is split into three parts, explaining the basics of AI before going on to give examples of explaining AI in practice, and looking at what explainable AI means for an organisation.

When it comes to actually explaining AI decisions, the guidance identifies the following six main types of explanation:

(i). **Rationale explanation**: an explanation of the reasons that led to an AI decision, which must be given in an accessible and non-technical way.

(ii). **Responsibility explanation**: an explanation of who is involved in the development, management and implementation of the AI system, and who to contact for a human review of an AI-decision.

(iii). **Data explanation**: an explanation of the data used in a particular decision and how such data was used.

(iv). **Fairness explanation**: an explanation of the design and implementation steps taken across an AI system to ensure that the decisions it supports are generally unbiased and fair (including in relation to data used in the AI system), and whether or not an individual has been treated fairly.

[106] ICO and Alan Turing Institute, *Explaining decisions made with AI*, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence/ (last consulted 26 March 2021).

(v). **Safety and performance explanation**: an explanation of the design and implementation steps taken across an AI system to maximise the accuracy, reliability, security and robustness of its decisions and behaviours.

(vi). **Impact explanation**: an explanation of the design and implementation steps taken in AI system to consider and monitor the impacts that the use of an AI system and the decisions it supports have, or may have, on individuals and on wider society.

There is however no "one-size-fits-all" explanation. The relevant MDM actor should consider different explanations in different situations and use a layered approach that allows for more detail to be provided if required.

(b) *The use of location data and ethical issues*

Location data is likely to form a significant part of the data collected and shared through the MDM platform. For this reason, it is important to draw attention to a recent initiative by EthicalGEO, the Locus Charter[107], which sets out a number of principles for the ethical use of location data.

The Locus Charter is a set of general principles published in February 2021 by an international collaboration of governments, organisations and individual practitioners with the objective of supporting ethical practices with respect to location data. Though it consists in non-binding guidelines, such a charter remains of particular relevance for all MDM participants intending to use, create, collect, analyse and store location data.

MDM participants should pay attention to the use of location data, given the numerous risks that the use of location data may entail, including bias in datasets, invasion of privacy and misuse of power imbalances in markets. Besides, although it is not entirely the same, being tracked around the internet has parallels with being followed around wherever you go. On top of this, the risks posed by location data are expected to grow in the coming years due to the development of geospatial technologies alongside AI and the Internet of Things. Dealing with such risks is all the more difficult because so far there has been no common set of guidelines for the responsible use of location data.

Following this line, the Locus Charter was drafted in order to simulate discussion about ethics in information technologies, as well as to promote responsible use of location data. The guidelines may be useful for MDM actors using location data to better understand the potential harm of their activity, and may also provide guidance on how to better manage potential risks and communicate how they make sensitive decisions with respect to this kind of data. The charter consists of 10 principles, some of which are similar to those for Trustworthy AI[108]:

[107] EthicalGeo, *Locus Charter*, https://ethicalgeo.org/wp-content/uploads/2021/03/Locus_Charter_March21.pdf (last consulted 29 March 2021).
[108] EthicalGeo, Locus Charter, https://ethicalgeo.org/wp-content/uploads/2021/03/Locus_Charter_March21.pdf (last consulted 29 March

- **Realise opportunities**: understanding that location data offers many social and economic benefits, and these opportunities should be realised responsibly.
- **Understand impacts**: realising the effects of uses of location data, including knowing who and what could be affected, and how.
- **Do no harm**: ensuring that the individual or collective location data pertaining to all people, flora and fauna is not used to discriminate, exploit or harm.
- **Protect the vulnerable**: taking additional care with respect to vulnerable people and then act proportionately, and positively to avoid causing harm.
- **Address bias**: understanding bias in the datasets and avoid discriminatory outcomes, which may otherwise remove some groups from mapping or amplify negative impacts of inclusion in a dataset.
- **Minimize intrusion**: avoiding unnecessary and intrusive examination of people's lives and the places they live in, pursuant to the principle of human dignity.
- **Minimise data**: complying with practices using only the necessary personal data that is adequate, relevant and limited to the objective under the data minimisation principle.
- **Protect privacy**: when using location data that identifies individuals, this should be respected, protected, and used with informed consent where possible and proportionate.
- **Prevent identification of individuals**: putting in place measures to prevent subsequent use of the data resulting in identification of individuals or their location.
- **Provide accountability**: giving to people the ability to interrogate how location data is collected and used in relation to them and their interests, and appeal uses.

5.1.3. *Conclusion*

Based on the above, we suggest the following actions to be taken in the context of the MDM. Please note that these are just suggested first steps and will depend on the specific use cases.

(i) Draft (a) appropriate and clear guidelines for the use of the AI system or location data and (b) ethical and legal guidelines that protect individuals' right at group level in the context of the MDM;

2021).

(ii) Impose commitments for MDM (Mobility) Service Providers when using the MDM around algorithmic inference, addressing ethical data sharing, transparency and business practices and protecting of data and privacy;
(iii) Develop meaningful, standardised transparency strategies to inform End-users about the data collected within the MDM;
(iv) Design and operate the MDM in such a way to neither discriminate against individuals or groups of users nor create or reinforce large-scale social inequalities;
(v) Implement measures to increase End-Users' awareness of potential risks of bias;
(vi) Develop and apply user-centred methods and interfaces for the explainability of AI;
(vii) Promote dialogue between MDM actors to identify, establish and accept their respective ethical obligations in relation to the MDM.

6. Legal and Ethical Challenges in specific use cases

6.1.1. *Mobility Data for Insurance Purposes*

(a) *Mobility Data as a basis for tailored insurance premiums*

The use of Mobile Data Marketplaces implies the collection of vast sets of data relating to devices and, depending on the specific use case, users. As such data may allow for analysing behavioral patterns of users, it may be interesting for insurance companies to obtain such data. These data may enable insurance companies to make for instance statistical analyses of behavioral patterns of specific users and allow them to better quantify the risk profile of such specific users.

On the basis of such analyses, insurance companies could subsequently offer more tailored insurance services such as a vehicle or travel insurance policy tailored to certain characteristics of a specific user or type of user.

(b) *Legal and ethical considerations – risk of discrimination*

Even though a tailored insurance policy may bring benefits with it, it nevertheless raises some legal and ethical concerns. On the basis of such data, an insurance company could determine that certain users, for instance based on age, gender or social background, could be prone to causing more accidents and therefore require the payment of different insurance premiums from such users.

Although such approach would have merit from an insurance provider's perspective, it may nevertheless raises some legal concerns.

(i) *Discrimination*

First and foremost, the use of data and algorithms to determine the pricing of insurance premiums for specific types of users, may result in an undesired discrimination. In this scenario, it could be foreseeable that categories of users (based on gender, age or social background) may be charged more as compared to other categories of users.

Although (insurance) companies are in principle prohibited from basing pricing decisions on certain protected traits such as gender, social origin etc.,[109] it does not preclude that certain other data points would be used to arrive to the same conclusions.[110]

[109] Discrimination on the basis of certain "protected characteristics" is in principle prohibited. In Belgium for instance, such discrimination is prohibited by among others (i) the Act of 10 May 2007 regarding the combatting of discrimination, *Official Gazette* 30 May 2007 (the "**Anti-discrimination Act**"), (ii) the Act of 30 July 1981 on the criminalisation of certain actions based on racism or xenophobia, *Official Gazette* 8 August 1981 (the "**Anti-racism Act**") and (iii) the Act of 10 May 2007 on combatting discrimination between men and women, *Official Gazette* 30 May 2007 (the "**Gender Act**").

[110] BEUC, *The use of Big Data and Artificial Intelligence in insurance*, Beuc-x-2020-039, p. 12, https://www.beuc.eu/publications/beuc-x-2020-039_beuc_position_paper_big_data_and_ai_in_insurances.pdf (last consulted 22 March 2021).

(ii) Data Protection

Aside from the possible discriminatory effect from using certain data types, the use of such data for tailored insurance policies also raises concerns from a data protection perspective.

Further to Article 22 of the GDPR, there is a general restriction on the use of personal data in the context of automated decision making (see Section 4.1.5(a) above).

(c) Tackling the legal and ethical issues for this use case

(i) Discrimination

Discrimination is prohibited by various legal instruments, including Article 21 of the Charter of fundamental rights of the European Union[111]. Consequently, as to avoid that the data exchanged by the MDM would be used for products and or services that could be discriminatory, the MDM Operator could restrict certain uses of the MDM data.

In this regard, the MDM Operator could include in the terms and conditions of the MDM that any use of data for any illegal purposes, including any discriminatory purposes, would be strictly prohibited. The MDM Operator could further limit the use of the MDM and the MDM data for illegal purposes by clearly stating that, a violation of this requirement, would allow the MDM Operator concerned to suspend the infringing Service Provider's access to the MDM, without prejudice to the MDM Operator's other legal rights, such as the right to claim damages.

(ii) Automated decision making

In order to ascertain that any automated decision making based on data exchanged through the MDM is in line with the GDPR, it is recommended that the MDM Operator at least ensures that such automated decision making complies with requirements set forth in Article 22 of the GDPR. In that respect, the MDM operator should, in its terms and conditions provide that, if a Service Provider aims to use personal data for automated decision making, is it only to be applied (i) in accordance with applicable laws, (ii) on data other than *special categories of data* as defined in the GDPR and (ii) provided that any data subject whose personal data are processed by the MDM, has given his prior explicit consent thereto.

Moreover, the MDM Operator should also include in its terms and conditions that the Service Provider who aims to process (personal) data for automated decision making, (i) complies with all data subject's rights as set forth in the

[111] Charter of fundamental rights of the European Union, 2012/C 326/02, OJ C 326, 26.10.2012, p. 391–407, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT (last consulted 22 March 2021), hereafter the "**Charter**"; Article 21 Charter: "*Non-discrimination 1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. 2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.*"

GDPR and further clarified in Section 4.1.5(a) above and (ii) foresees a human intervention in the decision making process.

7. Conclusion

The issue on urban mobility has led to the emergence of alternative modes of transport such as micromobility solutions. Since many mobility and micromobility solutions have become smart through the implementation of IoT devices, a vast set of raw usage and vehicle data is being generated. Although such raw data by itself has only limited value, the combination of the data sets of different (micro)mobility solutions and the subsequent analysis thereof creates new opportunities. In this context, an MDM, which (i) aims at consolidating all these data and (ii) might allow for alternative (business) opportunities for End-Users, Service Providers and public authorities, plays a crucial role.

Even though MDMs can create opportunities and generate additional value, they also pose certain legal challenges. As an MDMs core operation relies on the acquisition, use and dissemination of data from vehicles, sensors and potentially End-Users, it raises questions as regards its compliance with data protection laws such as the GDPR and intellectual property rights in data.

As set forth in Section 4.1.8 above, an MDM can operate within the boundaries of the GDPR provided however that the key principles and obligations under the GDPR are properly implemented by the participants of the MDM. This would imply among others that MDM Operators and Service Providers properly map (i) the types of personal data they aim to use, (ii) the purposes for which they use such data and (iii) properly assess their roles as either a (joint) controller or processor. Once data usage and potential personal data streams are properly mapped, such participants will, depending on their respective roles under the GDPR, need to implement the proper business processes as to comply with GDPR requirements as regards among others the deployment of data registers, data protection policies, the exercise of data subject's rights, potential designation of DPOs and performance of DPIAs. In addition thereto and to mitigate the MDM Operators risk exposure and facilitate GDPR compliance, the MDM Operator and Service Providers should also adopt proper terms and conditions and data processing agreements as further clarified in Section 4.1 above.

With regard to the intellectual property rights in data, it is clear that the protection of *raw* data is not evident. As raw data is typically not "original", it would not enjoy the benefit of copyright protection. However, as specified in Section 4.2.1(b) above, sets of raw data might be protectable by the database right or the *sui generis* right provided that either:

(a) the structuring of the database is original, in which case such database might be protectable under the database right; or

(b) the MDM Operator or Service Provider has/have made a substantial investment in obtaining and verifying the data, in which case the database might be eligible for the protection under the *sui generis* right.

In terms of *derivative data*, being the data that is based on the raw data further to an analysis, such data might benefit from copyright protection provided that it would meet the "originality" criterion and be materialised. Even if such data would not be original, such data sets might still enjoy the benefit of the *sui generis* protection provided that a substantial investment in obtaining and verifying the data has been made.

As an MDM relies on the sharing and use of data, the ownership and *de facto* monopoly position of the participant who has the rights in these data, might be problematic (see Section 4.2.3(a) above). As to overcome these issues, it is recommended that the MDM Operator imposes appropriate licensing models upon the participants to the MDM as to enable such participants to exchange and use such data in the context of the MDM (see Section 4.2.3(c) above).

An MDM ecosystem is characterised by different (contractual) relationships between different parties. The MDM ecosystem could rely on smart contracting and DLT or blockchain technology to govern the relationships and interactions between the different participants. The use of DLT for transactional purposes would in principle be permissible. However, as contracting law and more in particular the rules on the enforceability of (smart) contracts are not fully harmonised, the MDM Operator should assess the legal validity of such smart contracts in accordance with the local laws of the geographical market in which it operates (see Section 4.3 above).

The advent of information technology in general and the emergence of *IoT* and *Big Data*, have increased the social and economic importance of data marketplaces. As the current regulation on online services has proven to be insufficient to tackle newly emerging issues regarding among others the dissemination of illegal content, a new regulatory regime was proposed in the form of the Digital Services Act. Although the Digital Services Act has not been adopted, it is likely that it will apply to MDMs and that it will impose more business process requirements upon data marketplaces such as MDMs (see Section 4.4 above). This is an upcoming legal and operational challenge that needs to be addressed by the MDM Operator once the Digital Services Act chrysalises into its final form.

As an MDM may generate substantial benefits for urban mobility in general and for End-Users and Service Providers in particular, it also raises important ethical questions. An MDM relies on mobility data exchanged by End-Users and Service Providers. Since such mobility data might enable to discern behavioral patterns of users or enable to determine certain characteristics of users, it might also allow for automated decision makings on the basis of such data. In this context, certain ethical issues may arise as the use of these data and the conclusions that are based thereon, might result in an inadvertent discrimination on the basis of gender, social background or physical characteristics (see Section 5 above). As such issues would be diametrically opposed to core values of an MDM as envisaged by Moliere, they need to be addressed upfront and with proper scrutiny. In light thereof, MDM Operators should implement appropriate ethical policies or guidelines and control mechanisms to monitor and tackle these challenges. Moreover, to avoid that the MDM data would be used for unethical practices by Service Providers, the terms and conditions to be entered into between the MDM and the Service Providers should clearly state that such data may not be used for any illegal purposes, including but not limited to any use in violation with the MDMs ethical guidelines (see Section 5 above).