Mobility as a Service in a multimodal European cross-border Corridor **(MyCorridor)**

Deliverable 7.4

Analysis of legal and regulatory barriers in MaaS

Osborne Clarke LLP

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 723384

MyCorridor report:	D7.4: Analysis of legal and regulatory barriers in MaaS
Dissemination level:	PU
Work package:	WP7: Business models, incentives and legal issues
Lead beneficiary:	Osborne Clarke LLP
Date due to EC:	30/11/2020, M42
Date of Delivery to EC:	21 December 2020
Status (F: final; D: draft; RD: revised draft):	Final
File Name:	MyCorridor_D7.4_LegalRegulatoryinMaaS_Final
Version:	Final

Document history

Version No.	Date	Details
0.1	20.04.2020	1st draft version, provided by OC with the skeleton of the Deliverable.
0.2	28.09.2020	2nd draft version, encompassing the key contents of the version for internal revision.
1.0	20.11.2020	Final draft version sent for Peer Review
Final	17.12.2020	Final version towards submission to the EC.

Reviewers list

Name	Company
Dr. Maria Gkemou	CERTH/HIT

This project is co-funded by the European Union under the Horizon 2020 Research and Innovation Programme. The content of this document reflects solely the views of its authors. The European Commission is not liable for any use that may be made of the information contained therein.

This deliverable is a draft document subject to revision until formal approval by the European Commission.

The MyCorridor project Consortium consists of:

No.	Name	Short name	Country
1.	NEWCASTLE UNIVERSITY	UNEW	UK
2.	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	EL
3.	OSBORNE CLARKE LLP	OC LLP	UK
4.	WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES EPE	Wings ICT	EL
5.	SWARCO MIZAR SRL	SWARCO MIZAR	IT
6.	SWARCO HELLAS SYSTIMATA KYKLOFORIAS ANONYMI ETAIREIA	SWARCO Hellas	EL
7.	CHAPS SPOL SRO	CHAPS	CZ
8.	HACON INGENIEURGESELLSCHAFT MBH	HACON	DE
9.	MAP TRAFFIC MANAGEMENT BV	MAPtm	NL
10.	VIVA WALLET HOLDINGS - SOFTWARE DEVELOPMENT SA	VivaWallet	EL
11.	AMCO OLOKLIROMENA SYSTIMATA YPSILIS TECHNOLOGIAS ANONYMI VIOMICHANIKI KAI EMPORIKI ETAIRIA	AMCO	EL
12.	TOMTOM DEVELOPMENT GERMANY GMBH	TOMTOM	DE
13.	ROMA SERVIZI PER LA MOBILITA SRL	RSM	IT
14.	TTS Italia	TTS	IT
15.	PANEPISTIMIO PATRON	UPAT	EL
16.	IRU PROJECTS ASBL	IRU	BE
17.	SALZBURG RESEARCH FORSCHUNGSGESELLSCHAFT M.B.H.	SFRG	AT

Table of Contents

Executive Summary

This Deliverable, "Analysis of the legal and regulatory barriers in MaaS", has been prepared in the context of Work Package 7: "Business models, Incentives and Legal Issues" of the MyCorridor project. The Deliverable has two objectives:

- To set out the MyCorridor Consortium's analysis of legal and regulatory issues encountered during the MyCorridor project. Where appropriate, we have also considered the implications of those issues for MaaS in general as well as any practical steps taken during the MyCorridor project to address those issues.

- To present examples of the key legal agreements, policies and other documents that Osborne Clarke ("**OC**") developed for the MyCorridor project, as a MyCorridor Consortium partner. These are described in paragraph 1.2, below, and are attached in full in the Annexes to this Deliverable. By way of example, we have included the 'MyCorridor service provider platform terms and conditions' in Annex IIA. These terms and conditions were prepared for the purpose of the trials of the MyCorridor MaaS platform (the "**Pilots**") and provided a contractual basis for integrating service providers into the platform in order to run the Pilots. Although prepared in the context of a research project, the documents set out in the Annexes to this Deliverable do give an indication of the agreements, policies and other documents that would underpin the commercial deployment of a MaaS platform (subject to requisite adaptation in that setting).

The Deliverable is structured as follows:

Sections 2 to 6, summarised below, explore the key legal and regulatory issues that we encountered during the MyCorridor project, and the challenges and opportunities they create for MaaS. Where appropriate, we also consider potential legal reforms.

- Section 2: Data Protection. With data protection being a key focus for the MyCorridor project, this section reviews the application of data protection laws in MaaS, and considers the challenges and opportunities this can bring. A move towards opening up access to data to support adoption of MaaS is also explored.

- Section 3: Competition Law. As well as reviewing the general application of competition law to MaaS, we explore the way in which competition law can be used to encourage market access to MaaS platforms, including for new entrant providers of transport or other services.

- Section 4: Payments Law. This section considers the payments regulatory framework and its applicability to MyCorridor and the commercial deployment of MaaS, while exploring some challenges faced by the MyCorridor project in this area.

- Section 5: Consumer Law. Consumer law is an important dimension for a MaaS platform because compliance generates consumer trust and encourages participation by consumers in MaaS. This section explores the latest developments in consumer law at an EU level, with particular focus on the EU's New Deal for Consumers, which introduces strengthened enforcement and others rights to promote compliance with consumer law.

- Section 6: Platform to Business Regulation. In this section we explore the new Platform to Business Regulation and the impact this may have on MaaS platforms.

In the Annexes to this Deliverable, as mentioned above, we reproduce some of the key legal agreements, policies and other documents that OC developed during the MyCorridor project.

OC also supported its fellow MyCorridor Consortium partners with advice on legal, regulatory and contractual matters that arose throughout the project. A notable area of support, connected to the overarching focus on data protection, came in drafting and assisting MyCorridor Consortium partners in devising the 'Data Protection Impact Assessment' ("DPIA"), one of the key privacy documents for any MaaS project or platform. The DPIA is reproduced in Deliverable 2.16.3 "Data Management Plan Impact Assessment", and helped frame the MyCorridor Consortium's consideration of Data Management issues in Work Package 2. The importance of DPIAs and the need to ensure "privacy by design" in MaaS is also discussed further in the Data Protection Section of this Deliverable (at Section 2).

Key contractual and other legal documentation

As part of the process of identifying legal issues in MaaS, OC, as a MyCorridor Consortium partner, drafted or otherwise advised the other MyCorridor Consortium partners on the following key legal documentation required for the MyCorridor MaaS platform and the Pilots:

- **MyCorridor's privacy policy** – OC prepared a privacy policy based on the personal data processing activities which the MyCorridor Consortium carried out during the MyCorridor MaaS project, both for the website and the mobile application. OC also advised the MyCorridor technical partners and Pilot leaders in relation to the integration of the privacy policy within the mobile app itself, and how the privacy policy should be presented to individuals participating in Pilots, prior to individuals sharing any personal data with the MyCorridor Consortium .

- **MyCorridor's use of cookies** - OC provided advice in relation to the use of cookies and similar technologies on the website and in the mobile app, and provided template cookie policies for the MyCorridor Consortium's completion and consideration.

- **Template external service provider agreement** – OC prepared a template service provider agreement to be entered into between the relevant MyCorridor Consortium partners and external service providers, which OC also helped negotiate with Karhoo.

- **MyCorridor Platform terms and conditions for external service providers** – OC prepared terms and conditions for external transport service providers, summarising the key provisions from the template external service provider agreement. These form part of the MyCorridor application.

- **MyCorridor platform terms and conditions for Pilot participants** – OC prepared consumer terms and conditions for participants of the MyCorridor platform trials (the "**Pilots**"), that are also part of the MyCorridor application.

- **MyCorridor platform terms of use** – OC prepared some terms of use to govern individuals' and service providers' use of the website and app.

- **Data processing and sharing agreements** - OC also advised on the importance of having these in place both between MyCorridor Consortium partners and with external service providers. These were ultimately managed by the relevant MyCorridor partner entities themselves.

While there were multiple stakeholders in the MyCorridor Consortium, which is indicative of a commercial MaaS ecosystem, given the majority of stakeholders were partners of the MyCorridor Consortium research project, with only a few external service providers contributing to the project, the MyCorridor Consortium partners took the view that some legal and contractual issues would be dealt with in-house. For example, certain data protection matters, such as contractual measures relating to sharing personal data within the MyCorridor Consortium were understood to have been covered separately between those organisations and were not explored in-depth. Of course, in a commercial MaaS environment, detailed data processing agreements and data sharing agreements may be heavily negotiated, sometimes between multiple stakeholders.

Contractual terms were also drafted and negotiated taking a risk-based approach, trying to keep terms plain and intelligible and fair. In particular, when negotiating contracts with external service providers to the project, it was acknowledged that established external service providers had to protect their businesses, whereas any loss that may be suffered by the MyCorridor research project would likely be comparatively low or possibly nil, and therefore certain matters such as those relating to liability and indemnities were conceded, when they would most likely be more heavily negotiated in a commercial MaaS context. Further, the risk of any loss to the MyCorridor Consortium in practice was particularly low given the short length of the MyCorridor app trials and the limited number of participants, compared with the considerably higher number of users there would be in a commercial MaaS ecosystem.

The terms and conditions for the MyCorridor platform trial participants were also drafted acknowledging that there were only a limited number of users taking part, for research purposes. Therefore, these were drafted from an English law perspective, while the MyCorridor Consortium partners acknowledged that in a commercial cross-border MaaS model, these consumer-facing terms would need reviewing and updating at a local law level in the relevant jurisdictions where the services are being provided.

Summary of key legal considerations explored during the MyCorridor project

In addition to the legal issues explored in further detail in Sections 2-6 of this Deliverable, the table below sets out a high-level summary of other legal issues considered during the MyCorridor project as applicable to MaaS.

Legal issue	Comment
Data protection	Data protection must be a top priority for any MaaS ecosystem, which is heavily dependent on quality data, including personal data, as explored further in Section 2 of this Deliverable.
Cybersecurity	Cybersecurity must also be a top priority for a MaaS ecosystem, given the vast amount of data that a MaaS ecosystem processes, as noted in Section 2 of this Deliverable.
Intellectual Property Rights / licensing agreements	In a commercial MaaS context, greater control of intellectual property rights would be required. This would not only be to protect any rights in software and other technical solutions, but also where and to the extent intellectual property rights may be used to protect, control and monetise valuable data. However, the use of intellectual property rights, where possible, to protect data, could further restrict access to data and stifle the development of MaaS.

Legal issue	Comment
Consumer law	Platforms and stakeholders working within MaaS must consider the consumer laws applicable to each jurisdiction in which they provide services to consumers. This requires considerable time and may prevent a uniform approach across borders. Consumer law is discussed further in Section 5 of this Deliverable.
Contractual framework	Owing to the numerous stakeholders involved in a MaaS ecosystem, there can be a complex network of contracts to consider and negotiate.
Legal and contractual liability between MaaS stakeholders	Contractual liability in MaaS may be an area worthy of further research and possibly EU-level legislative intervention, to ensure that liability can be apportioned fairly and appropriately within MaaS, particularly where a MaaS platform already enjoys significant market power.
Payments law	Payment services providers will play a key role in any MaaS platform, bringing challenges and considerations from a payments law perspective, as explored in Section 4 of this Deliverable.
Platform regulation	The applicability of the Platform to Business Regulation is discussed in more details in Section 6 of this Deliverable.
Competition law	Competition law is a key framework relevant to MaaS, which could be a concern to those organisations who already hold significant market power in the mobility sector. However, competition law can also help to grow the deployment of MaaS, by preventing market leaders from blocking off access to MaaS to new entrants. Competition law in MaaS is discussed in more detail Section 3 of this Deliverable.
Data standardisation and interoperability	A lack of data standardisation and technical interoperability requirements, both at national levels and at an EU-level, can complicate, and even restrict, access to data in MaaS and the integration of various MaaS solutions. While legislative movements are being made at an EU-level, particularly as a result of the ITS Directive, at the time of writing, there is still a long way to go to facilitate MaaS. Notably, a lack of data standardisation and technical interoperability brought challenges to the MyCorridor Consortium when seeking to integrate third party solutions and access data provided by external service providers.
Local regulations and industry agreements / legal interoperability	Local regulations and industry agreements, regulating fares and ticketing, can complicate or even create barriers to the integration of ticketing functions into a MaaS platform. An example of this during the MyCorridor project came in the context of rail ticketing. Following discussions with the provider of an existing EU-wide ticketing platform, with the goal of integrating that platform's services into the MyCorridor platform for the purposes of the Pilots, the provider decided it would be unable to participate in the Pilots because in some

Legal issue	Comment
	countries the local regulation and industry agreements that regulate the creation of rail fares and the issuance of rail tickets made it too difficult to integrate their services in time to join the Pilots.

1 Introduction

1.1 Purpose of the document

The purpose of this Deliverable D7.4, "Analysis of the legal and regulatory barriers in MaaS", is to explore the legal and regulatory issues encountered by the MyCorridor Consortium during the MyCorridor project, and the implications of those issues for the deployment of commercial MaaS. This Deliverable has been prepared in the context of WP7 "Business models, incentives and legal issues", with the focus on legal issues in MaaS.

Where relevant, this Deliverable also sets out practical steps taken during the MyCorridor project to address the legal and regulatory challenges encountered. The final section of this Deliverable provides examples of the legal documents and contracts prepared by Osborne Clarke, as a MyCorridor Consortium partner, for (and used by) the MyCorridor Consortium, to provide an indication of the framework of documents and contracts required within a MaaS ecosystem.

We hope this Deliverable will help to raise awareness of the legal, regulatory and commercial challenges and opportunities in the deployment of cross-border MaaS.

1.2 Intended audience

This Deliverable will be made publicly available and is targeted at anyone with an interest in MaaS, including lawyers and all MaaS stakeholders (for example, software engineers, platform providers, payment providers, passenger transport providers and other MaaS service providers, as well as researchers and existing or prospective end-users of MaaS platforms). This Deliverable will also be of interest to public bodies, policy makers and legislators.

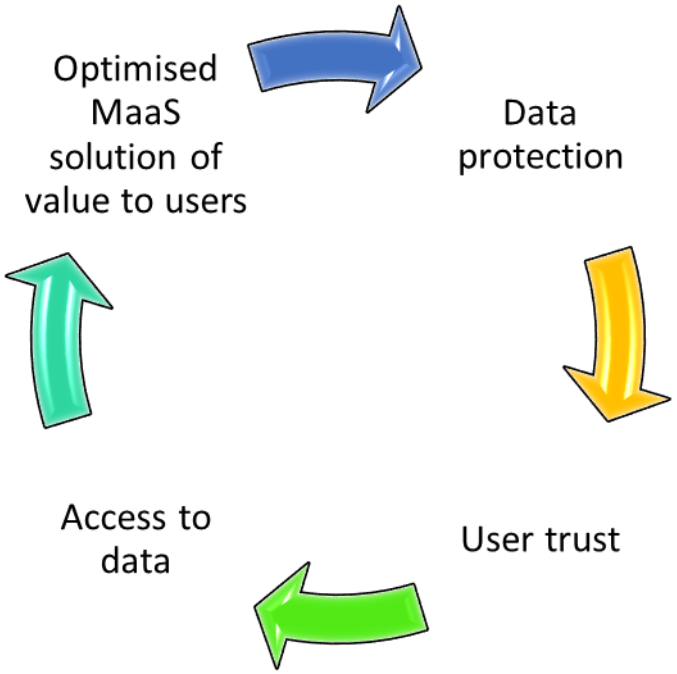
1.3 Interrelations

This Deliverable covers the legal challenges and opportunities identified within the MyCorridor project as a whole. As a result, it has interrelations with all other Work Packages, because the legal issues were cross-cutting.

2 Data Protection

2.1 Introduction: overview of applicable data protection law in the EU

MaaS ecosystems can offer users accurate, tailored, personalised and seamless travel solutions. To enable this, access to vast amounts of quality data is imperative. Data, or "big data" are central to a successful MaaS ecosystem, and user and stakeholder trust is intrinsically linked to access to this data, particularly given that this data often amounts to personal data.



2.2 The General Data Protection Regulation (EU) 2016/679

During the first year of the MyCorridor Project the EU General Data Protection Regulation (the "**GDPR**")[1], governing the protection and privacy of individuals based within the EU, came into force. The GDPR introduces greater accountability, transparency and compliance requirements than under its predecessor Directive[2], and goes some way to harmonise data protection laws across the EU. However, there are still some areas where Member States have the freedom to specify their own national rules and therefore data protection laws are still not completely harmonised across the EU, with some variations being greater across Member States than we might have originally envisaged. The differences in application across Member States add a layer of complexity to cross border MaaS, with some examples of this set out below. Breaches of the GDPR bring the risk of enforcement action, including fines of up to €20m or 4% of worldwide turnover (whichever is higher), and damage to reputation.

[1] The General Data Protection Regulation EU 2016/679
[2] Data Protection Directive - Directive 95/46/EC

2.3 Privacy and Electronic Communications Directive 2002 (ePrivacy Directive)

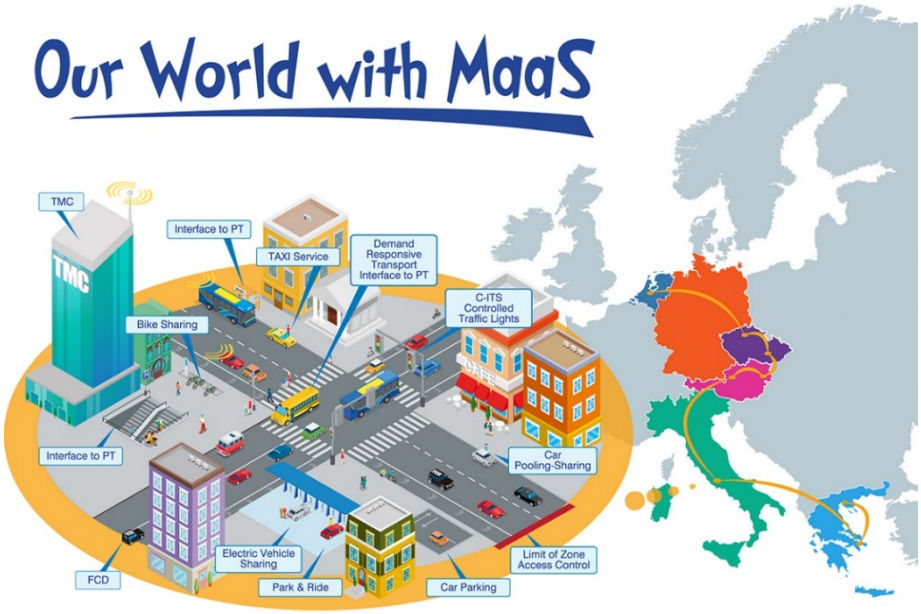
MaaS ecosystems also need to consider the application of the ePrivacy Directive[3] and local implementing laws (together "**ePrivacy Laws**"), which sit alongside the GDPR, setting out specific privacy rights relating to electronic communications. One example of this relates to the fact that successful MaaS solutions will require or desire access to location data, to offer suitable travel solutions and travel and traffic updates, including updated journey solutions, where appropriate. The ePrivacy Laws will apply to the storage or accessing of information in the terminal equipment of a subscriber or user within the EEA. In the case of MaaS, this is currently most likely to relate to a user's mobile phone. The European Data Protection Board, the body that brings together representatives from the national data protection authorities of all EU Member States (the "**EDPB**"), released guidance in May 2019, on the interplay between the ePrivacy Directive and the GDPR, and the EDPB confirmed that Article 5(3) of the ePrivacy Directive makes clear that consent is required for storing or accessing information on a user's device. This consent must be GDPR-grade consent, i.e., it must be freely given, specific and informed, obtained through an unambiguous, clear, affirmative action. Note, however, that the ePrivacy Directive applies whether or not the data is personal data so a broad standard is being imposed here. Any further processing of personal data thereafter, will additionally be subject to the GDPR.

Of further consideration for the future of MaaS, is the working draft of the ePrivacy Regulation, which is intended to replace the ePrivacy Directive and is, at a high level, largely aimed at broadening the scope of the protection currently offered to cover new technologies, including Internet of Things ("**IoT**") services. Given that this is also a 'Regulation', rather than a 'Directive', this means that it would have direct effect across Member States and should lead to greater harmonisation across the EU. The draft Regulation is subject to ongoing negotiations between EU Member States, so, at this stage, it is not certain how this will impact access to location data, or other information used in MaaS, but more stringent rules relating to access to location data could add a further complication to the deployment of MaaS platforms / ecosystems.

2.4 Impact on cross-border sharing

A MaaS ecosystem is formed of numerous stakeholders, including, to list a few:

- the MaaS aggregator;
- the digital platform developers and operators;
- software providers;
- telecom providers;



[3] Directive 2002/58/EC

- traffic and route data providers;
- payment services providers;
- transport service providers,

with additional layers of stakeholders added to this, such as cloud and marketing service providers.

Cross-border sharing of data is likely, whether this is within the EU / EEA, or to outside the EU / EEA (e.g., to offer cross-border MaaS solutions or where stakeholders use US-based cloud providers). Therefore, a harmonised, consistent way in managing that data, whether personal or non-personal, particularly within the EU, is key.

2.5 Applicability to MyCorridor and the deployment of commercial MaaS

User trust has been identified as key to a successful MaaS ecosystem, and was a focus and discussion point between industry stakeholders at the first pan-European MyCorridor Project workshop, held in Osborne Clarke's London office on 9 February 2018. User trust will inevitably require MaaS stakeholders' transparency and compliance with applicable data protection laws. However, trust needs to be obtained not only from consumers, but also between the various stakeholders within the MaaS ecosystem so that public and private sector stakeholders are willing to open up their data to others for successful MaaS deployment. Therefore, the focus for any MaaS ecosystem must be on the legal and ethical considerations around managing and using data (personal and non-personal data), including data protection, as well as good governance, accountability and transparency. Meeting the GDPR's transparency, accountability and compliance requirements means that user and public / private sector trust is more likely to be achievable, and quality data more accessible.

The MyCorridor Consortium partners dedicated significant time from the start of the MyCorridor project to discussing the types of personal data the MyCorridor project would require access to; how this personal data would need to be used; who this personal data would need to be shared with; how this personal data would be protected; the potential security risks; how such risks could be mitigated; and, how users would be informed about the MyCorridor project's processing activities in accordance with the GDPR's transparency requirements, particularly Article 13 of the GDPR.

Article 13 of the GDPR requires specific information to be provided to individuals at the time personal data is collected from them, including (among other matters): details of the controller; who personal data will be shared with; the purposes of the processing; retention periods; individuals' rights; processing carried out for the purposes of profiling (and the consequences of such profiling); and the period for which personal data will be stored. This information is most commonly presented to users via a privacy policy. Importantly, this information must be presented to individuals, using clear and plain language, **before** that individual shares any personal data, and thereafter individuals must be able to easily access that privacy policy at all times throughout the life of the project.

The above will apply equally to real life commercial deployment of MaaS. That said, MaaS in a commercial context (as opposed to the research project setting of MyCorridor) will come with increased risks and challenges in relation to data, given the vast amounts of data and the scale of processing and sharing of data required to ensure that the multiple stakeholders involved in delivering a successful MaaS solution can work together seamlessly to deliver accurate and tailored travel solutions to individuals on a large scale.

Therefore the initial stages of any MaaS project should be focused on incorporating privacy by design, to ensure that the processing of personal data is limited only to what is necessary to achieve its purpose, that this personal data is encrypted and pseudonymised where and to the extent possible, and that access to personal data is limited to those who need it to provide the MaaS services to users. In the initial stages of developing a MaaS platform or ecosystem, focus should therefore be immediately on the security architecture required to minimise any risks of unauthorised access or loss to that personal data. Privacy by design, pseudonymisation and other measures which can be taken to ensure the protection of personal data are discussed further below.

2.6 Broad definition of "personal data"

Personal data is *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an* ***identification number****,* ***location data,*** *an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*[4]

This broad GDPR definition, which expressly lists 'location data' and 'online identifiers' will capture a significant portion of data used in MaaS, particularly given the broad definition of 'processing' under the GDPR, which covers "***any operation*** *or set of operations which is performed on personal data or on sets of personal data*".

The MyCorridor project dedicated time from the outset, before the deployment of the MaaS platform, to identifying which data was personal data. While some personal data may be clearly identifiable as personal data, such as a name, email address, home address, and bank account / card payment details, sometimes it is not always as clear.

One example of this is where data about an individual is well encrypted, so that there is no immediate identification of an individual by a person viewing that data. However, if a holder of the encryption key has the ability to decrypt the relevant data sets and re-identify individuals, or if additional information could enable identification of individuals, this amounts to personal data.

Location data is also an example of personal data which can reveal a lot more about an individual than may be immediately obvious on its face. For example, any location data which gives visibility over the fact that someone commutes from A to B at the same time every day, or on regular days, may enable identification of that individual or at least certain characteristics relating to that individual, such as their home or work location.

Indeed, for a MaaS solution to operate effectively, and enable a user to get from A to B seamlessly, including through the provision of live travel updates, location data is fundamental. Location data enables a MaaS provider to offer an accurate and valuable service, but also to subsequently learn insights about

[4] Article 4 GDPR

travellers, usually in the aggregate, to improve the quality of the services provided or even to manage traffic flow and congestion to improve journey efficiency. Indeed, geolocation data can reveal a lot about an individual. However, this location data is likely to be considered highly personal by the individual, given that it provides MaaS stakeholders who can access this data with a window into other personal data about that individual; while invaluable to the relevant MaaS stakeholders, this may be seen as intrusive or a security risk by that individual. Importantly, location data may reveal a user's religious beliefs, sexual orientation or health-related information (based on places they regularly visit), all amounting to 'special categories of personal data', subject to more stringent requirements under the GDPR. We consider 'special categories of personal data' further below.

2.7 Data protection principles

Individuals are unlikely to sign up to use a MaaS platform if the platform operator is not clear and transparent about how personal data is processed, or if a MaaS platform or other stakeholder within the MaaS ecosystem uses personal data in a manner which is inconsistent with the key principles relating to the processing of personal data under the GDPR. These principles are:

(a) 'lawfulness, fairness and transparency', i.e., that personal data must be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*"[5];

(b) 'purpose limitation', which requires personal data to be used for "*specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*"[6];

(c) 'data minimisation', requiring personal data to be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*[7];

(d) 'accuracy', to ensure personal data is "*accurate and kept up to date*"[8];

(e) 'storage limitation', requiring personal data to be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*"[9];

(f) 'integrity and confidentiality', requiring personal data to be processed "*in a manner that ensures appropriate security of the personal data"*[10]; and

(g) 'accountability', imposing a responsibility for ensuring and demonstrating compliance with the requirements set out in (a) to (f) above.[11]

These principles can be looked upon as a challenge by stakeholders within a MaaS ecosystem. Owing to the high value of data in MaaS, stakeholders within a MaaS ecosystem might seek to hold on to all data, including personal data, for as long as possible, in case it can be used for providing any further valuable insights in the future, given the reliance on these insights to optimise a MaaS solution.

2.8 Lawful grounds for processing

The processing of personal data must be carried out based on one of the six lawful grounds set out in Article 6 of the GDPR. The following three lawful grounds are most likely to be appropriate for a MaaS

[5] Article 5(1)(a) GDPR
[6] Article 5(1)(b) GDPR
[7] Article 5(1)(c) GDPR
[8] Article 5(1)(d) GDPR
[9] Article 5(1)(e) GDPR
[10] Article 5(1)(f) GDPR
[11] Article 5(2) GDPR

ecosystem. However, reliance on any of these grounds will require a careful assessment prior to any processing of personal data.

The 3 lawful grounds most applicable to MaaS:

- 'consent'
- 'legitimate interests'
- 'necessary for the performance of a contract'.

It is often assumed that consent is required to process personal data, when in fact another lawful ground may be more appropriate. Valid consent can be difficult to obtain within a MaaS ecosystem, which relies on vast amounts of data and large scale data processing among numerous stakeholders. To be valid, consent must be freely given, specific, informed and unambiguous, obtained through a clear, affirmative, action. Obtaining this level of consent may not always be practicable, and may limit access to data and add complexities to sharing that data with third parties within the MaaS ecosystem. The data subject is also free to withdraw their consent at any time, which could be disruptive and challenging where personal data is shared with multiple parties. Where consent is required, stakeholders must additionally ensure they have appropriate practices in place to obtain and document that appropriate consent was obtained.

'Legitimate interests' or the fact that the processing is 'necessary for the performance of a contract' may be more appropriate for some processing activities relating to MaaS. When seeking to rely on the 'legitimate interests', a three-step balancing exercise must be carried out beforehand. This balancing test requires an assessment and documentation of whether the processing meets each limb below.

1) Purpose test: are you pursuing a legitimate interest?
2) Necessity test: is the processing necessary for that purpose?
3) Balancing test: do the individual's interests override the legitimate interest?[12]

Importantly, these legitimate interests cannot override the interests or fundamental rights and freedoms of the data subject, requiring protection of personal data, and legitimate interests cannot be relied on if there is another reasonable and less intrusive way to achieve the same result.

Owing to the vast amount of personal data and processing activities that a MaaS ecosystem may need to rely on, assessing and ensuring that there is an appropriate lawful ground for each processing activity can be time consuming and challenging for stakeholders. Sufficient time must be dedicated to assessing the appropriate lawful ground in each context, and documenting that assessment process.

2.9 Special categories of personal data

To ensure the MyCorridor platform offered users a personally valuable and fair service, particularly from an equality perspective, the MyCorridor Consortium spent time assessing how they could ensure that users with specific requirements (including mobility disabilities) were not excluded from using the MyCorridor platform /mobile app and could receive tailored travel solutions suitable for them.

The aim of any MaaS service is to facilitate mobility and, where possible, to offer tailored mobility solutions. This is what the MyCorridor platform sought to do. However, in order to deliver users tailored solutions, users may wish to provide a MaaS platform with additional information about themselves, which may either expressly state, or otherwise enable MaaS providers to infer, certain characteristics, which could constitute 'special categories of personal data' for the purposes of the GDPR.

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

'Special categories of personal data' are defined in Article 9 of the GDPR as "*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".

The type of transport modes selected by an individual or any special requests made by an individual could lead to access to information about that user's disabilities, i.e. health related data. Further, location data may also reveal certain sensitive information falling within the definition of 'special categories of personal data'. For example, regular visits to hospitals might reveal health problems, or visits to a place of religion may reveal religious beliefs.

Processing special categories of personal data not only requires a lawful ground under Article 6 of the GDPR, as discussed above, it is actually prohibited under the GDPR except in specific circumstances set out in Article 9 of the GDPR. For the purposes of a commercial MaaS application, explicit consent from the data subject (being one of the permissible circumstances set out in Article 9 of the GDPR) is likely to be the most appropriate Article 9 ground for MaaS stakeholders to process special categories of personal data. However, explicit consent requires a very clear, specific, informed, statement of consent, which is specific to the processing activity. It should also be noted that this is one area where Member States may introduce further conditions or limitations, particularly with regards to genetic data, biometric data or health-related data; therefore, this is one example where cross-border challenges may impact the seamless cross-border deployment of MaaS, requiring extra care to be taken to ensure compliance across borders.

2.10 Data protection by design and security

Data protection should be central to the way that stakeholders within a MaaS ecosystem plan and operate. This requires each stakeholder with access to personal data within the MaaS ecosystem ensuring that it has appropriate technical and organisation measures in place, which are appropriate to the risk involved (a key requirement under the GDPR), and minimising any processing of personal data to only that which is necessary for the purpose. While the GDPR does not itself go into detail about specific security methods, it does require the implementation of the following, as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[13]

MaaS platforms and ecosystems must ensure that appropriate technological protections are implemented by design and default, such as technical barriers, regular security testing, and the pseudonymisation and encryption of data where possible. Some specific transport operators, including operators of ITS, and some service providers may also have to consider enhanced security obligations, for example, under the NIS Directive[14] (and its corresponding local implementing legislation) which provides measures for ensuring a common EU-level of security of network and information systems, or, if you're an entity that stores, processes or transmits cardholder data, under PCI DSS[15], which sets out an information security

[13] Article 32 GDPR
[14] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[15] Payment Card Industry Data Security Standard

standard to increase security controls with respect to cardholder data. Building ethical practices into how personal data is collected and processed, including around who can access personal data is also key.

Within the MyCorridor project, in-depth discussions were held between MyCorridor Consortium partners, to ensure that appropriate technical and organisational measures were in place, including pseudonymising data and creating technical barriers to prevent unauthorised access to personal data.

Each MyCorridor Consortium partner also carried out an assessment of whether a data protection officer (a "**DPO**") should be appointed. Under the GDPR a DPO must be appointed, if:

(a) you are a public authority;

(b) your *core activities* require *large scale, regular and systematic monitoring* of individuals; or

(c) your *core activities* consist of *large scale processing* of special categories of personal data or data relating to criminal convictions and offences.[16]

A DPO has specific requirements under Article 39 of the GDPR, including (among others) monitoring compliance with the GDPR and applicable data protection laws.

'Core activities' must be the primary business activities of the organisation. To determine whether the core activities involve *'regular and systematic monitoring'*, the Article 29 Working Party ("**WP29**"), the EDPB's predecessor, provided guidance[17], explaining that this would include all forms of tracking and profiling, both online and offline, and that '*large scale'* processing, may require consideration of the following factors:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.

While the MyCorridor project was not processing personal data about significant numbers of data subjects, in a commercial MaaS environment there would be large scale processing of a wide range and volume of personal data, and, possibly, large scale tracking of individuals. In a cross-border MaaS ecosystem, this would significantly increase the geographical extent of that processing as well.

It is clear that significant time and resource must be dedicated to ensuring that appropriate data protection, technical and organisational measures, and strong governance measures are in place from the inception and throughout the life of a MaaS ecosystem, with ongoing proactive monitoring and updating of such practices.

[16] Article 37 GDPR
[17] Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016, as last revised and adopted on 5 April 2017, 16/EN WP 243 rev.01 - http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

2.11 Data mapping and Data Protection Impact Assessments

Data mapping is key when dealing with big data. The MyCorridor Consortium partners were aware of this from the start of the MyCorridor project. While the MyCorridor project partners did receive personal data from a variety of internal and external service providers and from individuals participating in MyCorridor's trials of its MaaS platform (the "**Pilots**"), in a commercial MaaS ecosystem tracking personal data flows would likely be more complicated and could become a complicated web, which would be difficult to untangle if not mapped out from the start.

Tracking and mapping personal data flows and subsequent personal data processing activities are important to assist a MaaS ecosystem in ensuring compliance with the GDPR and applicable data protection laws, but can also be used to help track and maximise the value in data accessible to a MaaS ecosystem.

Not only will data mapping form part of the documentation process required by Article 30 of the GDPR, this exercise should also be considered as a first step when looking to carry out a Data Protection Impact Assessment (a "**DPIA**").

The GDPR states: *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data".*[18] This 'assessment' is a DPIA.

Even where a DPIA is not mandatory under the GDPR, it is highly recommended by various data protection regulators, particularly where large scale processing of personal data is taking place.

The UK's data protection regulator, the Information Commissioner's Office (the "**ICO**"), makes clear that a DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.[19]

[18] Article 35 GDPR
[19] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

The GDPR identifies 'new technologies', 'large scale processing' and 'monitoring' as types of processing requiring a DPIA.[20] These are of course highly applicable to MaaS, where vast amounts of data are processed on a large scale by multiple stakeholders, relying on the most effective, modern technologies, where possible, to process various types of personal data, including location data to track users as part of the provision of seamless and accurate journey solutions.

The ICO has also identified (among others) the following as practical examples of types of processing requiring a DPIA, which are highly relevant to MaaS: (a) machine learning; (b) some Internet of Things ("**IoT**") applications (depending on the specific circumstances of the processing); and (c) Intelligent Transport Systems ("**ITS**"). The ICO suggests that in these cases a DPIA may be mandatory under the GDPR. The ITS Directive[21] defines ITS as *"systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport"*. To be successful, a MaaS ecosystem will, where possible, rely on innovative technologies, including IoT and ITS to offer a seamless travel experience for users, and therefore it would be good practice, if not mandatory, for a MaaS platform and certain stakeholders within a MaaS ecosystem to carry out a DPIA or similar assessment.

Even where carrying out a DPIA is not mandatory under the GDPR, it is indeed good practice to carry out a DPIA. While the MyCorridor project wasn't processing personal data to anywhere near the same extent as a commercial deployment of a MaaS ecosystem would, the MyCorridor Consortium decided that it would be good practice to complete a DPIA. Despite this being a research project, with limited access to data, owing to the numerous stakeholders and various types of data (predominantly personal data) required to provide users with a tailored MaaS solution, even at a research project level, this was a complex task.

In a commercial MaaS context, it is recommended that time is dedicated to carrying out a DPIA from the outset, even if a DPIA is not considered mandatory under the GDPR and applicable data protection laws. This DPIA should also be regularly revisited (and where necessary, updated) throughout the life of the MaaS ecosystem. This will ensure that all stakeholders are clear on the risks associated with the personal data they are processing and enable strong mitigation measures, including appropriate security architecture, to be put in place in advance, and minimise the risks of unauthorised access to or loss of personal data.

Public trust can be damaged by data breaches, so MaaS ecosystems must implement and maintain robust data security and data governance procedures. Of course, without these, businesses also risk exposure to enforcement action (which may be from multiple regulators for a cross-border MaaS solution), including potentially very high fines, as noted earlier.

Significant investment in robust security technologies, data mapping and carrying out a DPIA from the project's inception, can also add value to MaaS, by minimising the security risks and thereby creating a path to ensuring and demonstrating compliance with the GDPR and applicable data protection laws. These activities can create opportunities to build individuals' trust, which, in turn, will increase the number of users of a MaaS solution and the MaaS platform's access to data, to facilitate accuracy and optimisation for a competitive MaaS solution.

[20] Article 35 GDPR
[21] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport Text with EEA relevance

2.12 Controllers and processors

The GDPR places obligations on both controllers and processors. Controllers are, at a high-level, the main decision makers in relation to personal data, in particular over the means and purposes of the processing of that personal data. Processors act on the instructions of the relevant controller in relation to the processing of that personal data. However, identifying which entity is or which entities are, controllers or processors in a MaaS ecosystem, where there are numerous stakeholders sharing personal data, can be a complex task. It may even be the case that, in some circumstances, a MaaS stakeholder is both a controller and a processor of personal data. MaaS stakeholders will need to also consider whether, in relation to some processing activities, they might be joint controllers, i.e., jointly determining the purposes and means of the processing of the same personal data. Understanding whether a MaaS stakeholder is a (a) controller, (b) joint controller, (c) controller in common with another controller, or (d) a processor is key in determining the responsibilities and compliance obligations of each stakeholder within the MaaS ecosystem, both towards other stakeholders in the MaaS ecosystem (or external data providers) and towards data subjects / users of the MaaS platform. Therefore, considerable time will likely need to be dedicated to this from the inception of any MaaS project.

2.13 Pseudonymisation

The GDPR encourages the use of 'pseudonymisation' techniques, which result in personal data no longer being attributable to a specific individual without the use of additional information (with such additional information being kept separately and subject to appropriate technical and organisational measures)[22]. Importantly, 'pseudonymisation' is not 'anonymisation', as defined in Recital 26 of the GDPR. Anonymisation is the process of removing all direct and indirect identifiers, to the extent that there are no means of identifying the individual (even through the addition of other information). Anonymised data falls outside the scope of the GDPR, but pseudonymised data does not; pseudoymised data is nevertheless a highly recommended safeguard to protect personal data. Truly 'anonymising' data can be difficult to do in practice, and sometimes impractical in a MaaS environment[23], where access to personal data will sometimes be required.

There is sometimes a misconception that personal data has been anonymised when in fact it has just been pseudonymised. When dealing with big data in a MaaS context, extra time and care must be taken to assess whether anonymising personal data is possible, and if so whether appropriate techniques have been carried out to ensure that this data is truly anonymised. Where anonymising personal data is not possible, pseydonymising personal data should be carried out where and to the extent possible. However, it is important to appreciate that, while pseudonymising personal data may reduce risks associated with the processing of that personal data, such as unauthorised access to that personal data, pseudonymisation does not lower compliance requirements with the GDPR and applicable data protection laws.

2.14 Processing of children's personal data

A MaaS ecosystem will want to offer its services to as many people as possible, and this may include people under the age of 16. However, the GDPR imposes stricter rules in relation to obtaining consent for

[22] Article 4(3)(b) GDPR
[23] Guidance on how to practically anonymise data was released by the EDPB's predecessor (the Article 29 Working Party) – 'Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014' https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

'children', who, at a GDPR-level, are those people under the age of 16, when offering online services, namely 'information society services'[24].

Article 8 of the GDPR prohibits reliance on consent from a person under the age of 16 without parental or legal guardian consent. However, this is one area where Member States' laws do vary, therefore, depending on which Member State the platform is operating in, there may be stricter rules around consent for users under the age of 16. In the UK, the Data Protection Act 2018 has set this age at 13, being the lowest age permitted by the GDPR, meaning that, in the UK, the stricter rules in relation to consent for 'children' do not apply to any users of the platform who are aged over 13. However, the Netherlands, for example, requires parental or legal guardian consent for anyone aged under 16 years. Ensuring parent or guardian consent has actually been obtained can be difficult in practice, and care must be taken to ensure reasonable steps have been put in place to verify that consent in practice.

In a commercial MaaS environment, it is assumed that a MaaS platform would not wish to cut off a demographic of users under the age of 16 completely. Therefore, given the potential for MaaS platforms to be fairly privacy intrusive, particularly through the collection of location data, extra care and consideration must be given to how this parental consent will be obtained and verified, from the platform's inception. This is particularly the case with a MaaS solution offering services across borders.

2.15 Individuals' rights

The GDPR grants specific rights to individuals in relation to their personal data, (the rights of access, rectification, erasure, restriction of processing, data portability, objection and the right not to be subject to decisions based solely on automated decision making, including profiling[25]), as well as timeframes within which to respond to certain data subject requests.[26] This can bring challenges to a MaaS ecosystem owing to the potentially complex network of data flows and range of data processing activities.

Individuals must be notified of their rights, including their right to lodge a complaint with the relevant supervisory authority. These rights must be clearly presented to individuals in a transparent way. MyCorridor ensured this information was accessible to individuals in a privacy policy, accessible via the website and in the mobile app, before a user shared any personal data and created an account. However, the challenge to a MaaS ecosystem, isn't so much about notifying users of these rights, but on ensuring MaaS Stakeholders are clear about who is responsible for responding to requests from individuals exercising their rights, and how such requests will be communicated and managed between the relevant MaaS stakeholders, so that this information can be clearly communicated to individuals. This is why these responsibilities must be clearly assessed and documented in appropriate contracts between the relevant MaaS stakeholders in advance of sharing any personal data, as discussed further below.

Technological and organisational measures must also be appropriate to ensure that, where an individual exercises its data protection rights, a response can be issued promptly and in accordance with the timeframes stipulated within the GDPR.

2.16 Contractual frameworks

Businesses are reluctant to share valuable data, so where data is to be shared, (personal and non-personal data), contractual frameworks are key to ensuring that stakeholders within a MaaS ecosystem can access data and share data in a protected way, without losing control of that data. Owing to the numerous

[24] defined as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*" (Article 1(1)(b) Directive 2015/1535)
[25] As set out in Articles 15-22 GDPR.
[26] Article 12(3) GDPR.

stakeholders involved in a MaaS ecosystem and the potentially vast amount of personal data being processed, complex data flows can be at the centre of MaaS, requiring strong contractual protections for all parties involved. This can result in a complex contractual chain of obligations, responsibilities, warranties and liabilities in relation to that data. Notably, the EU Commission has acknowledged the challenges which arise from data-driven solutions, where data needs to be shared between businesses or between businesses and government, and has provided some guiding principles and considerations in this regard in its 2018 Communication 'Towards a common European data space'.[27]

With respect to personal data, the GDPR requires specific contractual provisions to be entered into between controllers and processors, and between joint controllers. However, as noted in section 2.12 above, determining whether the relationship is one of (a) controller to controller; (b) controller to processor; (c) processor to processor; or (d) joint controllers, or a combination of the above can be a challenging task within MaaS. While the GDPR does not require contractual provisions to be entered into between two controllers, this is highly recommended. Indeed, MaaS stakeholders need to dedicate time to overcoming challenges in determining who should be responsible and ultimately liable for any incidents, errors and breaches, contractually.

In particular, the MyCorridor project identified potential difficulties in practice in determining where liability should fall in some circumstances within a MaaS ecosystem. For example, where a user complaint arises as a result of the provision of inaccurate data, should this liability sit solely with the platform, or can the platform carve out and pass on its liability to its suppliers and service providers? Alternatively, where there is a misuse of data and a security breach arises, how is this managed contractually between all relevant stakeholders? Owing to these complexities, contracts need to be carefully considered and negotiated, to ensure reasonable protections are in place in relation to all data being shared (personal and non-personal data).

A potential solution to some aspects of these complex networks of negotiations and contracts can be seen in the emergence of 'data institutions', which are designed to offer a form of data governance, to encourage access to, and sharing of, data (not just personal data). These 'data institutions' could offer a governance solution for data sharing within MaaS, by building trust between various stakeholders and thereby increasing access to data, while also gaining and maintaining user trust. A 'data trust' is one type of a data institution, which is currently being explored at EU and national levels. Data trusts can take various legal and commercial forms. A data trust creates a common approach across stakeholders to how the data is managed, shared and otherwise processed, ensuring this is done in an ethical way in compliance with applicable data protection laws. The proposed EU Data Governance Act is targeted at creating a regulatory framework to facilitate these data institutions and trusts in a bid to open new business opportunities, while ensuring good data governance.

Data trusts can work as a new way to encourage parties to pool together data and share data, including personal data, with a data trust as the intermediary. All stakeholders agree on the terms of the data trust, but the trustee (or 'data steward') has some control over that data, taking on responsibility and liability over decisions made relating to the data held in the trust, based on the terms and the purpose of the trust as agreed between all stakeholders. In turn, this can facilitate data sharing between competitor stakeholders by ensuring that confidentiality is maintained.

Users' privacy interests as well as confidentiality of business stakeholders may be better protected with such a data sharing model, thereby potentially encouraging data sharing and unlocking greater benefits

[27] Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions: "Towards a common European data space"

for users and stakeholders, which could help the deployment and growth of MaaS, particularly through the emergence of new entrants in MaaS, who may otherwise not have access to that data.

2.17 Access to data

Access to data was repeatedly raised throughout the term of the MyCorridor project, in workshops and related events, as a concern among industry stakeholders, which was viewed as a potential barrier that could stifle the deployment of MaaS. Indeed, as highlighted in this Deliverable, data lies at the heart of a successful MaaS ecosystem. Therefore, those with access to data, who are likely to be already well-established in the mobility market, are likely to succeed, while preventing access to the MaaS market for new entrants. In the 'Competition law' section of this Deliverable (Section 3) we acknowledge that competition law could be used as a form of shield in this area. However, on its own, competition law is unlikely to be the solution.

Barriers to access to data often result from a mixture of commercial, legal and technical concerns. Legal barriers arise from the protection afforded to personal data, and the added challenges in protecting this personal data when it is being shared with third parties. These challenges are increased when looking to share personal data outside the EU or the European Economic Area ("**EEA**"), particularly to third countries such as the United States, where there is significant reliance on US-based cloud storage or hosting providers. Notably, the EU Commission has identified the dependency on non-EU based providers, owing to the EU's small share in the cloud market.[28] Transfers to third countries now also bring further challenges, following the Court of Justice of the European Union's recent decision which invalidated the EU-US Privacy Shield[29] and placed stricter obligations on data exporters to assess whether transfers to data importers in third countries are subject to a level of protection essentially equivalent to that guaranteed in the EEA, and to implement supplementary measures where required. Therefore, as mentioned earlier, MaaS stakeholders need to ensure that they carefully assess and map their potentially complex network of data transfers to ensure appropriate measures are in place for the ongoing protection and security of that personal data during and post transfer.

Measures are being taken at an EU-level to try to address some of the legal, technical and commercial barriers that exist, such as the lack of technical standardisation, particularly in relation to ITS, which could, in turn, assist the development of MaaS ecosystems and deployment of MaaS. For example, the ITS Directive, which is largely aimed at interoperability, has led to the introduction of delegated acts, implementing data sharing obligations, including in relation to EU-wide multimodal travel information services; the provision of EU-wide real-time traffic information services; and safety-related information. The EU Commission has also committed to reviewing the ITS Directive and its delegated regulations in 2021, to further encourage data availability, reuse and interoperability across Member States.[30]

Further, the Open Data Directive[31], which revised the PSI Directive[32] aimed at encouraging the re-use of public sector information, is focused on expanding access to public sector data. However, this sharing of data will still be subject to licensing and contractual requirements which may not always favour new entrants, and the EU Commission has also identified that access to the most valuable data in mobility, dynamic data, is limited, which can cut off access to valuable transport and travel data[33].

[28] The EU's Data Strategy – 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data, Brussels, 19.2.2020 COM(2020) 6 final
[29] Judgment in Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems
[30] See footnote '28'
[31] Directive (EU) 2019/1024
[32] Directive 2003/98/EC subsequently amended by Directive 2013/37/EU
[33] 'Sharing Europe's digital future: From the Public Sector Information (PSI) Directive to the open data Directive' - https://ec.europa.eu/digital-single-market/en/public-sector-information-psi-directive-open-data-directive

In any event, where and to the extent this open data consist of personal data, personal data protection is still key and could even create barriers to accessing certain data. Notably, the GDPR expressly states that the Open Data Directive "*should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data*"[34]. Indeed, there is a clear and recognised tension between opening up access to data and the protection of personal data.

This is nevertheless an evolving area, and under the EU's Strategy for Data,[35] a focus is on ensuring that more data is made widely available by opening up access of high-value public datasets free of charge, in machine-readable format, through standardised APIs.

In its Strategy for Data[36], the EU Commission stated that transport and mobility are at the forefront of the debate on data sharing, and the Commission is exploring rolling out common European data spaces in mobility, to offer EU-level governance and to facilitate access to, pooling and sharing of data (including personal data). The focus is on ensuring harmonised compliance across the EU, with the aim of facilitating cross-border data use, and ensuring the prioritisation of interoperability requirements and standards. The Commission is also exploring measures necessary for establishing data pools for data analysis and machine learning, among various other matters which could offer opportunities for the future deployment of MaaS. The proposed EU Data Governance Act (mentioned earlier), released on 25 November 2020, begins to address these issues by creating an enabling legislative framework with a focus on: (a) the re-use of public sector data subject to data protection legislation, intellectual property, or containing trade secrets or other commercially sensitive information; (b) data intermediaries; (c) data altruism; and (d) the development of a European Data Innovation Board expert group.

It is clear that EU-level intervention is required to not only open up access to data, but to ensure harmonisation, interoperability, and a level of access which will enable smaller businesses and new entrants to play a part in the deployment of MaaS. However, this will need to be balanced with ensuring good governance and ethical uses of personal data in compliance with applicable data protection laws; a challenge that will not be easy to address.

2.18 Conclusion

Data lies at the heart of MaaS. It is integral to developing an accurate and valuable MaaS solution. The data relied on by a MaaS ecosystem is often personal data, including sensitive personal data, such as location data, which can reveal very sensitive information about an individual, including about their health or religious beliefs, among other sensitive matters.

Access to data is therefore intrinsically linked to user trust. Without user trust, a MaaS ecosystem will not have access to the data it requires to offer an optimised, accurate, tailored and valuable solution, which offers a competitive level of service to users. MaaS ecosystems need to therefore ensure that personal data is protected and only used to the extent necessary, in compliance with the GDPR and applicable data protection laws. Further challenges are introduced when looking at offering a seamless MaaS solution across borders, where laws and the regulatory framework may differ. However, without user trust, the data sets available to a MaaS operator are going to be minimal, incomplete, and consequently lacking in value.

[34] Recital 154 GDPR
[35] Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, 'A European strategy for data', Brussels, 19.2.2020, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf
[36] As above.

The GDPR can be seen as a hindrance, but it in fact offers opportunities to MaaS stakeholders, by prescribing measures with which to comply when processing personal data. By ensuring, and being able to demonstrate, compliance with the stringent levels of protection afforded to individuals under the GDPR and ePrivacy Laws, user-trust will be more easily obtained. In turn, this will increase quality personal data available to stakeholders in a MaaS ecosystem.

New entrants to the mobility and MaaS market are faced with increased challenges with respect to access to data. While EU and national policy and legislative movements could encourage data pooling, sharing and access to data, there are also technical and commercial challenges to consider, together with the inherent tension between opening up access to data and ensuring ongoing data protection.

National and EU-level policy and legislative movements to facilitate large scale data sharing in mobility could shape the development of MaaS. However, opening up access to data brings a natural tension between access to data and protection of personal data.

The key takeaway is that, in order to establish user trust, data protection must be a top priority for a MaaS platform and ecosystem from its inception, before any personal data is processed. This includes ensuring privacy by design and default, mapping out the projected data flows, and identifying any risks and ways of mitigating these risks through a DPIA. Given the vast amounts of data processed and the numerous stakeholders involved in a MaaS ecosystem, market-leading security measures are key. Proactive and ongoing governance, security and regulatory compliance procedures will encourage users to sign up to the MaaS solution and share their personal data.

3 Competition law

3.1 Introduction: overview of competition law in the EU

There are two fundamental principles of EU competition law:

- **Article 101 TFEU** prohibits anti-competitive agreements (including verbal/informal agreements and concerted practices) between undertakings. Undertakings are entities carrying out economic activities and we anticipate that, as it provides services to consumers, MyCorridor would be caught be considered an 'undertaking' and caught by competition law.

  Anti-competitive agreements are those which have the object or effect of restricting trade between EU Member States without objective justification. In order to be justifiable, a restrictive agreement must produce efficiency benefits that are shared with consumers and go no further than is required to achieve those benefits. 'Block exemptions' for certain categories of agreement are also available – these are measures that set conditions for certain types of agreement which, if met, provide an automatic exemption from the Article 101 prohibition.

- **Article 102 TFEU** prohibits the abuse of a dominant position. Dominance normally arises where an undertaking has more than a 40% market share and will be presumed above 50%. Dominant companies are under a 'special responsibility' not to allow their conduct to distort competition on the common market. This may, for example, require that a dominant company provides access to certain assets on 'fair, reasonable and non-discriminatory terms'.

Companies in breach of competition law are liable to fines of up to 10% of worldwide turnover. Third parties affected by the breach can also take court action to enforce competition law and/or bring a damages action in respect of any losses.

Certain markets/companies are also subject to ***ex ante* regulation** to create conditions of competition where this would not otherwise exist – for example, in markets characterised by monopoly infrastructure. The European Commission is currently considering whether/how digital markets, characterised by leading platforms, should be regulated in this way. Two proposed pieces of legislation: the **Digital Services Act** and the **Digital Markets Act** (together referred to below as the "**DSA**") would potentially regulate 'gatekeeper' platforms in markets and may therefore have an impact on MaaS platforms. If implemented, the DSA would give the Commission the power to intervene to address systematic problems of contestability, fairness and market entry. For example, the Commission might prevent certain market 'gatekeepers' from 'self-preferencing' (discriminating in favour of their own services on their platforms); refusing reasonable data access requests and imposing unfair contractual provisions. There may also be positive obligations to make data portable to and/or interoperable with other services. All of these developments would have an impact on the development of MaaS platforms within the EU.

3.2 Applicability of existing competition law to MyCorridor

A MaaS platform could be subject to competition law in the following ways:

- If it is party to restrictive agreements;
- If it coordinates the competitive conduct of third parties that compete with each other; and/or
- If it gains a dominant position in any market;

It is also possible that a MaaS platform may be impacted by competition law to the extent that it interacts with a dominant player.

3.3 Restrictive Agreements – Article 101

The MyCorridor Consortium entered into a range of agreements with mobility providers and others in order to operate its service for the purposes of the Pilots. We consider that in the context of a research project, and given that the agreements were designed for non-commercial Pilots, there was a very low risk of these arrangements including restrictions that would fall within the Article 101 prohibition.

In a commercial cross-border MaaS setting, to the extent that agreements could impact trade between Member States (for example, if they contain exclusivity provisions) they will be caught by competition law and will need either individual or block exemption. In this regard, a key aspect of the MyCorridor project is cross-border MaaS and the single market imperative of Article 101 may support this objective, including by giving a cross-border MaaS platform potential grounds to resist any attempt to geo-block (i.e. restricting access to content or services by geographical location) or otherwise restrict cross-border trade.

3.4 Vertical agreements

Where a MaaS platform such as MyCorridor does not compete with mobility providers (for example, the platform provider does not offer its own transport services), its agreements with mobility providers will be treated as vertical for competition law purposes. Provided both parties have **less than 30% market share** of any relevant markets, these agreements will fall within the 'safe harbour' of the Vertical Agreements Block Exemption Regulation ("**VBER**"), provided they do not contain any **'hard core'** or **'excluded'** restrictions (which include certain pricing, territorial and sales restrictions considered to be particularly egregious from the perspective of competition law). In particular, to fall within the VBER the following requirements apply:

- There must be no resale price maintenance (pricing arrangements between mobility providers and MyCorridor will need to be competition law compliant);
- Any exclusivity cannot exceed five years; and
- There must be no unlawful partitioning of the EU market (e.g. restrictions on providing cross-border services).

If either party has more than 30% market share (for example, a mobility provider with a strong local market position) then more detailed competition law assessment of any restrictions will be required.

3.5 Horizontal agreements

Where mobility providers have a competing service (or could be expected to launch one in the short to medium term), they will be considered to be an actual or potential competitor and additional assessment will be required to ensure compliance with competition law. For example, a MaaS platform will need to ensure that it does not receive **competitively sensitive information** (e.g. future pricing or strategy information) or otherwise agree to coordinate its commercial conduct with competitors. Where it is strictly necessary to receive competitively sensitive information for the operation of a MaaS platform, such information will need to be appropriately ring-fenced from any personnel involved in competing activities.

We would also flag that MyCorridor and other MaaS platforms engage with third parties that compete with each other – for example, competing ride hailing service providers. In these circumstances, MyCorridor must ensure that it does not coordinate their competitive conduct, including sharing competitively sensitive information between providers. If this may be necessary (for example to facilitate through-ticketing), we would recommend that specific competition law advice is taken and ring-fencing or other measures are implemented. We would also recommend that key platform personnel engaged

with competing mobility providers receive competition law training to help them avoid sharing sensitive information between competitors. To the extent that information will be ring-fenced automatically (e.g. so that only MyCorridor and the consumer sees journey information), this will minimise the prospect of any competitively sensitive information being shared between providers.

3.6 Abuse of dominance – Article 102

At launch, the MyCorridor platform will not have a dominant position. However, it is possible that any MaaS platform could gain one in the short to medium term – either in a particular geographic market or because of its EU-wide coverage.

In these circumstances, the MaaS platform would be subject to the 'special responsibility' of dominant companies and might find that other services make claims on competition law grounds. These could include requesting access to the platform on 'fair, reasonable and non-discriminatory terms' or that customer data is portable/interoperable (e.g. so that a consumers can port their profiles – including, for example, travel preferences identified by MyCorridor – to another provider). It is also possible that, if a MaaS platform abused its dominant position, a competition authority might investigate.

3.7 Interacting with dominant companies

At least in the short term, it may be more likely that Article 102 will bite on a new MaaS platform's transport service providers – for example, a leading ride hailing provider or regional transport monopoly. In these circumstances, the dominant player will be subject to its own 'special responsibility' under competition law. This may give MyCorridor or other start-up MaaS platforms greater scope in negotiations – for example, to ensure pricing is not excessive and that the platform gains reasonable access to any requisite data or services.

In addition, we would flag that the VBER will not apply where a partner has more than 30% share of the market and so additional assessment of the agreement may also be required under Article 101.

3.8 Pilot

We did not consider that dominance would be a significant concern during or coming out of the Pilots – at least in respect of MyCorridor itself. However, where a new MaaS platform anticipated that it could gain a dominant position in the short to medium term, it would be worth it considering the potential implications of this as soon as possible. For example, assessment could be made of the policy for granting access to the platform.

Article 101 will have applied from the point that MyCorridor first entered into agreements (whether formal/informal) with third parties. As mentioned, we consider that in the context of a research project, and given that the agreements were designed for non-commercial Pilots, there was a very low risk of these arrangements including restrictions that would fall within the Article 101 prohibition. If the platform were to transition towards commercial operation we would recommend that existing and new agreements with service providers are assessed for compliance with competition law, in particular to identufy any restrictions on how participants are able to act in their relevant market.

3.9 Looking forward: Broader considerations in MaaS

MaaS platforms and other journey integrators will inherently coordinate competing services and gain insight into future strategy (for example upcoming pricing changes, promotional activity and the launch of new services). Competition law should therefore always be on the agenda to ensure that this collaboration does not expose the provider to a competition law risk.

Market share may also grow quite rapidly – particularly as mobility markets are often local. Competition law is increasingly focused on dominant positions in digital markets and may intervene to force access to integrator platforms, require data sharing, interoperability and portability; and/or require the provision of APIs to competing services.

A good example of the ways in which a regulator might intervene in MaaS, including under the DSA, is the recent European Commission merger control decision on the Daimler/BMW/ Car sharing JV[37] . In that case, Daimler operated an integrator app called 'moovel' and the Commission was concerned that the merger of Daimler's car sharing activities with BMW's would increase its incentives to favour moovel over competing integrators. In response to these concerns, Daimler offered to provide API access to third party aggregator platforms so that they could redirect users to Daimler/BMW; access to moovel was also provided for interested car sharing providers.

As set out above, if implemented, the DSA (and parallel proposals underway in several EU Member States and the UK) has the potential to impose new regulation on key players in the MaaS ecosystem – for example, Uber has been mooted as a company that might be designated a 'gatekeeper', which would result in Uber being subject to a code of conduct regulating its behaviour in the market, including potentially the terms of its contracts with third parties such as MyCorridor. Other ancillary services – for example Google's digital advertising ecosystem, which MyCorridor may rely on for marketing – may also be subject to DSA regulation.

It is also possible that, in the longer term, MyCorridor might itself be considered a 'gatekeeper', if it transitioned to commercial operations and acquired this position in the market.

Any 'gatekeeper' would be subject to future regulation under the DSA. Although we await the final provisions, it is possible that this would cover key areas relevant to MaaS including the data, access and contract requirements set out above. It is also possible that it will regulate 'nudging' of consumers to particular services (e.g. if a MaaS integrator favoured journey options using a particular provider).

[37] See *Case M.8744 - DAIMLER / BMW / CAR SHARING JV*

4 Payments law

4.1 Introduction: overview of payments law in the EU

One of the most important operational features of MyCorridor and 'mobility as a service' (**MaaS**) is the ability for a consumer traveller to easily pay for combined transport services from multiple providers (who may be based in different Member States) and potentially of contingent amounts. Both consumer payer and transport merchant payee will be in receipt of regulated payment services of some kind when completing a transaction via a MaaS platform.

Notably (and helpfully in this context) the European Commission has introduced a legislative framework with the intention of creating an integrated market for payment services in the EU:

4.1.1 The Electronic Money Directive 2009/110/EC (EMD)

The EMD introduces the concept of "electronic money", which is defined below. The EMD prohibits persons from issuing e-money unless they are excluded under the 'limited network exclusion' (considered further below) or authorised as;

(i) a credit institution (i.e. a bank); or

(ii) as an 'electronic money institution' (**EMI**) authorised by the relevant national competent authority in accordance with the EMD;[38]

In addition to setting out the authorisation regime, the EMD also contains the prudential and conduct of business requirements that apply to EMIs when issuing e-money.

4.1.2 The Revised Payment Services Directive (EU) 2015/2366 (PSD2)

PSD2 is similar to the EMD in that it defines 8 different 'payment services' and prohibits persons from providing such payment services unless they are excluded[39] or authorised as:

(i) a credit institution (i.e. a bank);

(ii) an EMI; or

(iii) a 'payment institution' authorised by the relevant national competent authority in accordance with PSD2 (**API**).[40]

PSD2 sets out the prudential requirements for APIs. An API must be expressly authorised for each one of the 8 payment services it provides. So, for example, an API that was only authorised for money remittance would not be permitted to carry out merchant acquiring services or to offer

[38] National central banks and certain 'post office giro institutions' and other public authorities may be entitled to issue e-money in accordance with domestic law. Note also that persons may fall outside of scope if eligible for the 'limited network exclusion' which is considered later in this note.
[39] under any of the exclusions set out in PSD2.
[40] Note that PSD2, like EMD2, also contains provisions dealing specifically with national central banks, 'post office giro institutions' and other public authorities.

payment accounts. EMIs that are authorised under EMD are entitled to provide all payment services under their EMI permission.[41]

PSD2 also contains the conduct of business requirements that apply to every category of 'payment service provider' (**PSP**) listed above, when providing payment services. The prudential requirements applicable to APIs and the conduct of business rules that apply to all PSPs will apply differently depending on the payment services being provided.

It is also worth noting that the European Banking Authority has, pursuant to its mandate under PSD2, issued numerous 'regulatory technical standards' and 'guidelines' that expand upon the PSD2 compliance requirements for PSPs.

4.1.3 The Cross Border Payments Regulation (EC) No 924/2009 as amended by Regulation (EU) 2019/518 (CBPR2)

CBPR2 requires PSPs to charge the same fees for cross-border payments in euro as would be charged for equivalent domestic payments in the local currency. It also requires PSPs and other parties providing currency conversion services at ATMs or point of sale terminals to disclose information on the currency conversion rates and fees prior to the initiation of the transaction.

4.1.4 The SEPA Regulation 2012 (EU) No 260/2012

The SEPA Regulation sets the rules for euro area countries to make credit transfers and direct debits in euro under the same conditions. It also contains arrangements for euro transfers in euros in countries outside of the euro area.

4.1.5 The Interchange Fee Regulation (EU) 2015/751 (IFR)

The IFR applies to card-based payment transactions and sets a cap for the 'interchange fees' charged by a card issuing PSP to a merchant card acquiring PSP for card payments. It also sets conduct of business rules, for example around transparency of fees and unbundling, for merchant acquiring PSPs and card schemes (e.g. Visa and Mastercard) that are designed to increase competition in the card payment sector.

PSD2 and EMD2 are likely to be the most relevant to the MyCorridor proposition (and MaaS more generally) for the following reasons:

(i) The regulatory perimeter: these directives set the 'regulatory perimeter' for payment and e-money services within the EU, i.e. what activities are in scope and therefore regulated. In terms of structuring a MaaS model, it will be necessary to understand what payments capability is required and to ensure that the relevant PSP has the requisite authorisation in order to lawfully deliver the required capability. If, for example, the MaaS model involves the payer or payee creating a stored or prepaid balance, this could amount to the issuance of e-money under EMD, which would require the involvement of an authorised EMI or a credit institution. If the model involves 'mere' payment services under PSD2 then such services may be provided by an EMI, credit institution, or an API that is authorised to provide the relevant payment service.

[41] Although in the UK, the new data-based payment services of account information and payment initiation services are subject to special rules that require pre-notification by the EMI before providing such.

PSD2 and EMD both provide an authorisation framework whereby non-bank PSPs, like VivaWallet, can provide services (such as acquiring or card issuing) that were historically the reserve of banks. PSD2 and EMD also expressly allow EMIs and APIs to appoint 'agents' to carry out payment services on their behalf. This means that MaaS providers can choose from a wider range of providers, payment-related products, services and models.

(ii) The conduct of business rules: these directives also contain the main body of rules that govern the relationship between the PSP and the 'payment service user' (**PSU**). PSD2 is almost certain to apply to some extent to the PSP of the payer and payee in a MaaS or e-commerce platform context. The other Regulations listed *may* apply depending on the nature of the services provided and, with the exception of the currency conversion rules in CBPR2, do not directly apply to payment services provided to consumers (i.e. they set B2B rules).

4.2 Applicability to MyCorridor

In this section 4.2, we have considered how the MyCorridor payments ecosystem was *originally* described and envisaged in the MyCorridor Grant Agreement. We have considered some of the high-level concepts – such as e-money tokens - contemplated in the Grant Agreement and how these concepts may fit into the EU payments regulatory regime. In section 4.3, we consider how the payment functionality was *actually* structured in the Karhoo Pilot.

The Karhoo Pilot reflects one way in which it is possible to structure MyCorridor/MaaS payments, but it is not the only way (and other structures could be considered for future projects). We think it is useful not just to look at how the Karhoo Pilot was, in fact, structured, but to further explore *possible* ways to structure MyCorridor or MaaS platforms more generally. The objective in this section 4.2 and sections 4.4 and 4.5 is to draw out some of the broader regulatory issues that may need to be considered in the next phase of MyCorridor development or MaaS projects more generally.

(a) The MyCorridor Grant Agreement originally envisaged the following payments capability:

(i) In respect of the consumer payer: the consumer payer was envisaged as purchasing 'e-money vouchers' or 'e-money mobility tokens' (which may be held in an e-wallet of similar). These mobility tokens could be used to make purchases with their chosen, participating transport provider(s) via the MyCorridor platform. Depending on the functionality, these 'e-money vouchers' could fall within scope of EMD as regulated e-money issuance (although, as we explain below, the consumer payer is not issued with e-money in the Karhoo Pilot):

"'Electronic money' means "electronically, including magnetically, *stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions (as defined in PSD2) accepted by a natural or legal person other than the electronic money issuer".* If, for example: (i) the consumer payer used their payment card (or other payment method) to purchase e-money mobility tokens (from the "issuer" of such tokens); and (ii) these tokens created a stored monetary value; and (iii) the tokens were accepted as a form of payment by transport providers (i.e. persons other than the issuer), then such tokens could fall within the definition of e-money.

Unless e-money instruments (which could include tokens) are eligible for the 'limited network exemption' (considered further below), the relevant 'issuer' of such tokens

would need to be duly authorised for e-money issuance, i.e. authorised as an EMI or an e-money issuing credit institution.

(ii) In respect of the payee transport service provider: the original MyCorridor specification (set out in the Grant Agreement) also acknowledges the need for settlement of payment to the transport service provider ("**merchant**") and contemplates such settlement via "wallets" held for the merchant. As with the consumer payer, if the merchant wallet comprises 'stored monetary value' (i.e. a balance) that can spent by the transport provider with third parties (i.e. "*persons other than the issuer*" as per the definition of e-money), this could also amount to regulated e-money issuance.

It is, however, possible to structure payment settlement services for the seller in a marketplace platform without creating an e-money stored balance. For example, the merchant could be receiving the payment service of 'acquiring' or 'money remittance' rather than holding electronic money.

(b) The original proposed model for MyCorridor therefore appears to envisage e-money being issued to the consumer and the merchant by the same PSP. In this model, the PSP would have regulatory and compliance obligations vis-à-vis both the payer consumer and the payee merchant under PSD2 and, where the payer and/or payee was issued with e-money, also under the EMD. However, as we note below, in the Karhoo Pilot, VivaWallet, as PSP, only provides regulated services to the merchant (i.e. Karhoo) and not the consumer payer.

(c) Provided that the PSP in the MyCorridor model is an EMI, no separate authorisation for payment services would be required (as an e-money permission automatically covers payment services). In this regard it is worth noting however, that issuing e-money will always involve the provision of related payment services, e.g. payments into, between, and out of an e-money stored balance will constitute 'payment transactions' under PSD2 and will be subject to the conduct of business rules therein.

4.3 Karhoo Pilot

(a) In the Pilot involving Karhoo, a ride hailing platform, VivaWallet acts as the authorised EMI and PSP, which means that it can issue e-money and provide payment services.

Our understanding is that, in the Karhoo Pilot, the consumer does not receive regulated services from VivaWallet: rather, the consumer will simply make a MyCorridor 'Booking' using their payment card, with such funds transferred to VivaWallet, acting in its capacity as PSP for the payee merchant. This transfer of funds from the payer consumer to payee merchant (albeit via VivaWallet) is analogous to any other e-commerce transaction made by the consumer using his or her payment card: the payer's PSP, i.e. their card issuer, has regulatory responsibility for that card transaction, but this falls outside of scope of the MyCorridor arrangements (i.e. the payer's card issuer has no direct relationship with VivaWallet or Karhoo). The 'MyCorridor platform terms and conditions for Pilot participants', appended at Annex IIB of this Deliverable, reflect this arrangement and recognise VivaWallet's role in accepting the consumer payer's card payment.

In a card payment context, the relationship and liability as between the card issuing PSP and the merchant's PSP (i.e. VivaWallet) is governed, directly or indirectly, by the card scheme rules (e.g. Visa or Mastercard scheme rules).

The MyCorridor agreement with Karhoo provides at clause 8, that the "*Payment Services Provider* [VivaWallet] *is solely responsible for providing the regulated payment and e-money services* to *Karhoo contemplated under this section 8 in accordance with the Payment Services Provider's Terms of Business and shall do so in accordance with its obligations under the relevant national law implementing the Payment Services Directive (EU) 2015/2366 and the Electronic Money Directive 2009/110/EC and any applicable card scheme rules (including for example the Visa and MasterCard scheme rules) ("Applicable Requirements")*. This provision makes clear that VivaWallet will provide Karhoo with regulated payment services and e-money pursuant to VivaWallet's Terms of Business. We did not carry out a comprehensive review of VivaWallet's Terms of Business for the purposes of this project, however, our understanding is that VivaWallet will provide Karhoo with a 'wallet' into which the consumer's card payment funds are transferred and held prior to settlement to Karhoo. On the face of it, this wallet appears to meet the 'stored monetary value' limb of the e-money definition: this initial assessment aligns with the VivaWallet Terms of Business which also refer to the provision of an e-money "wallet".

As set out above, the MyCorridor agreement with Karhoo and the VivaWallet Terms of Business both contemplate VivaWallet providing e-money services pursuant to its authorisation as an EMI. For clarity, it's important to note that a bank account involves regulated "deposit taking": this is not the same as an e-money wallet and requires specific authorisation as a 'credit institution' (i.e. authorisation as a bank). EMIs are not permitted to offer bank accounts. If a PSP is proposing to provide banking services in a MaaS context, it must be authorised as a credit institution and must comply with specific conduct of business rules relating to the operation of bank accounts. We have not considered this "banking" functionality further, as our understanding is that VivaWallet is authorised as an EMI rather than a credit institution and this is reflected in the MyCorridor contractual documentation (VivaWallet's regulatory status – as a bank or EMI - must be confirmed by VivaWallet).

(b) The rule in PSD2 and EMD prohibiting unauthorised persons from providing payment or e-money services extends to *promising* (i.e. contracting) to provide payment services or issue e-money.[42] We included the following language at clause 8.1 of the MyCorridor agreement with Karhoo to reflect this:

> *"The parties acknowledge and accept that the Payment Services Provider [i.e. VivaWallet] is solely responsible for providing the regulated payment and e-money services contemplated under this section 8 in accordance with the Payment Services Provider's Terms of Business and shall do so in accordance with its obligations under the relevant national law implementing the Payment Services Directive (EU) 2015/2366 and the Electronic Money Directive 2009/110/EC and any applicable card scheme rules (including for example the Visa and MasterCard scheme rules) ("Applicable Requirements")."*

The purpose of this wording is to ensure that the other MyCorridor Consortium partners were not inadvertently *promising* to provide Karhoo with payment or e-money services in breach of the prohibition in PSD2 and EMD (because they are not authorised to carry out such regulated activities).

(c) VivaWallet, as the authorised PSP, is responsible for compliance with the relevant requirements when delivering its payment service to Karhoo and is liable under statute (PSD2 and EMD as

[42] Under the UK law transposing PSD2, the Payment Services Regulations 2017, it is a criminal offence to provide, or purport to provide payment services without authorisation (regulation 138). Regulation 139 similarly makes it a criminal offence for an unauthorised person to describe themselves or hold themselves out as a person that is authorised to provide payment services. Regulations 63 and 64 of the Electronic Money Regulations 2011 (the UK law transposing EMD) contains similar prohibitions on purporting to provide e-money.

relevant) and under the contract it has with Karhoo (i.e. 'Payment Services Provider's Terms and Conditions of Business').

VivaWallet is required to comply with the information requirements for payment services in Title III of PSD2 (these rules apply to all PSPS, including credit institutions and EMIs). Amongst other things, VivaWallet must enter into a separate 'framework' contract with Karhoo for the provision of regulated payment services which sets out the information proscribed in PSD2. The 'Payment Services Provider's Terms and Conditions of Business' acts as the framework contract.

(d) One of the potentially challenging payment related features of the MyCorridor proposition is that the final purchase price may change once the journey is completed (e.g. if a Karhoo journey is longer than anticipated, the final price may be higher than the original price displayed at the time of booking). In this pilot, Karhoo requested a pre-authorisation feature to deal with this issue (in the same way that card pre-authorisations are often used by car hire companies or hotels where the final price may not be known). The ability for a merchant to request a card pre-authorisation from a payer involves a number of contractual and regulatory considerations:

(i) The contract between the merchant and their PSP (i.e. their merchant acquirer) must permit such pre-authorisation requests and the payer's PSP (i.e. their card issuer) must comply with the request to block the pre-authorised amounts for the required amount of time. In the context of the VivaWallet pilot, it was not clear whether VivaWallet acted as Karhoo's 'acquirer (from a card scheme perspective) or whether it received funds from its own acquirer as merchant of record. In the latter case, VivaWallet's own merchant acquirer would need to permit pre-authorisation requests.

(ii) The card schemes (e.g. Visa and Mastercard) set rules in relation to card pre-authorisations and may impose maximum time limits for blocking funds on a card. The card scheme rules will apply to both card issuers and acquirers and we would expect to see such rules flowed down into the framework contracts that the PSPs have with their PSUs (i.e. the consumer payer and the merchant payee).

(iii) PSD2 also sets rules relating to the authorisation of transactions generally which may be relevant in the context of card pre-authorisations. PSD2 also provides for refund rights (subject to certain conditions) where the payer is able to show that the final amount pulled from the card was not duly authorised.

(e) For all of the reasons listed above, it is, in our view, relatively high risk for a merchant to rely on pre-authorisation as a means of receiving payment in full. Providing the consumer payer with a pre-paid e-money option could potentially solve some of these issues: for example, the EMI could transfer the 'excess' funds to the merchant's e-wallet (imposing restrictions on withdrawal as necessary and in compliance with the EMD) with any unused balance being transferred to the consumer's e-wallet at the end of the journey. The key difference is that, in this scenario, the EMI is the PSP to both the payer and the payee and therefore has more control over the funds and fund transfers between payers and payees (and further, where there is no card payment, transfers between e-wallets would fall outside of scope of the card scheme rules).

4.4 Exclusions

(a) MyCorridor has many features in common with other marketplace platforms in the sense that it connects travellers with travel providers and provides the ability for the traveller to make payment via the MyCorridor platform. There are numerous ways to structure such two-sided

marketplace platforms and the most appropriate solution will depend on what the parties want to achieve contractually and operationally. It may be possible to structure the platform so that the payment element falls out of scope of regulation entirely, for example by relying on an express exclusion. The most relevant for present purposes are likely to be the 'limited network exemption' or the commercial agent exemption, although we have flagged some others.

Limited network exclusion

(b) Both of the EMD and PSD2 contain the 'limited network exclusion' (**LNE**). Note that the LNE is the only exclusion in EMD, whereas there are numerous exclusions set out in PSD2. The scope of the LNE under PSD2 and EMD is almost identical:

Under PSD2, the following is excluded from regulation: "*services based on specific payment instruments that can be used only in a limited way, that meet one of the following conditions: (i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a limited network of service providers under direct commercial agreement with a professional issuer; (ii) instruments which can be used only to acquire a very limited range of goods or services; (iii) instruments valid only in a single Member State provided at the request of an undertaking or a public sector entity and regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer*;

(c) In the context of MaaS, it may be possible to rely on the LNE under either the first or second limb: for example, where the issuer of a payment instrument (e.g. a pre-paid card or stored value voucher):

(i) has a direct contractual relationship within a "limited network" of transport service providers for the purposes of accepting such payment instrument; or

(ii) where the payment instrument can only be used to acquire a "very limited range" of transport services.

(d) Note that (in the UK at least) the regulator tends to interpret the LNE narrowly, which typically means that, in relation to limb (i) the limited network of transport service providers must be fixed (and not capable of continually expanding) and that the relationship must be "direct", i.e. it would not be sufficient to have indirect relationships with the payee merchant (e.g. through an operating company or franchise arrangement). The number of merchant payees who accept such payment would, in our view, need to be few in number in order to be eligible. Similarly, the limited range of services test is also interpreted very narrowly. For example, a fuel card that is limited only to the purchase of fuel may be eligible, but if expanded to cover, say any purchase at a gas station, this could take it out of scope of the LNE.

(e) Note that PSD2 introduced a notification requirement for providers wishing to rely on the LNE where the total value of payment transactions executed over the preceding 12 months exceeds the amount of EUR 1 million. There is currently no mechanism by which an LNE provider can 'passport' an LNE approval received in one Member State to another Member State. This means that an LNE provider that operated across the EU would need to obtain LNE exclusion status in each Member State in which it operates (if the conditions for notification are met). This can be contrasted with an EMI that offers regulated e-money services: an EMI can, subject to certain notification and approval requirements, passport its services into other Member States in accordance with the freedom to provide services and the freedom of establish.

Commercial agent exclusion

(f) PSD2 also excludes "payment transactions from the payer to the payee through a commercial agent authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee;"

(g) This exclusion has historically been used by marketplace platforms to avoid regulation under PSD1. However, PSD2 tightened the scope of the this exclusion specifically to deal with platforms, as explained in recital (11) to PSD2:

"The exclusion from the scope of [PSD2] of payment transactions through a commercial agent on behalf of the payer or the payee is applied very differently across the Member States. Certain Member States allow the use of the exclusion by e-commerce platforms that act as an intermediary on behalf of both individual buyers and sellers without a real margin to negotiate or conclude the sale or purchase of goods or services. Such application of the exclusion goes beyond the intended scope set out in that Directive and has the potential to increase risks for consumers, as those providers remain outside the protection of the legal framework. Differing application practices also distort competition in the payment market. To address those concerns, the exclusion should therefore apply when agents act only on behalf of the payer or only on behalf of the payee, regardless of whether or not they are in possession of client funds. Where agents act on behalf of both the payer and the payee (such as certain e-commerce platform), they should be excluded only if they do not, at any time enter into possession or control of client funds."

(h) To illustrate, if the entity providing payment capability in a MaaS marketplace platform was expressly authorised by each payee transport provider to conclude the sale of a combined package of services with a consumer on the providers behalf, or had the authority to set the price of such services (in accordance with agreed parameters) this could be sufficient for that entity to argue the payment collection and settlement services (provided to the payee merchants) were out of scope on the basis that it was receiving such payment as commercial agent of the merchant.

Low-value mobile payments for tickets

(i) Although unlikely to be relevant to a marketplace platform like MyCorridor (given the value caps), it is worth flagging the PSD2 exemption for low-value mobile payments for "tickets".

The following is out of scope of regulation under PSD2: *"payment transactions by a provider of electronic communications networks or services provided in addition to electronic communications services for a subscriber to the network or service…performed from or via an electronic device and charged to the related bill …(ii) for the purchase of tickets; provided that the value of any single payment transaction referred to in points (i) and (ii) does not exceed EUR 50 and the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month"*

Recital (16) of PSD2 explains how this could be relevant in a MaaS context: [this specific exclusion was] "introduced to take into account the development in payments where, in particular, customers can order, pay for, obtain and validate electronic tickets from any location and at any time using mobile phones or other devices. Electronic tickets allow and facilitate the delivery of services that consumers could otherwise purchase in paper ticket form and include transport, entertainment, car parking, and entry to venues, but exclude physical goods. They thus reduce the production and distribution costs connected with traditional paper-based ticketing channels and increase customer convenience by providing new and simple ways to purchase tickets."

4.5 Other compliance considerations in a MaaS context

(a) In this final section, we have flagged some broader compliance issues that may be relevant to MaaS participants in the EU:

Cross-border services and harmonisation issues

(b) Throughout this note we have, for ease, referred to VivaWallet or a PSP being "subject" to PSD2 or EMD. However, from a legal perspective, the PSP is in fact subject to the national law implementing the relevant directive in the PSP's 'home state' (i.e. the Member State in which the PSP is authorised). In VivaWallet's case, it will be subject to the Greek law implementing PSD2 and EMD as this is where it is established and authorised as an EMI. In order to provide services in other Member States, a PSP must obtain a (services or establishment) 'passport' pursuant to the provisions in PSD2 or EMD as applicable. Both PSD2 and EMD are maximum harmonizing directives, so the expectation is that compliance requirements will not differ significantly between Member States to allow the service to be provided in the same way across the EU. This is clearly helpful when designing a pan-European MaaS platform, however, in our experience there can nonetheless be differences in the way that national competent authorities interpret the rules, and in particular the regulatory perimeter: for example, an activity viewed by some continental regulators as the operation of payment accounts under PSD2 is often viewed by the UK regulator as e-money under EMD, which can lead to discrepancies in the scope of permissions required between different Member States. Similar discrepancies can be seen in the way that national regulators interpret the scope of exclusions, so that a business may be treated as out of scope on the basis of the commercial agent exemption in one Member State but not another. PSD2 has sought to address this, but it is likely that some differences in interpretation remain.

(c) Consideration may also need to be given to non-EU consumers, for example, tourists resident in third countries that want to use MyCorridor or similar European MaaS platform. If a PSP provides non-EU residents with payment or e-money services from an establishment in the EU, then such services will likely continue to fall within scope of PSD2 and EMD to a large extent. There may, however, be some differences in the level of protection available, for example non-EU citizens may be ineligible for Member Sate dispute resolution services. In this context, it is also worth noting that the EU Commission has (by way of a competition decision) recently extended the ban on interchange fees to cards issued in third countries when used in the EU.

(d) For a pan-EU marketplace, participants will need to consider how to deal with payers and payees using different currencies. This could impact in a number of ways, for example: a PSP or a non-regulated party that provides currency conversion services conversion at a point of sale (e.g. an e-commerce payment page) will need to comply with the disclosure requirements introduced under CBPR2. PSD2 also requires the PSP to provide the PSU with information on currency conversion rates and charges. Similarly, if the PSP is required to safeguard "relevant funds" (in accordance with PSD2 or EMD) the PSP will need to consider how to hold such funds to reflect the different currencies used.

Anti-money laundering

(e) A PSP that enters into a business relationship for the purposes of providing regulated payment or e-money services to a 'customer' will fall within scope of the fourth anti-money laundering directive (EU) 2015/849 (**4MLD**) as an 'obliged entity'. Amongst other things, that PSP will be obliged to carry out 'customer due diligence' on the customer (i.e. the recipient of the regulated service). This can be quite an onerous compliance requirement and applying such customer due

diligence (e.g. identifying and verifying the customer) at onboarding stage will necessarily add friction into the customer journey. Clearly, identification and verification measures in a financial services context are key to mitigating the risk of money laundering or terrorist financing, and most consumers will be familiar with requests for ID in a banking context for example. However, consumers may be less willing to identify themselves (e.g. by providing a copy of their ID) in a MaaS or e-commerce context. In our experience, structuring the payment element of a marketplace platform so as to avoid falling within scope of 4MLD can often be a key consideration for platform providers.

Future developments?

(f) The **European Payments Initiative,** recently launched by 16 European banks seeks to replace national schemes for card, online and mobile payments with a unified card and digital wallet that can be used across Europe, thereby doing away with the existing fragmentation. As it is based on the SEPA instant credit transfer (SCT Inst) scheme, it can immediately capitalise on powerful and sophisticated existing infrastructures, such as the Eurosystem's TARGET Instant Payment Settlement (TIPS).

5 Consumer law

5.1 Introduction: New Deal for Consumers

Following a recent review of EU consumer law by the Commission, it was identified that EU consumer law should be updated, as it had not kept pace with recent developments in e-commerce, and that the enforcement regime relating to breaches of consumer law should also be strengthened. As a consequence of this, the EU Commission launched its "New Deal for Consumers" initiative. In practice the New Deal for Consumers will introduce two new pieces of legislation.

The first is Directive 2019/2161, commonly referred to as the "Omnibus Directive", which must be implemented by Member States by 28 November 2021, with the local implementing laws entering into force by 28 May 2022. The Omnibus Directive introduces greater enforcement and enhances existing EU consumer protection rules, by requiring Member States to introduce GDPR-style fines for breaches of existing EU consumer law. Currently, breaches of consumer protection law do not generally attract substantial fines but, in the future, maximum regulatory fines could be at least 4% of turnover in the Member State or Member States concerned. Group actions will also be possible. Companies will therefore need to ensure proper compliance with consumer protection law. The Omnibus Directive also introduces greater transparency requirements and obligations to deal with e-commerce platforms such as "online marketplaces"[43] (which would likely capture MaaS platforms), including requirements around search result rankings and online reviews of goods and services.

The second piece of legislation is still currently at proposal stage but is expected to be brought into EU law imminently. It is a directive to provide collective redress for consumers. This proposed directive will require Member States to allow consumer bodies to bring collective actions for compensation with respect to breaches of various regulations and directives which give consumers rights. This includes not only the general body of EU consumer law but also various transport specific directives and regulations.

5.2 Applicability to MyCorridor

5.2.1 Exemptions from EU consumer law

There is an important carve out from the pre-contractual information requirements under EU consumer law for providers of passenger transport services[44], as passenger transport services are already subject to other EU legislation, or in the case of public transport and taxis, by national-level regulation. However, this carve out is disapplied in ways which are relevant to MaaS. For example, the Omnibus Directive does require that certain provisions of the Consumer Rights Directive[45] do still apply to passenger transport services.

For example, Article 22 of the Consumer Rights Directive, which deals with pre-contract requirements in relation to payments will apply to passenger transport services. Article 22 requires that, before a consumer can be bound by a contract or offer, they must provide their express consent to any extra payments in addition to the remuneration already agreed. Failure to obtain this consent from the consumer could entitle the consumer to a reimbursement.

[43] defined in the Omnibus Directive as a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers;
[44] although please note that mode-specific transport regulation typically includes pre-contract information requirements prior to purchase of a ticket: see for example Article 8 (Travel Information) of Regulation 1371/2007/EC on rail passengers' rights and obligations.
[45] Directive 2011/83/EU

These obligations came to light in the MyCorridor project, when the MyCorridor partners were contracting with a transport service provider that offered ride-hailing services. This provider sought to impose strict contractual obligations on the MyCorridor partners operating the MyCorridor MaaS platform. These were focused on ensuring that consent was obtained from trial participants with respect to any extra payments falling due that were above the original marked price. The consent to impose such charges was sought in advance of the individual providing their payment details and a booking being confirmed. The extra prices for the ride-hailing service related to (a) waiting time; (b) multiple stops; and (c) physical damage caused by the consumer (among other matters).

Contractual liability was also imposed on the MyCorridor partners to reimburse the ride-hailing service provider where a consumer had to be reimbursed, as a result of advanced consent to such extra charges not being obtained.

The Omnibus Directive also disapplies the carve out for passenger transport services in relation to certain pre-contractual information requirements set out in the Consumer Rights Directive, relating to distance contracts concluded by electronic means. This is relevant in the context of passenger transport services being offered by a MaaS platform, and therefore, in the context of MaaS, there are likely to still be requirements to provide certain pre-contractual information.

For example, Article 8(2) of the Consumer Rights Directive will require passenger transport service providers entering into distance contracts to provide consumers with (among other information): (a) a clear description of the services offered; and (b) the total price of the goods or services (inclusive of taxes), or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated.

However, when considering consumer law obligations from the perspective of the MaaS platform itself, it is likely that any carve outs to the applicability of consumer law will not apply to MaaS platforms themselves in any event, because these platforms will not be providing the actual transport service, rather they contract with consumers to facilitate access to various transport modes. As a consequence, MaaS platforms operating within the EU will most probably need to comply with the full body of EU consumer law.

That said, the above conclusion remains slightly uncertain because "*passenger transport services*" are not actually defined in EU consumer law. While the recitals to the Consumer Rights Directive suggest that passenger transport services should be taken to mean any transport regulated by other EU legislation, as well as public transport and taxis[46] regulated at a national level, Member State implementing legislation may diverge from this in a way that could catch platforms offering passenger transport services as well as the transport providers themselves. This means there could be inconsistencies across the EU in how the requirements to provide pre-contractual information to consumers apply to MaaS platforms and other stakeholders in a MaaS ecosystem. For this reason, any MaaS platform and other MaaS stakeholders that operate across multiple Member States will need to look at this in relation to the implementing legislation in each individual Member State in which they operate.

5.3 New Deal for Consumers and MaaS

The New Deal for Consumers will likely impose certain additional obligations on MaaS platforms. For example:

- transparency obligations where consumers are offered various transport options / journey solutions via the MaaS platform;

[46] Recital 27 of the Directive 2011/83/EU

- transparency obligations in relation to the due diligence carried out with respect to reviews published on the MaaS platform relating to the various transport services offered; and
- other transparency obligations, which are imposed on "online marketplaces", which will likely capture MaaS platforms, as noted in the 'Introduction' section (section 5.1), above.

We examine each of these 3 themes in the paragraphs below. As a general comment, it is worth noting that all of these transparency measures are likely to be viewed as baseline consumer expectations for MaaS. In other words, providing transparency about the range of transport options and service quality are probably already key elements that go to the heart of consumer trust in MaaS platforms. An example of this experienced during the MyCorridor project (and noted by another MyCorridor Consortium partner), was that, where a user found the MyCorridor mobile app difficult to navigate, they simply stopped taking part in the MyCorridor trials of the app. In other words, factors like ease of use and transparency of information are likely to provide a competitive advantage to a MaaS platform, by encouraging user trust in the platform.

In addition to the 3 themes noted above and discussed below, as a result of the New Deal for Consumers, MaaS platforms in the EU could be subject to collective actions for compensation from consumer groups where they do not comply with these transparency obligations. In the context of cross-border MaaS, this could result in actions from consumers based in multiple Member States, potentially resulting in significant fines and reputational damage, as well as costly litigation.

5.3.1 Transparency obligations where consumers are offered various transport options / journey solutions via the MaaS platform

The New Deal for Consumers places transparency obligations on online market places in relation to their methods of "*ranking*", with "*ranking*" being defined broadly to include any means by which one option is made more prominent to the consumer than another. In the context of MaaS, this could capture where a MaaS platform displays one transport service or one journey solution at the top of a list of travel options, or otherwise draws the user's attention to one particular transport service or journey solution. This definition is aligned with the definition of "*ranking*" in the Platform to Business Regulation (which we discuss further in the Platform to Business section of this Deliverable (Section 6, below)). In the context of MaaS, this transparency obligation means that, where a MaaS platform provides consumers with alternative transport-mode / journey options and these are "*ranked",* the MaaS platform must be able to provide details as to the main parameters used to rank these options, and this information must be made publicly available to consumers.

5.3.2 Transparency in relation to due diligence on reviews of services

Where an online market place publishes consumer reviews, in relation to good and services offered, they will be obliged to provide information, publicly, with respect to the due diligence they have carried out to ensure that consumers who are submitting reviews have genuinely purchased and/or used the relevant goods or service(s) reviewed. It is therefore conceivable that, where a MaaS platform enables users to publish user reviews on the platform, the provider of the MaaS platform will have to ensure they carry out appropriate due diligence in relation to each review published, and properly document this due diligence.

6 Platform to Business Regulation

6.1 Introduction

Over the last few years there has been increasing recognition that some internet platforms have incredible market power, as many businesses are dependent on them to sell their goods and/or services to consumers. This often places businesses who offer goods and/or services via such platforms in a weak negotiating position when it comes to negotiating the terms on which those goods and/or services will be offered via the platform. In many ways the position of these businesses is similar to consumers, in that they are forced to accept the policies, practices and terms offered by platforms with little or no opportunity to negotiate or even deal directly with the operator of the platform.

The EU has responded with a series of proposals and legislation intended to address this disparity in negotiating position and extend consumer law-style protections to businesses that use platforms to sell goods and/or services to consumers. The Platform to Business Regulation 2019/1150 ("**the P2B Regulation**") is the first piece of EU legislation in this area. It is also expected that the Digital Services Act, if implemented, will build on the P2B Regulation and impose additional obligations on certain platforms which have particularly strong market power. For further discussion of the Digital Services Act please see the Competition Law section of this Deliverable (Section 3).

The P2B Regulation imposes obligations on "*online search engines"* and so-called "*online intermediation services*" (each as defined below) in relation to their interactions with "*business users*" (being the businesses selling or promoting their goods and/or services via a platform to consumers).

6.2 Applicability to MyCorridor and MaaS

It is conceivable that MaaS platforms fall within the scope of the type of platform that the P2B Regulation is intended to regulate. In a situation where a MaaS platform itself exercises a significant degree of market power, (a practical example of this might be an app like WHIM, in Helsinki, which we understand may have a dominant market share in the territory in which it operates), transport providers may well have no other choice but to accept the contractual terms and other policies and practices imposed on them by the dominant MaaS platform. The P2B Regulation includes regulatory levers which could potentially address this scenario.

As discussed in section 6.1, above, the P2B Regulation applies to two categories of businesses: "*online search engines"* and *"online intermediation services*". A MaaS platform is unlikely to fall within the definition of an "*online search engine*", defined in the P2B Regulation as "*a digital service that allows users to input queries in order to perform searches of all websites on the basis of a query"*. However, it is conceivable that MaaS platforms could fall within the definition of "*online intermediation services*". "*Online intermediation services"* means services which meet all of the following requirements:

(a) *they constitute "information society services"*[47]*;*

[47] This broadly refers to any service normally provided for remuneration, at a distance, (in other words without the parties being simultaneously present), as defined in Article 1(1)(b) of Directive (EU) 2015/1535

(b) *they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; and*

(c) *they are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers.*

In the context of a MaaS platform, limb (b) simply means that the platform is the means through which the transport services providers are introduced to travellers (their consumers), and limb (c) refers to the necessary contractual terms between the MaaS platform and the transport service providers.

However, it is unclear whether a MaaS platform would constitute an *"information society service*" and satisfy limb (a). An "*information society service*" broadly covers any service normally provided for remuneration, at a distance, (in other words without the parties being simultaneously present). While it would appear conceivable that a MaaS platform would fall within this definition, as it offers services to individuals online, in December 2017, the Court of Justice of the European Union (the "**CJEU**") ruled that Uber's intermediation service, which consists of connecting users with Uber drivers, via an app, was not an *'information society service'* (as defined above).

The CJEU held that the Uber app did not constitute an "*information society service*" as it was actually a *"transport service"*, meaning that Member States can, themselves, regulate the conditions which such services are subject to.

The CJEU's decision turned on the fact that Uber exercises significant influence over the terms which users sign up to in relation to their use of the transport services provided by those Uber drivers, because, without the app, those Uber drivers would not be able to offer transport services. Importantly, the CJEU referred to the fact that Uber's services formed an "*integral part of an overall service whose main component is a transport service"*. Considering this statement in the context of MaaS, MaaS platforms enable users to travel from A to B, in some cases across borders, using multiple transport modes with just one ticket. The user is buying a "journey", rather than just a ticket for one mode of transport which they could purchase elsewhere. The MaaS platform service will therefore form an integral part of the overall transport service, as without the MaaS platform the users would not have access to these seamless transport solutions.

The above creates uncertainty as to whether MaaS platforms will be considered *'information society services'*, and thereby an *'online intermediation service'*, falling within the scope of the P2B Regulation, and indeed the P2B Regulation is silent on this point. MaaS platforms will need to determine whether their services form an integral part of an overall transport service. If that is the case, their service might not be classified as an "*information society service*" and therefore would fall outside the scope of the P2B Regulation, and would not be subject to the transparency obligations described in the sections below. However, given the lack of certainty in this area, it may be advisable for MaaS platforms to comply with the transparency obligations imposed by the P2B Regulation. In turn, this could help to build trust in the mobility industry and help to grow the deployment of MaaS. In the interim it would be helpful if the EU Commission issued guidance in this area.

6.3 Consequences of a MaaS platform being *"online intermediation services"*

The P2B Regulation imposes certain obligations on "*online intermediation services"* in relation to their dealings with business users. Of particular relevance to MaaS platforms are the obligations set out below.

(a) Obligations to ensure that the contract between the platform and the business user is drafted using plain and intelligible language, and that business users are provided with sufficient notice of any changes.

(b) Transparency obligations with respect to the conditions for access and use of data held by the platform (whether this is personal or non-personal data), and with respect to the platform's data sharing practices.

(c) Transparency obligations in connection with the way in which goods or services are ranked on the platform (we discuss ranking in the context of MaaS further below).

(d) Obligations to have formal suspension and internal complaints procedures with respect to business users. This includes an obligation to publicly report on these procedures in some cases (we discuss this further below).

(e) Obligations to be transparent about when certain business users are offered more favourable terms or access to data, or more prominence on the platform.

Some implications of these obligations for MaaS platforms (if they do fall within the scope of the P2B Regulation) are discussed in detail below.

6.3.2 Plain and intelligible drafting

Where the MaaS platform's contracts with transport service providers are on standard terms and the transport service providers have little or no ability to negotiate these terms, the MaaS platform will have an obligation to ensure that the drafting is "*plain and intelligible*" which broadly means that the contract should be easy to read and understand by a non-lawyer.

The test of "*plain and intelligible"* drafting has been adopted from EU consumer law however under the P2B Regulation the EU has diverged from EU consumer law in relation to the implications for the contract if the drafting is not plain and intelligible. Under EU consumer law, where a term in a contract is held not to be plain and intelligible, that term will only be void if it can further be shown that the effect of that term is that it is also unfair to the consumer. Article 3(3) of the P2B Regulation is stricter than the EU consumer law framework because where a contract or any clause thereof fails the "plain and intelligible" test that drafting shall be null and void, i.e. it will cease to exist and will not bind either of the parties. In practice this emphasises the importance of platform terms being drafted as clearly and plainly as possible, so that business users, or in the context of MaaS, transport service providers, enjoy a reasonable degree of predictability on the most important aspects of the contractual relationship. MaaS platforms that focus on this area, will enjoy a competitive advantage over competing MaaS platforms.

6.3.3 Notice period for the platform to amend terms and conditions

The intention behind the P2B Regulation obligations in relation to notice periods is to ensure that business users are given adequate time to adapt their business or cancel the contract before they are bound by any changes imposed on them by the MaaS platform. The notice period should be no less than 15 days from the date of notice, unless a longer period is necessary to allow business users to make "*technical or commercial adaptations to comply with the changes*". In a MaaS setting, the platform could involve a very diverse range of transport service providers, from ride-hailing service providers to micromobility, to public transport in various modes. Given this diversity, it is conceivable that some transport providers may require a lengthy period to adapt to the proposed changes (for example, public sector operators may need time to carry out consultations and some providers may need to carry out other technical or commercial adaptations to their service provision). For these reasons, within a MaaS

context, the notice period may need to be extended beyond the minimum 15 day notice period. In practice this is going to mean that MaaS platforms may find it difficult to change contractual terms once they have been entered into by transport service providers.

6.3.4 Transparency regarding options

Were a MaaS platform provides consumers with alternative transport options and journey solutions, and these are "*ranked*", the P2B Regulation would require the MaaS platform to provide details of the parameters used for ranking. The definition of "*ranking*" in the P2B Regulation is broad and includes any means by which one option is made more prominent to the consumer than another, such as by putting one option at the top of the list or otherwise drawing it to the consumer's attention. Therefore, MaaS platforms should be prepared to explain to transport service providers the main parameters through which those transport service providers are ranked on the platform. From the perspective of a transport service provider, issues around ranking are commercially sensitive because they potentially subject the transport service provider to a greater degree of scrutiny from travellers than would normally be the case where their services are offered outside the context of a MaaS platform.

Conversely, a MaaS platform may be able to differentiate itself from competing MaaS platforms through the quality of its ranking algorithm, where this algorithm enables it to provide better quality transport information to potential travellers. In light of this possible competitive advantage, a MaaS platform is likely to consider the obligation to disclose its ranking process to its transport service providers as this information would be considered by the MaaS platform as commercially sensitive. Indeed, this information could be the basis on which one MaaS platform offers a better service to consumers than another. Interestingly, the P2B Regulation is explicit that this transparency obligation should not require the disclosure of trade secrets[48], which may offer some protection. However, in spite of this helpful position in the P2B Regulation, there remains some uncertainty about the extent of the information which does need to be disclosed.

6.3.5 Data transparency obligations

The P2B Regulation requires MaaS platforms to be transparent as to the data that they hold. This obligation applies to all data, not just personal data (as defined in the GDPR[49]). Therefore MaaS platforms will need to make certain information publicly available about the data they hold. This is also an obligation which is likely to be considered commercially unattractive to MaaS platforms, because, for example, it would provide competitors and other interested parties with insight into how a MaaS platform is using data for commercial purposes.

6.3.6 Formal processes for dealing with business users

The P2B Regulation requires MaaS platforms to have formal processes in place for dealing with business users – particularly in relation to when problems arise. For example, where a transport service provider's access to a MaaS platform is being suspended, restricted or terminated, the platform provider will need to give a statement of reasons for such suspension, restriction or termination and an opportunity for the service provider to clarify any concerns. Further, there must be formal internal complaints procedures, and the MaaS platform must specify at least two mediators they are willing to engage with. All of the above obligations require significant investment in compliance and process development which would be a burden on a MaaS platform.

[48] as defined by Directive (EU) 2016/943 on trade secrets
[49] EU General Data Protection Regulation 2016/679

6.3.7 Transparency as to differential treatment

The P2B Regulation requires MaaS platforms to be transparent about when they (a) contract on different terms with different transport providers, (b) offer more prominent ranking positions to transport service providers, and/or (c) provide transport service providers with access to data that wouldn't ordinarily be provided.

In principle this would not prevent MaaS platforms offering more favourable terms or benefits to certain transport providers, but MaaS platforms should be aware of the above transparency obligations that come with this.

6.4 Future developments?

The P2B Regulation is relatively new, it only came into force in July 2020. Currently we are still awaiting formal EU guidance on certain key areas, including with respect to ranking and there is, as yet, no case law in this area. There is also uncertainty as to whether MaaS platforms will fall within the scope of the P2B Regulation. As a consequence, the application of the P2B Regulation to MaaS platforms and any resulting obligations imposed on MaaS platforms will evolve in the coming years.

7 Conclusions

Various legal and commercial issues can create challenges to the deployment of MaaS. In this Deliverable we focused on some of these issues and explored practical and legislative measures which could assist with the development of MaaS ecosystems and MaaS platforms.

One of the key lessons learned from the MyCorridor project is that access to data and stakeholder trust are integral to the success of a MaaS platform and ecosystem. To establish user trust, data protection must be a priority from the inception of the MaaS project, prior to any personal data being processed, and throughout the life of the project. This includes (among other measures) ensuring privacy by design and default, mapping out the projected data flows, and identifying any risks and ways of mitigating these risks through a DPIA. Proactive and ongoing governance, security and regulatory compliance procedures will encourage users to sign up to a MaaS solution and share their personal data.

During the MyCorridor project it became clear that EU-level intervention is required to open up access to data and create a harmonised framework to address the existing legal, technical and commercial issues which currently exist and create barriers to data sharing. The EU's proposed Data Governance Act aims to address some of these challenges through an enabling legislative framework and trusted data sharing mechanisms, and the EU's Strategy for Data indicates that we'll see a continued focus at an EU-level on opening up access to data and harmonised compliance across the EU, to facilitate cross-border data sharing, while seeking to protect commercial interests and privacy, which could facilitate the deployment of MaaS.

A lack of data standardisation and technical interoperability requirements, both at national levels and at an EU-level, can complicate, and even restrict, access to data in MaaS and the integration of various MaaS solutions. While legislative movements are being made at an EU-level, particularly as a result of the ITS Directive, at the time of writing, there is still a long way to go to facilitate MaaS. Notably, a lack of data standardisation and technical interoperability brought challenges to the MyCorridor Consortium when seeking to integrate third party solutions and access data provided by external service providers.

Competition law is a key framework relevant to the deployment of MaaS, which could be a concern to those organisations who already hold significant market power in the mobility sector. However, competition law can also help to grow the deployment of MaaS, by preventing market leaders from blocking off access to MaaS to new entrants. Importantly, to enable platforms such as MyCorridor or other start-up MaaS platforms to have greater scope in negotiations, (for example, to ensure pricing is not excessive and that the platform gains reasonable access to any requisite data or services), competition law could bite on existing dominant players.

With respect to integrating payment services into a MaaS platform, consideration needs to be given to this early on. In particular, time needs to be dedicated to assessing the payments model required for the MaaS platform, and which regulated payment service the prospective payment services providers are licensed to perform, together with the scope of the provider's licensed activities. These considerations become particularly important in a cross-border MaaS environment. The European Payments Initiative could facilitate payments in MaaS in the future. Launched by 16 European banks, the Initiative seeks to replace national schemes for card, online and mobile payments with a unified card and digital wallet that can be used across Europe, thereby doing away with the existing fragmentation.

The MyCorridor project evidenced the complex network of contracts required within a MaaS ecosystem, and the lengthy negotiations that can take place, particularly in relation to liability, with numerous

stakeholders involved in a MaaS ecosystem. Contractual liability in MaaS may be an area worthy of further research and possibly EU-level legislative intervention, to ensure that liability can be apportioned fairly and appropriately within MaaS, particularly where a MaaS platform already enjoys significant market power.

From a consumer law perspective, MaaS platforms will have to consider the consumer laws applicable to each jurisdiction in which they provide services to consumers. While there is a level of harmonisation across the EU, differences do exist which will require considerable time to ensure compliance and may prevent a uniform approach across borders. Further complications arise as a result of passenger transport services being governed by their own transport-mode specific consumer laws.

Uncertainty exists as to whether a MaaS platform would be considered an "*information society service*", and therefore be subject to various platform regulations, including the Platform to Business Regulation ("**P2B Regulation**") which came into force in July 2020 to address the disparity in negotiating position (and extend consumer law-style protections to businesses that use platforms to offer goods and/or services to consumers). The application of the P2B Regulation to MaaS platforms and any resulting obligations imposed on MaaS platforms will evolve in the coming years.

Local regulations and industry agreements, regulating fares and ticketing, can complicate or even create barriers to the integration of ticketing functions into a MaaS platform. An example of this during the MyCorridor project came in the context of rail ticketing. Following discussions with the provider of an existing EU-wide ticketing platform, with the goal of integrating that platform's services into the MyCorridor platform for the purposes of the Pilots, the provider decided it would be unable to participate in the Pilots because in some countries the local regulation and industry agreements that regulate the creation of rail fares and the issuance of rail tickets made it too difficult to integrate their services in time to join the Pilots.

Overall, it is clear that EU-level intervention is required to facilitate the deployment of MaaS, particularly across borders, to create enabling legislative frameworks, that can help to overcome some of the challenges faced in MaaS.

Annexes

Introduction

Key legal documentation produced by MyCorridor

To support the establishment of the MyCorridor platform and the implementation of the Pilots OC prepared the following key contracts and legal documentation:

Data Protection Documents

- **MyCorridor's privacy policy** – a privacy policy based on the personal data processing activities which the MyCorridor Consortium carried out during the MyCorridor MaaS project, both for the website and the mobile application. OC also advised the MyCorridor technical partners and Pilot leaders in relation to the integration of the privacy policy within the mobile app itself, and how the privacy policy should be presented to individuals participating in Pilots, prior to individuals sharing any personal data with the MyCorridor Consortium .

- **MyCorridor's use of cookies** - OC provided advice in relation to the use of cookies and similar technologies on the website and in the mobile app, and provided template cookie policies for the MyCorridor Consortium's completion and consideration.

Contractual Framework

- **Template external service provider agreement** – a template service provider agreement to be entered into between the relevant MyCorridor Consortium partners and external service providers, which OC also helped negotiate with Karhoo.

- **MyCorridor Platform terms and conditions for external service providers** – terms and conditions for external transport service providers, summarising the key provisions from the template external service provider agreement.

- **MyCorridor platform terms and conditions for Pilot participants** – consumer terms and conditions for participants of the MyCorridor platform trials (the "Pilots").

- **MyCorridor platform terms of use** – terms of use to govern individuals' and service providers' use of the MyCorridor website and app.

Annex I. Data Protection documents

Annex IA. Privacy Policy

Overview – the key information you should be aware of

(A) Who we are

"**MyCorridor**" is a research project funded by the European Commission as part of its Horizon 2020 initiative, researching facilitated, sustainable travel, across European borders, based on the principles of Mobility as a Service (MaaS).

The research partners within the MyCorridor consortium, listed in section 13.1 (the "**MyCorridor Research Partners**"), are conducting research pilots ("**Pilots**") to trial the mobile application developed as part of the MyCorridor research project, with the aim of providing a mobile, one-stop ticket shop, to facilitate cross-border MaaS travel (the "**App**").

The MyCorridor Research Partners promote the MyCorridor research project, and carry out wider research into MaaS with volunteers, through the use of focus groups and other events, which are largely promoted through the MyCorridor website (www.mycorridor.eu) (the "**Website**").

The MyCorridor Research Partners are data controllers of your personal information (together the "**MyCorridor Research Partners**", "**we**", "**us**", "**our**"). This means that the MyCorridor Research Partners are responsible for deciding how your personal information is used for the purposes of MyCorridor's research. The MyCorridor consortium partners listed in section 13.2 are data processors of your personal information processing your personal information in accordance with the MyCorridor Research Partners' instructions, for the purposes of MyCorridor's research, as set out in this privacy policy.

(B) Our values and what this policy is for

We value your privacy and want to be accountable and fair to you as well as transparent with you in the way that we collect and use your personal information. We also want you to know your rights in relation to your information, and you can find details of these here [*insert hyperlink to section 9*].

In line with these values, this privacy policy tells you what to expect when we collect and use personal information about you. We have tried to make it easy for you to navigate this privacy policy so you can find the information that is most relevant to you and our relationship with you.

We are always looking to improve the information we provide to our contacts so if you have any feedback on this privacy policy, please let us know using our contact details in section 14 [*insert hyperlink*].

In this privacy policy, we refer generally to your "**personal information**", which means any data relating to you which identifies you (such as your name) or could indirectly identify you (such as an identification number, or an online identifier).

Please read this privacy policy carefully to understand how we handle your personal information. By engaging with us in the ways set out in this privacy policy, you confirm that you have read and understood the entirety of this privacy policy as it applies to you.

This privacy policy was last updated on [●] November 2019. Please check back regularly to keep informed of updates to this privacy policy.

(C) Who this policy applies to

This policy applies to:

1. People who sign up to receive email updates on the MyCorridor research project (MyCorridor "**Interest Group**" members) *[insert hyperlink]*;
2. Attendees and participants of MyCorridor focus groups, Pilot meetings, and other events organised by the MyCorridor Research Partners *[insert hyperlink]*;
3. Visitors and users of the Website *[insert hyperlink]*;
4. People who contact us with enquiries *[insert hyperlink]*; and
5. People who participate in our Pilots or otherwise use the App *[insert hyperlink]*.

(D) What this policy contains

This privacy policy describes the following important topics relating to your information (you can click on the links to find out more):

1. How we obtain your personal information *[insert hyperlink]*;
2. The personal information we collect about you, how we use it and the lawful bases on which we rely *[insert hyperlink]*;
3. How we share your personal information and who we share it with *[insert hyperlink]*;
4. International transfers *[insert hyperlink]*;
5. Cookies *[insert hyperlink]*;
6. Marketing *[insert hyperlink]*;
7. Security *[insert hyperlink]*;
8. How long we store your personal information for *[insert hyperlink]*;
9. Your rights *[insert hyperlink]*;
10. Children *[insert hyperlink]*;
11. Changes to our privacy policy *[insert hyperlink]*;
12. Third party websites *[insert hyperlink]*;
13. MyCorridor Research Partners *[insert hyperlink]*;
14. Complaints, questions and suggestions *[insert hyperlink]*.

(E) Your rights to object

You have various rights in respect of our use of your personal information in certain circumstances. Two of the fundamental rights to be aware of are that:

1. you may ask us to stop using your personal information for direct-marketing purposes. If you exercise this right, we will stop using your personal information for this purpose.

2. you may ask us to consider any valid objections which you have to our use of your personal information where we process your personal information on the basis of our, or another person's, legitimate interest.

You can find out more information in section 9 *[insert hyperlink]*.

The key information you should be aware of

1. **How we obtain your personal information**

1.1 You may provide us with personal information about yourself voluntarily or we may automatically collect personal information from you, as set out in this privacy policy. We may also receive information about you from third parties such as our service providers, group companies of MyCorridor Research Partners, public websites or public agencies.

1.2 You may provide us with or we may obtain personal information about you if you access the Website sign up to our MyCorridor Interest Group, set up an account with us, use the App, agree to participate in a MyCorridor research focus group or MyCorridor App research Pilot, attend a MyCorridor workshop or other MyCorridor project-related event, complete MyCorridor user surveys or any MyCorridor-related forms, whether online or in hard copy (for example during MyCorridor focus groups and/or other MyCorridor events), contact us by phone, email, or other means. If you are a service provider, you may also provide us with personal information about you when you are offer or provide services to us. We may also receive information about you from third parties.

2. **The personal information we collect about you, how we use it, and the lawful bases on which we rely**

2.1 MyCorridor Interest Group members

If you have signed up to the MyCorridor Interest Group, we, or third parties on our behalf, will collect the following information from you:

(a) your email address;

(b) other information provided when you correspond with us; and

(c) any updates to information provided to us.

How we use your personal information and the legal bases on which we rely

We collect, use and store your email address with your consent for the purposes of providing you with communications relating to the MyCorridor research project. You can withdraw your consent at any time.

To unsubscribe from the MyCorridor Interest Group at any time, you can do so by clicking the 'UNSUBSCRIBE' link at the bottom of any email we send you, or by sending your name and email address to info@iruprojects.org, stating 'UNSUBSCRIBE' in the subject line of the email.

2.2 ***Attendees and participants of MyCorridor focus groups, Pilot meetings, and other events organised by the MyCorridor Research Partners***

If you are attending a MyCorridor focus group, Pilot participant meeting or other event organised by a MyCorridor Research Partner, we will collect all or some of the following personal information from you:

(a) your name;

(b) your email address;

(c) your company's name (where applicable);

(d) other information provided when you correspond with us (this includes information which may be audio transcribed during focus groups and Pilot participant meetings. Further information relating to this will be provided to you during or before the relevant focus group or Pilot participant meeting);

(e) any updates to information provided to us;

(f) your telephone number;

(g) any health-related information, which you may voluntarily provide to us, including (but not limited to) any accessibility/disability issues, such as wheelchair access requirements; any dietary requirements; or visual or hearing impairments;

(h) if you attend our focus groups, Pilot participant meetings, or events, photograph(s) or video-footage in which you feature, (we will provide you with further information relating to this at the relevant focus group or Pilot participant meeting, or event); and

(i) if you attend one of the MyCorridor Research Partners' premises, the relevant MyCorridor Research Partner may record CCTV footage.

2.3 ***How we use your personal information and the legal bases on which we rely***

Our legitimate interests

We will collect, use and store the information listed in section 2.2 above where it is in our legitimate interests, as follows:

(a) your email address so that we can confirm your attendance at the relevant focus group;

(b) your name and email address to request feedback relating to the MyCorridor focus group or event which you attended, to assist in our research and development and to improve and develop MyCorridor, its events and services;

(c) your company's name, to understand the types of people interested in MyCorridor and MyCorridor events;

(d) your email address or other contact information you have provided to us for the purposes of responding to your queries or requests for information in relation to MyCorridor or MyCorridor focus groups and events;

(e) your contact details to provide you with follow-up information relating to the MyCorridor focus group or event which you attended and invite you to other MyCorridor focus groups and events;

(f) photograph(s) or video-footage in which you feature for the purposes of promoting MyCorridor and its research activities, including (without limitation) via online platforms, such as LinkedIn, Twitter and via the MyCorridor website; and

(g) CCTV footage may be recorded if you visit one of the MyCorridor Research Partners' premises, for ensuring the security of their staff and visitors, and their property.

2.4 ***Special categories of personal data***

Some of the personal information that you provide to us may be special categories of data (such as health data). Special categories of data that we might process in connection with the MyCorridor research project, include information relating to your dietary; visual; hearing; accessibility issues; and other health-related requirements. We shall process this personal information:

(a) with your consent, where you voluntarily provide it to us for the purposes of a MyCorridor focus group, Pilot participant meeting, or other related-event, to enable us to cater to your dietary needs, and provide you with any necessary assistance, at such events; and

(b) otherwise, to the extent necessary for scientific research purposes to meet MyCorridor's H2020 research objectives, including to assess how any such requirements influence use of the App, choice of transport mode and other journey choices. Any such information will be pseudonymised and processed only as necessary for the purposes of our scientific research.

If we rely on your consent for us to use your personal information in a particular way, but you later change your mind, you may withdraw your consent by contacting us at info@iruprojects.org and we will stop doing so. However, if you withdraw your consent, this may impact the ability for us to provide certain services to you. For example, if you withdraw your consent to us processing your email address, we will no longer be able to send you information relating to the MyCorridor project.

2.5 ***Visitors and users of the Website***

We, or third parties on our behalf, collect the following information automatically when you visit our Website:

(a) e-mail address (if you register for our newsletter or the MyCorridor Interest Group);

(b) other information provided when you correspond with us;

(c) any updates to information provided to us; and

(d) the following information created and recorded automatically when you visit our Website:

(i) ***technical information***. This includes: the Internet Protocol (IP) address used to connect your computer to the internet address; the website address and country from which you access information; the files requested; browser type and version; browser plug-in types and versions; operating system; and platform. We use this personal information to administer our Website, to measure the efficiency of our systems and to undertake an analysis on the locations from which people access our webpages and frequency with which they do;

(ii) ***information about your visit and your behaviour on our Website***. For example, the pages that you click on. This may include the website you visit before and after visiting our Website (including date and time), time and length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page, and traffic data.

2.6 ***How we use your personal information and the legal bases on which we rely***

We will collect, use and store the information listed in section 2.3 above, where it is in our legitimate interests:

(a) to allow you to access and use our Website;

(b) to understand the content that you are most interested in, so that we can more appropriately tailor the Website to meet your preferences;

(c) to provide technical support;

(d) to ensure the security of our Website;

(e) to provide you with the information that you request from us; and

(f) for improvement and maintenance of our Website. Such details will be anonymised as far as is reasonably possible.

2.7 ***People who contact us with enquiries***

We, or third parties on our behalf, may collect and use any of the following information about you, if necessary to assist with a specific enquiry:

(a) your name including your title;

(b) your postal address;

(c) your email address;

(d) your telephone number;

(e) information provided when you correspond with us; and

(f) any updates to information provided to us.

2.8 ***How we use your personal information and the legal bases on which we rely***

We will collect, use and store the information listed in section 2.4 above, where it is in our legitimate interests to deal with:

(a) any enquiries or issues you have about MyCorridor;

(b) any questions you may have about how we collect, store and use your personal information; or

(c) any requests made by you for a copy of the information we hold about you.

2.9 ***People who participate in our Pilots or otherwise use the App***

We, or third parties on our behalf, may collect and use any of the following information about you:

(a) your name;

(b) your postal address;

(c) your email address;

(d) your telephone number;

(e) age group;

(f) your gender;

(g) nationality;

(h) your credit or bank card detail;

(i) travel and other preferences, which may include information about your home, work, saved locations, preferred transport modes, and other travel preferences;

(j) information provided when you correspond with us, including through the Pilot participant feedback process;

(k) any health-related information, which you may voluntarily provide to us, including (but not limited to) dietary requirements; accessibility issues, such as wheelchair access requirements; or visual or hearing impairments;

(l) any updates to information provided to us;

(m) information you provide to help us provide an improved service, for example if we ask you to fill in a survey or questionnaire;

(n) location data;

(o) booking information, such as journeys completed via the App, including date and time of travel;

(p) device ID;

(q) type of device you use;

(r) device operating system, versions and software;

(s) device preferred languages; and

(t) device time zone settings.

2.10 ***How we use your personal information and the legal bases on which we rely***

Legitimate interests

We will collect, use and store the information listed in the section 2.5 above where it is in our legitimate interests to:

(a) allow you to access and use our App for purposes relating to the Pilots;

(b) ensure the security of our App;

(c) provide you with the information that you request from us;

(d) enable you to make a booking via the App, and to provide you with the services requested by you in accordance with your personalised preferences;

(e) carry out our research, to meet the MyCorridor research objectives, as explained to you at the time you agree to participate in the relevant Pilot;

(f) consider any feedback you provide to us for research purposes, and to optimise the App;

(g) provide you with customer support and to improve our services;

(h) **travel preferences**: if you provide us with information relating to your travel and location preferences, we will process this information, so we can provide a tailored, personalised journey-planning service. This data will also be used in aggregated manner to help us to improve the service offered by MyCorridor; and

(i) **device information**: we collect information about the devices you use to access our App. This includes your device ID, the type of device you use, the hardware model, operating system, versions, software, preferred languages and time zone settings. This information helps us to diagnose and fix any bugs in the App, to ensure that the App can be improved and work at its optimum.

Consent

With your consent, we will use your information for the following purposes:

location data:

(i) if you have selected services via the MyCorridor App from a car, bike, or other mobility service which requires your current location data for the purposes of pick-up and drop-off, we shall collect your location information when the MyCorridor App is running both in the foreground and background of your device using your journey, as necessary to enable the relevant transport provider to provide you with the services you requested, and for on-trip support, and passenger and driver safety.

(ii) to enable us to provide you with the optimal route planning, ticketing and overall mobility as a service, services, we aggregate and analyse journey origin and destination points. If you have manually turned on the location function on your device, we will collect and use your start location information automatically, using GPS, WiFi and mobile phone towers. If you have not enabled your device to provide location information, you will need to manually enter a start and end point, and we will use this information to provide you with the services. If your location function is disabled, you shall not be able to receive the full benefit of the MyCorridor services.

(iii) if your location function is enabled on your device, we will collect location information throughout your journey, to offer ongoing support to you, such as alerting you to when you need to switch transport modes and to provide you with information about your current location, how much of your journey has been covered and how much is left to cover, including providing traffic updates along the way. We will also store and analyse this data in an aggregated manner, to optimise the App and MyCorridor journey results for all users.

You may withdraw your consent to us using your location data, by switching off access to your location. However, if you withdraw your consent in this way, this may impact the ability for us to provide certain services to you. For example, we will no longer be able to provide you with updates along your journey, such as information relating to traffic delays, changes to journey times, route or transport provider, nor will we be able to automatically share pick-up location data with drivers of transport services you have booked.

2.11 ***Special categories of personal data***

Some of the personal information that you may voluntarily provide to us through your use of the App may be special categories of data (such as health data), relating to your dietary; visual; hearing; accessibility requirements; and other health-related requirements. We shall process this personal information to the extent necessary for scientific research purposes to meet MyCorridor's H2020 research objectives, including to assess how any such requirements influence a user's use of the App, choice of transport modes and other journey choices. Any such information will be pseudonymised and processed only as necessary for the purposes of our scientific research.

2.12 ***Other information we collect***

Whatever our relationship with you is, we also collect, use and store personal information for the following additional reasons:

(a) to deal with any enquiries or issues you have about how we collect, store and use your personal information, or any requests made by you for a copy of the information we hold about you. If we do not have a contract with you, we may process your personal information for these purposes where it is in our legitimate interests for customer service purposes;

(b) for internal reporting, administration, and research and development. We may process your personal information for these purposes where it is in our legitimate interests to do so;

(c) to comply with any procedures, laws and regulations which apply to us – this may include where we reasonably consider it is in our legitimate interests or the legitimate interests of others to comply, as well as where we are legally required to do so;

(d) to establish, exercise or defend our legal rights – this may include where we reasonably consider it is in our legitimate interests or the legitimate interests of others, as well as where we are legally required to do so;

(e) if you are a journalist or work for an institution/trade association in our industry, we may collect information about you from public sources. Where it is in our legitimate interests to do so, we will use your contact details to invite you to write news articles about MyCorridor; to invite you to our events; to send you promotional material; and for press releases; and

(f) if you visit one of the MyCorridor Research Partners' premises, the relevant MyCorridor Research Partner may also collect personal information about you on CCTV where it is in their legitimate interests.

If we rely on our (or another person's) legitimate interests for using your personal information, we will undertake a balancing test to ensure that our legitimate interests are not outweighed by your interests or fundamental rights and freedoms which require protection of the personal information. You can ask us for information on this balancing test by using the contact details at section 14 *[insert hyperlink]*.

2.13 ***Further processing***

Before using your personal information for any purposes which fall outside those set out in this section 2, we will undertake an analysis to establish if our new use of your personal information is compatible with the purposes set out in this section 2. Please contact us using the details in section 14 *[insert hyperlink]* if you want further information on the analysis we will undertake.

2.14 ***Profiling***

The purpose of the MyCorridor App is to provide you with tailored travel solutions. Therefore the MyCorridor App is designed to process the personal information you provide to us via the App, and information we collect based on your use of the App, including information relating to your traveller behaviour history of searching and selecting services using the App, to personalise the travel solutions offered to you via the App. You can amend your travel preferences and other personal information you provide to us via the App, in your personalised profile section of the App, at any time.

MyCorridor does not currently use and has no intention of using automated processing or profiling to make automated decisions about you that could significantly impact you. However, should this change in the future, we shall notify you of this in advance

3. **How we share your personal information and who we share it with**

3.1 The personal information that we collect or that you otherwise provide to us with will be shared within the MyCorridor consortium, with the MyCorridor consortium members listed in sections 13.1 and 13.2 of this privacy policy , who will process your personal information for purposes relating to the MyCorridor research project.

3.2 In accordance with the European H2020 guidelines, we have agreed to publish the results of MyCorridor's research by way of open access. Any information that we share for the purposes of research publication, including at international conferences and exhibitions and in peer-reviewed and open-access scientific and academic journals will be anonymised and will not include any personal information. You will not be identifiable from these publications. Anonymised data sets may also be shared with third party data repositories for the purposes of research archiving.

3.3 Unless set out below, we will not disclose, sell or rent your personal information to any third party unless you have consented to this. If you do consent but later change your mind, you may contact us using the contact details in section 14 *[insert hyperlink]* and we will cease any such activity.

3.4 We disclose information to third parties under the following circumstances:

(a) with companies that assist us with delivering the MyCorridor Interest Group and corresponding communications, with our marketing, advertising and promotional activities. This includes Mailchimp, who assists us in providing you with the MyCorridor Interest Group;

(b) other third-party service providers: when we share anonymous information with them, to facilitate or to provide the Website, App, and Interest Group on our behalf. This will include:

(i) IT infrastructure companies that facilitate our provision of the Website and App to you, including suppliers of technical and support services, insurers, logistic providers, and cloud service providers;

(ii) analytics and search engine providers that assist us in the improvement and optimisation of our Website and App. For example, Firebase Crashlytics;

(c) If you are using the App as a Pilot participant for real-life travel, we share the following information (as necessary) with transport-related service providers, delivering transport services to you: first and last name, phone number, route information, current location, and pick-up and drop-off location;

(d) upon their request, with the European Commission, and the Innovation and Networks Executive Agency (acting on powers of the European Commission), as funders of MyCorridor research project, as necessary for the purposes of demonstrating the progress and outcomes of the MyCorridor research in accordance with MyCorridor's H2020 objectives. Where possible, information shared with the European Commission and the Innovation and Networks Executive Agency will be anonymised.

3.5 Any third parties with whom we share your personal information are limited (by law and by contract) in their ability to use your personal information for any purpose other than to provide services for us, or in the case of the European Commission and Networks Executive Agency, as part of their overall funding of MyCorridor. We will always ensure that any third parties with whom we share your personal information are subject to privacy and security obligations consistent with this privacy policy and applicable laws.

3.6 We will also disclose your personal information to third parties if:

(a) we are under a duty to do so in order to comply with any legal obligation, any lawful request from government or law enforcement officials and as may be required to meet national security or law enforcement requirements or prevent illegal activity;

(b) in order to enforce or apply our terms of use, our terms and conditions for users of the App, or any other agreement, or to respond to any claims, to protect our rights or the rights of a third party, to protect the safety of any person; and

(c) to protect the rights, property or safety of the MyCorridor Research Partners, our staff, our users, or other persons. This may include exchanging personal information with other organisations for the purposes of fraud protection.

3.7 We may also disclose and use anonymised, aggregated reporting and statistics about users of our Website or our App and services, for the purpose of internal reporting or reporting to other third parties, and for our marketing and promotion purposes. None of these anonymised, aggregated reports or statistics will enable our users to be personally identified.

4. **International transfers**

4.1 We do not transfer personal information we received about you outside the European Economic Area.

4.2 If it becomes necessary for us to start transferring your personal information outside the EEA we shall notify you of this in advance, and we shall take appropriate measures to ensure that the non-EEA recipient protects your personal information adequately in accordance with this privacy policy. These measures may include, entering into European Commission approved standard contractual arrangements with the recipient, or as otherwise permitted under Articles 45 and 46 of the General Data Protection Regulation.

5. **Marketing**

5.1 We will collect and use your personal information for undertaking marketing by email in accordance with this privacy policy.

5.2 We may send you certain electronic marketing communications to you if you are attended a MyCorridor event, or focus group, if you are a Pilot participant, have signed up to the MyCorridor Interest Group, and if it is in our legitimate interests to do so for marketing and research purposes.

5.3 We will always obtain your consent to direct marketing communications where we are required to do so by law and if we intend to disclose your personal information to any third party for such marketing.

5.4 If you wish to stop receiving marketing communications, you can contact us by email at info@iruprojects.org, stating ‘UNSUBSCRIBE’ in the subject line of the email, or you can click the ‘UNSUBSCRIBE’ link at the bottom of any email we send you.

6. **Cookies**

6.1 Some pages on our Website, and our App, use cookies and similar technologies to provide, support and improve MyCorridor's services. We use cookies in order to offer you a more tailored experience in the future, by understanding and remembering your particular browsing preferences, and so we can continue to produce appropriately tailored content and services. Cookies also enable us to provide you with an optimised and continued experience.

6.2 You may block these cookies at any time. To do so, you can activate the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies), you may not be able to access all or parts of our Website or to use all the functionality provided through our Website.

6.3 For detailed information on the cookies we use and the purposes for which we use them, please refer to our cookies policy here http://mycorridor.eu/cookies-policy/.

7. **Security**

7.1 We are committed to protecting personal information from loss, misuse, disclosure, alteration, unauthorised access, unavailability and destruction and takes all reasonable precautions to safeguard the confidentiality of personal information, including through use of appropriate organisational and technical measures.

7.2 Whilst we take appropriate technical and organisational measures to safeguard the personal information that you provide to us, no transmission over the Internet can ever be guaranteed secure. Consequently, please note that we cannot guarantee the security of any personal information that you transfer over the Internet to us.

8. **How long we store your personal information for**

We keep your personal information for no longer than necessary for the purposes for which the personal information is processed. The length of time for which we retain personal information depends on the purposes for which we collect and use it and/or as required to comply with applicable laws and to establish, exercise or defend our legal rights.

9. **Your rights**

9.1 You may have certain rights set out below in relation to some of the personal information we collect about you. If you would like further information in relation to these or would like to exercise any of them, please contact us via email at info@iruprojects.org at any time.

(a) **Right of access**. You may have a right of access to any personal information we hold about you. You can ask us for a copy of your personal information; confirmation as to whether your personal information is being used by us; and details about how and why it is being used.

(b) **Right to update your information**. You may have a right to request an update to any of your personal information which is out of date or incorrect.

(c) **Right to delete your information**. You may have a right to ask us to delete any personal information which we are holding about you in certain specific circumstances. You can ask us for further information on these specific circumstances by contacting us using the details in section 14 *[insert hyperlink]*.

We will pass your request onto other recipients of your personal information unless that is impossible or involves disproportionate effort. You can ask us who the recipients are, using the contact details in section 14 *[insert hyperlink]*.

(d) **Right to restrict use of your information**: You may have a right to ask us to restrict the way that we process your personal information in certain specific circumstances. You can ask us for further information on these specific circumstances by contacting us using the details in section 14 *[insert hyperlink]*.

We will pass your request onto other recipients of your personal information unless that is impossible or involves disproportionate effort. You can ask us who the recipients are using the contact details in section 14 *[insert hyperlink]*.

(e) **Right to stop marketing**: You may have a right to ask us to stop using your personal information for direct marketing purposes. If you exercise this right, we will stop using your personal information for this purpose.

(f) **Right to data portability**: You may have a right to ask us to provide your personal information to a third party provider of services.

This right only applies where we use your personal information on the basis of your consent or performance of a contract; and where our use of your information is carried out by automated means.

(g) **Right to object**. You may have a right to ask us to consider any valid objections which you have to our use of your personal information where we process your personal information on the basis of our or another person's legitimate interest.

9.2 We will consider all such requests and provide our response within a reasonable period (and, where required by applicable law, within one month of your request, unless we tell you we are entitled to a longer period under applicable law). Please note, certain personal information may be exempt from such requests in certain circumstances. For example, where it is necessary to process that personal information for research purposes, if we need to keep using the information to comply with our own legal obligations, or to establish, exercise or defend legal claims.

9.3 If an exception applies, we will tell you this when responding to your request. We may request you provide us with information necessary to confirm your identity before responding to any request you make.

10. Children

We do not and will not knowingly collect information from any unsupervised child under the age of 18. Our Website, focus groups and events are not designed for under 18s.

If you are a child and we learn that we have inadvertently obtained personal information from you from our Website, our App, or via any other source, then we will delete that information as soon as possible.

Please contact us at info@iruprojects.org if you are aware that we may have inadvertently collected personal information from a child.

11. Third party websites

Our Website or App may, from time to time, contain links to websites operated by third parties including social media websites, partner networks and our group companies. Please note that this privacy policy only applies to the personal information that we collect through our Website and App, and as otherwise stated in this privacy policy, and we cannot be responsible for personal information collected and stored by third parties. Third party websites have their own terms and conditions and privacy policies, and you should read these carefully before you submit any personal information to these websites. We do not endorse or otherwise accept any responsibility or liability for the content of such third party websites or third party terms and conditions or policies.

12. Changes to our privacy policy

We will update our privacy policy from time to time. Any changes we make to our privacy policy in the future will be posted on our Website and App, and, where appropriate, notified to you by post or email. Please check back frequently to see any updates or changes to our privacy policy.

13. MyCorridor Research Partners

13.1 MyCorridor joint data controllers of your personal information:

The entities listed below together form the MyCorridor Research Partners who are the controllers responsible for your personal information collected in accordance with this privacy policy (the **"MyCorridor Research Partners"**).

CERTH (Centre for Research & Technology Hellas) https://www.certh.gr/

CERTH Hellenic Institute of Transport

CERTH Informatics and Telematics Institute

AMCO Oloklиromena Systimata Ypsilis Technologias Anonymi Viomichaniki Kai Emporiki Etairia http://www.amco.gr/el/

TTS Italia Associazione https://www.ttsitalia.it/

IRU Projects https://www.iru.org/innovation/iru-projects

Viva Payments Services S.A https://www.vivawallet.com/en-eu/

Viva Wallet Holdings - Software Development S.A,

13.2 MyCorridor consortium entities acting as data processors of your personal information:

The entities listed below are the MyCorridor consortium partners, who will have access to and process your personal information for purposes relating to the MyCorridor research project, in accordance with our instructions.

Chaps spol sro https://www.chaps.cz/

HaCon Ingenieurgesellschaft MBH http://www.hacon.de/

MAP Traffic Management B.V. https://www.maptm.nl/

Roma Mobilita Servizi Per La Mobilita SRL https://romamobilita.it/it

Salzburg Research Forschungsgesellschaft M.B.H https://www.salzburgresearch.at/

Swarco Hellas A.E. http://www.swarco.gr/?lang=en

Swarco Mizar https://www.swarco.com/mizar

TomTom Location Technology Germany GMBH https://www.tomtom.com/en_gb/

Wings ICT Solutions Information & Communication Technologies Epe https://www.wings-ict-solutions.eu/

14. **Complaints, questions and suggestions**

14.1 If you have any queries, complaints or suggestions about our collection, use or storage of your personal information, or if you wish to exercise any of your rights in relation to your personal information, please contact us using the appropriate email address below. We will investigate and attempt to resolve any complaint or dispute regarding the use or disclosure of your personal information, and will respond to your queries.

MyCorridor Interest Group, Website, focus groups and events

Please contact info@iruprojects.org

MyCorridor Pilots

Please contact [insert appropriate email address]

For all other complaints, questions and suggestions

Please contact info@iruprojects.org in the first instance, and, where necessary, you shall be redirected to the appropriate MyCorridor contact.

14.2 In accordance with Article 77 of the General Data Protection Regulation, you may also make a complaint to the Information Commissioner's Office, or the data protection regulator in the country where you usually live or work, or where an alleged infringement of the General Data Protection Regulation has taken place. Alternatively, you may seek a remedy through the courts if you believe your rights have been breached.

14.3 The practices described in this privacy policy statement are current as of [insert date].

Annex IB. Cookie Policy [Template for MyCorridor to complete]

Who we are

"**MyCorridor**" is a research project funded by the European Commission as part of its Horizon 2020 initiative, researching facilitated, sustainable travel, across European borders, based on the principles of Mobility as a Service (MaaS).

Our Privacy Policy [*please insert link*] explains how we collect and use information we collect about you when you visit our website at www.mycorridor.eu ("Website") or our mobile application ("App"), create an account with us, or otherwise interact with us.

This Cookie Policy explains how we use cookies and similar technologies in the Website and our App and your choices concerning them.

Updated [*Insert Date*]

Our Website and App use cookies and other similar tracking technologies, such as [pixels, plugins, scripts, tags and device fingerprinting] (which we collectively refer to as "cookies" in this Cookie Policy).

We use cookies for many reasons, for example to distinguish you from other users. This helps us to provide you with a good experience when you use our Website and App and also allows us to improve our Website and App.

This Cookie Policy describes:

- What are cookies;
- Our use of cookies;
- How you can manage cookies used in our Website;
- Further information; and
- Changes to this Cookie Policy.

What are cookies?

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer, smart phone, tablet or other electronic device if you agree. Cookies contain information that is transferred to your device's hard drive and some cookies may collect personal data about you. You can find more general information about cookies at: www.aboutcookies.org or www.allaboutcookies.org.

Our use of cookies

We want you to understand the different types of cookies that we use. We use a variety of types of cookies for the following purposes:

- **Strictly necessary (essential) cookies:** these are cookies strictly necessary for the operation and performance of our Website, for example cookies that enable you to access your account and various account information such as trip history and make bookings.

- **Performance cookies:** these cookies allow us to recognise and count the number of visitors and to see how visitors move around our Website when they are using it. This helps us to improve the way our Website works, for example, by ensuring that users are finding what they are looking for easily.

- **Functionality cookies:** these cookies are used to recognise you when you return to our Website. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region).

You can find more information about the individual cookies we use and the purposes for which we use them in the table below:

Cookie Title **Cookie Name**	**Purpose**	**Duration***	**More information**
[OC Example] Universal Analytics (Google) _ga _gali _gat _gid	*[OC Example]* These cookies are used to collect information about how visitors use our Website. We use the information to compile reports and to help us improve our Website. The cookies collect information in an anonymous form, including the number of visitors to our Website.	*[OC Example]* 1 year	*[OC Example]* Read Google's overview of privacy and safeguarding data
[Please complete this table with the other cookies (or similar technologies used here)]			

**Duration means the period that our cookies are installed on your device. At the expiry of this period, you will be asked to agree to the cookies again.*

Except for strictly necessary cookies (which have a longer expiration date and, in some cases do not expire), all cookies will expire [*when you close your internet browser at the end of your session*]OR[*insert expiry period*].

How you can manage cookies used in our Website?

If you disable cookies, you may find that you have a less personalised experience when using our Website and that certain parts of our Website do not work at all or do not work correctly.

Cookies do lots of jobs on our website. However, most browsers allow you to disable them if you would like to. To find out more about cookies, including how to see what cookies have been set, visit www.aboutcookies.org or www.allaboutcookies.org.

Each browser is configured differently. To disable cookies via your browser settings, you should follow the instructions given by the publisher of your browser. As of the date of this Cookie Policy, these instructions are available for commonly used browsers through the following links:

Find out how to manage cookies on popular browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Microsoft Internet Explorer
- Opera
- Apple Safari

To find information relating to other browsers, visit the browser developer's website.

If you use different devices, make sure you configure the settings of the corresponding browser according to your preferences.

If you wish to opt-out of tracking by Google Analytics across all websites you can do so here: https://tools.google.com/dlpage/gaoptout.

Further information

If you have any queries relating to this Cookie Policy please [*insert contact methods/details*].

Changes to this Cookie Policy

If this Cookie Policy changes, the revised policy will include a new effective date and will be posted on this page. Please check back regularly to keep informed of updates.

Annex II. Contractual Matrix

Annex IIA. Template external service provider agreement

MyCorridor Collaboration Agreement

(1) [Insert Service Provider]

(2) The 10 entities listed in Schedule 5 to this Agreement (the "MyCorridor Technical Partners")

Dated [●]

Osborne Clarke LLP
One London Wall
London
EC2Y 5EB

Telephone +44 20 7105 7000

1069724/40424684.1/JDS

This Agreement is made on [DATE]

BETWEEN

(1) The 10 entities listed in Schedule 5 (the **"MyCorridor Technical Partners"**);

(2) [SERVICE PROVIDER'S FULL COMPANY NAME] incorporated and registered in [COUNTRY OF INCORPORATION] with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] (the **"Service Provider"**).

(each a **"party"** and together the **"parties"**).

Background

(A) The MyCorridor Technical Partners are members of the research consortium, the "MyCorridor Consortium" (defined below). The MyCorridor Consortium has received funding from the Project Funder (defined below) as a European Union H2020 research project (the "**MyCorridor Project**", as further defined below), and is governed by the Grant Agreement (as further defined below).

(B) The MyCorridor Project started on 1 June 2017 and will conclude on 31 May 2020. The Service Provider and the MyCorridor Technical Partners wish to collaborate to meet the MyCorridor Project objectives set out in Schedule 1 and Annex 2 to this Agreement.

(C) The parties have agreed to enter into this Agreement to set out their respective obligations to each other for the purposes of their collaboration relating to the MyCorridor Project.

(D) The MyCorridor Technical Partners have appointed [●] (the "MyCorridor Representative") as agent to sign this Agreement on their behalf. The MyCorridor Representative is also a member of the MyCorridor Consortium.

Agreed terms

1. **Interpretation**

The following definitions and rules of interpretation apply in this Agreement.

1.1 ***Definitions***

"Agreement" means this agreement (including any schedule or annexure to it).

"API" means the Service Provider's application programming interface used for the Service Provider's integration with the MyCorridor Platform.

"Background Intellectual Property" means any Intellectual Property Rights, other than Foreground Intellectual Property Rights, used in connection with this Agreement, the MyCorridor Project or the provision of the Services.

"Booking" means a booking for a Journey, selected and completed by a Traveller via the MyCorridor Platform and accepted or deemed to be accepted by [the Service Provider] via the Service Provider Platform.

"Business Day" means a day other than a Saturday, Sunday or a public holiday in the country where the relevant party is based.

"Confidential Information" means all information which is disclosed by one party to the other whether before or after the Effective Date, which is designated in writing as confidential or would appear to a

reasonable person to be confidential and which relates to a party's business (and in the case of the MyCorridor Technical Partners, shall include information which relates to the MyCorridor Consortium and the MyCorridor Project) including (without limitation) its research, results of work and research, products, operations, processes, plans or intentions, developments, trade secrets, know how, market opportunities, marketing, personnel, suppliers, financial information, Personal Data (as defined in Annex 1 (Data Protection)), ideas and concepts that a party presents, pitches or suggests to the other party during the Term, Intellectual Property, and all information derived from any of the above.

"Dispute" means any dispute, claim, difference or question of interpretation (whether contractual or non-contractual) arising out of or in connection with this Agreement, its subject matter or formation.

"Dispute Resolution Procedure" means the procedure for resolving disputes set out in clause 19 (Dispute Resolution)

"Effective Date" means the date of the last signature to this Agreement.

[**"Fare"** means the means the fixed price for a Booking calculated prior to the Journey according to the Service Provider's pricing structure, together with any VAT properly charged thereon].

"Foreground Intellectual Property" means any Intellectual Property Rights that arise or are obtained or developed by, or by a contract on behalf of, a party in the course of or in connection with this Agreement.

"Good Industry Practice" means the exercise of the highest degree of skill, care, prudence, efficiency, diligence, foresight and timeliness which would reasonably be expected from a well-managed service provider highly skilled and experienced in providing services similar to the Services.

"Grant Agreement" means the confidential agreement which the MyCorridor Technical Partners have entered into with the other members of the MyCorridor Consortium and the Project Funder, setting out the terms and conditions upon which the Project Funder is providing the Project Funding to the members of the MyCorridor Consortium for the purposes of the MyCorridor Project.

"Insolvency Event" means any one of the following:

(a) a party passes a resolution for its winding-up or a court of competent jurisdiction makes an order for the winding-up or the dissolution of that party;

(b) any steps are taken for the making of an administration order or the appointment of an administrator under the out-of-court procedure under the Enterprise Act 2002 or notice is given of an intention to appoint an administrator in relation to a party or any steps are taken for the appointment of a receiver or administrative receiver, or an encumbrancer takes possession of or sells any of a party's assets;

(c) a party makes an arrangement or composition with its creditors generally or makes an application to a court of competent jurisdiction for protection from its creditors generally;

(d) a party ceases to do business at any time for 30 consecutive days; or

(e) a party is unable to pay its debts (within the meaning of that term under section 123, Insolvency Act 1986).

"Intellectual Property" or **"Intellectual Property Rights"** means, without limitation, patents, utility models, rights to inventions, copyright and related rights, moral rights, trade marks and service marks, business names and domain names, rights in get-up, goodwill and the right to sue for passing off or unfair competition, rights in designs, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets), semiconductor topography rights, image rights, rights of personality and other similar rights, and all other intellectual property rights, in

each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

"ITS" means Intelligent Transport Systems.

"Journey" means the Service Provider's provision of transportation services to a Traveller in response to a Booking which enables the Traveller to travel from one agreed location to another agreed location at a specific time in accordance with the criteria set out in the relevant Booking.

"Lead Contact" means the individuals representing each party as identified in Schedule 5 as may be amended from time to time by written notice from the amending party to the other.

"MaaS" means Mobility as a Service.

"Mobility Products" means real-life, physical transportation service or transportation management products provided by private, public or part-public-part-private transport companies or authorities, which are sold (or provided free-of-charge during Pilots) to Participants via the One-Stop-Shop on the MyCorridor Platform.

"Mobility Tokens" means the e-money vouchers that the MyCorridor Consortium will provide to Participants as tickets for travel.

"MyCorridor Consortium" means the research consortium, which has received Project Funding from the Project Funder for the purposes of the MyCorridor Project and includes (among others) the MyCorridor Technical Partners and the MyCorridor Representative.

"MyCorridor Consortium Members" means those members of the MyCorridor Consortium listed in Schedule 6, which includes the MyCorridor Representative. Each a **"MyCorridor Consortium Member".**

"MyCorridor Platform" means the (mobile application) platform owned, developed and provided by the MyCorridor Technical Partners, as a technical base for the MyCorridor One-Stop-Shop, supported by ITS through which service providers shall make available their respective Services to Travellers and through which Travellers can access the One-Stop-Shop in accordance with the objectives of the MyCorridor Project.

"MyCorridor Project" means the project as detailed in Schedule 1 for which the MyCorridor Consortium has received Project Funding from the Project Funder under the Grant Agreement.

"MyCorridor Technical Partners" means those members of the MyCorridor Consortium listed in Schedule 5, who are responsible for and/or assist with the technical development and running of the MyCorridor Platform. Each a "MyCorridor Technical Partner".

"MyCorridor Services" means the connectivity services provided to the Service Provider by the MyCorridor Consortium to enable the Service Provider to connect to the MyCorridor Platform.

"One-Stop-Shop" means the one-stop-shop developed and owned by the MyCorridor Consortium to allow configuration, purchase and redemption (with only one ticket) of MaaS packages that consist of Mobility Products offered with the support of infomobility and other added-value services, whether paid for or not.

"Participants" means individuals who have voluntarily agreed to take part in the Pilots.

"Phase 1" means the first phase of the Pilots, to be performed in a controlled environment at each of the MyCorridor Pilot Sites, testing, primarily, for any functionality and usability issues in the MyCorridor

Platform. No actual booking or purchasing of tickets for real-life travel will take place. The output of this Phase 1 will assist with the optimisation of the MyCorridor Platform and will feed into Phase 2.

"Phase 2" means the real-life testing of the MyCorridor Platform and One-Stop-Shop, to be carried out both locally at MyCorridor Pilot Sites, and in a cross-border context. Phase 2 will include all aspects of the booking and travel process, from pre-trip planning, booking, payment and ticketing to real-life travel, supported by the MyCorridor Platform and the Mobility Tokens redemption process.

"Pilots" means the testing at each Pilot Site, of the MyCorridor Platform and the One-Stop-Shop in two separate phases, Phase 1 and Phase 2, at each Pilot Site. Each a "Pilot".

"Pilot Site" means the geographical site carrying out a Pilot and "Pilot Sites" shall be construed accordingly.

"Project Funder" means the Innovation and Networks Executive Agency (INEA) under the powers delegated by the European Commission

"Project Funding" means monies received from the Project Funder for the MyCorridor Project in accordance with the Grant Agreement. ["Service Provider Platform" means the proprietary software systems developed by the Service Provider, which shall be integrated into the MyCorridor Platform, allowing the MyCorridor Technical Partners and the Service Provider to connect and transact.]

"Service Registration Tool" means the service registration tool developed and owned by the MyCorridor Consortium, through which other service providers shall register their services with the MyCorridor Platform.

"Services" means the technology services detailed in Schedule 2 to be performed by the Service Provider in accordance with clause 5.1 (Service Provider Obligations) via the Service Provider Platform.

"Term" means the term of this Agreement as specified in clause 14.

"Traveller" means any individual who has made a Booking for a Journey, via the MyCorridor Platform, whether for business, leisure or for any other reason, and includes Participants. "Travellers" shall be construed accordingly.

1.2 Clause and Schedule headings shall not affect the interpretation of this Agreement.

1.3 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.4 A reference to a party is to a party to this Agreement.

1.5 A person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality).

1.6 References to clauses and Schedules are to the clauses and Schedules of this Agreement and references to paragraphs are to paragraphs of the relevant Schedule.

2. Scope and purpose

2.1 This Agreement governs the relationship between the parties and sets out each party's respective obligations in relation to their collaboration for the purposes of the MyCorridor Project.

2.2 The Service Provider understands and acknowledges that the Project Funding provided to the MyCorridor Consortium under the Grant Agreement is to be used for the purposes of the MyCorridor Project in accordance with the terms of the Grant Agreement.

2.3 In consideration of the mutual obligations of the parties under this Agreement, the parties have agreed to work collaboratively to further the MyCorridor Project's objectives set out in Schedule 1 and Annex 2, in accordance with this Agreement.

2.4 Each party agrees that any further collaboration following termination of this Agreement, whether connected to the MyCorridor Project or not, shall be managed and governed by a separate agreement to be negotiated and agreed between the parties at the relevant time.

3. **The collaboration**

3.1 Schedule 1 contains a summary of the MyCorridor Project and its objectives relevant to this Agreement and Annex 2 provides more detailed information. The Service Provider's provision of the Services under this Agreement shall assist the MyCorridor Technical Partners in meeting these objectives, as agreed between the parties and as may be amended from time to time by written agreement between the parties.

3.2 Each party shall be responsible for its own costs incurred in connection with this Agreement and the performance of their respective obligations under it.

4. **Mutual roles and responsibilities**

4.1 The parties shall:

(a) proactively work with each other party in relation to the MyCorridor Project;

(b) identify and agree any Background Intellectual Property used, or to be used, and any Foreground Intellectual Property created, or to be created, for purposes connected to this Agreement and the owner of the same, prior to or as soon as reasonably practicable following its disclosure or creation during the Term;

(c) perform their respective obligations under this Agreement in accordance with all applicable laws so as not to place the other party in breach of any applicable laws; and

(d) notify the other party immediately in writing if:

(i) any act or omission on their part may jeopardise or has jeopardised the proper and timely performance of their obligations under this Agreement (including, but not limited to, anything that is likely to significantly delay, threaten or make unlikely the successful completion of any Pilot or any objective of the MyCorridor Project); or

(ii) any legal claims are made or threatened which would adversely affect the MyCorridor Project.

5. **Service Provider obligations**

5.1 The Service Provider agrees to perform the Services (and such other related work as may be reasonably requested by the MyCorridor Technical Partners from time to time) and provide all equipment required to perform the Services, with all due skill and care and in accordance with Good Industry Practice. The parties agree that the Services may be amended by mutual written agreement between the parties at any time.

5.2 [The Service Provider shall register its Services through the Service Registration Tool following acceptance of the Platform Terms. Where the parties agree that the Service Registration Tool is unsuccessful, the parties may agree an alternative back-end registration process for the Service Provider.] OR

[The Service Provider shall provide the Services by integrating the Service Provider Platform into the MyCorridor Platform. Where, prior to any Journeys being offered to Travellers, the MyCorridor Technical Partners consider that the integration of the Service Provider Platform has not been successful to the extent that the Services cannot be performed as set out in this Agreement, the parties shall, acting in good faith, work together to find and agree an alternative method of providing the Services.]

5.3 The Service Provider understands and agrees that a key objective of MyCorridor Project and a key purpose of this Agreement, is for the MyCorridor Consortium to obtain feedback from the Service Provider and Participants to further the MyCorridor Project and to meet the MyCorridor Project objectives, as detailed in Schedule 1 and Annex 2. The Service Provider agrees to:

(a) provide the MyCorridor Technical Partners with feedback, as reasonably requested by the MyCorridor Technical Partners relating to, for example, the Service Provider's integration of, and Participant's experience of, the Services and the Service Provider's experience with the Service Registration Tool more generally; and

(b) the MyCorridor Technical Partners requesting and collecting feedback from Participants during Phase 1 and Phase 2 of the Pilots, connected to each Participant's user experience of the One-Stop-Shop and the MyCorridor Platform, which may include specific feedback relating to the Service Provider's Services, such as ease of use and Quality of Service (**"QoS"**), as well as MaaS more generally,

for use by the MyCorridor Consortium Members to assist the MyCorridor Consortium in optimising the One-Stop-Shop and the MyCorridor Platform and for other research purposes relating to the MyCorridor Project.

5.4 The Service Provider shall share the information contained in Schedule 2 (to the extent available) with the MyCorridor Technical Partners for each Service it provides. The MyCorridor Technical Partners may update or amend the information to be provided under this clause 5.4 or Schedule 2 at any time by providing advanced written notice to the Service Provider, setting out the information to be shared.

5.5 Service Provider agrees to provide the MyCorridor Technical Partners with access to its own API, as necessary, for the purposes of integrating its Services into the MyCorridor Platform.

5.6 The Service Provider acknowledges and agrees that a key objective of this Agreement is to test and evaluate the MyCorridor Platform and Service Registration Tool. The MyCorridor Technical Partners provide no assurance, guarantee or warranty that the integration of the Services or the MyCorridor Platform will be without fault or interruption and accept no liability in relation to the same. The Service Provider shall inform the Lead Contact as soon as it becomes aware of any faults in the MyCorridor Platform or any service problems in connection with the MyCorridor Platform.

5.7 The Service Provider shall notify the Lead Contact immediately of any problems in the Service Provider providing the Services in accordance with this Agreement.

5.8 The Service Provider understands and agrees that it shall not receive any compensation, whether financial or otherwise, under this Agreement and that MyCorridor may offer various incentives, which may include financial incentives, to Participants.

5.9 The MyCorridor Technical Partners do not accept any responsibility or liability for, and the Service Provider shall be fully and solely liable for, any losses which arise directly or indirectly from or in connection with a technical fault or technical malfunction of the Service Provider Platform.

5.10 The Service Provider agrees to attend progress meetings with the MyCorridor Representative throughout the Term of this Agreement and, where reasonably requested by the MyCorridor Representative, MyCorridor Consortium organised events, relating to the Service Provider's provision of Services.

6. **MyCorridor Representative Obligations**

6.1 [The MyCorridor Technical Partners shall use reasonable efforts to ensure that the Service Registration Tool is accessible to the Service Provider to enable the Service Provider to register its Services.]

OR

[The MyCorridor Technical Partners shall use reasonable efforts to assist the Service Provider in integrating its Services (including the Platform) into the MyCorridor Platform, to enable the Service Provider to provide the Services as set out in this Agreement.]

6.2 If the Service Provider reasonably requests, a MyCorridor Technical Partner shall provide reasonable information and guidance to assist the Service Provider with the integration of its Services into the MyCorridor Platform.

6.3 The MyCorridor Technical Partners shall provide the MyCorridor Services to the Service Provider in return for which the Service Provider shall provide the Services to the MyCorridor Technical Partners for the benefit of the MyCorridor Consortium.

6.4 Following integration of the Service Provider Platform into the MyCorridor Platform, the MyCorridor Technical Partners shall use reasonable endeavours to offer the [Service Provider transportation services] to Participants via the MyCorridor Platform, but Participants shall be under no obligation to make any Booking for any Service Provider transport services, and no MyCorridor Technical Partner guarantees that any such Bookings shall be made.

6.5 The MyCorridor Technical Partners shall be responsible for maintaining the MyCorridor Platform and shall use reasonable efforts to provide the necessary updates and upgrades to the MyCorridor Platform. The MyCorridor Technical Partners may suspend or terminate the MyCorridor Platform (or the Service Provider's access to it), without notice or liability to the Service Provider, at any time, if the MyCorridor Technical Partners consider that this is necessary (for example, for improvements, maintenance or upgrades), but the MyCorridor Technical Partners shall use reasonable endeavours to provide reasonable advance notice to the Service Provider of any suspension or termination of the MyCorridor Platform.

6.6 Subject to the Service Provider's compliance with its obligation under clause 5.6, the MyCorridor Technical Partners shall use reasonable efforts to ensure that any disruption to the MyCorridor Platform is kept to a reasonable minimum throughout the Term.

7. **Payment**

7.1 Where a Traveller makes a Booking via the MyCorridor Platform, payment shall be automatically transferred to the Service Provider via the integration of the Service Provider Platform into the MyCorridor Platform, upon payment by the Traveller.

7.2 The parties agree that there is no fee payable by the MyCorridor Technical Partners for the Services. The mechanism under which the Service Provider will collect any Fares and due for each Journey under this Agreement is the following:

[*insert payment mechanism*]

7.3 The Service Provider acknowledges that the MyCorridor Technical Partners may, at their discretion, offer financial incentives to Participants to encourage them to participate in a Pilot. Any such financial incentives shall not affect any payments owed to the Service Provider in accordance with section 8.

8. **Intellectual Property**

8.1 The MyCorridor Consortium owns all rights and interests in the MyCorridor Platform and the Service Registration Tool. The Service Provider owns all rights and interests in the Service Provider Platform.

8.2 Each party (or, where applicable, the third party from whom that party's right to use the Background Intellectual Property has derived) shall retain all rights and ownership to its Background Intellectual Property.

8.3 Each party shall own all Foreground Intellectual Property that it independently creates under or in connection with this Agreement.

8.4 Notwithstanding clause 8.3, the Service Provider agrees that the MyCorridor Consortium shall have all rights of publication, development, promotion, marketing, manufacture, distribution, exploitation and dealing in relation to the results of the parties' collaboration and the MyCorridor Project and the Intellectual Property created by, or arising from, these results.

8.5 The MyCorridor Technical Partners grant the Service Provider a royalty-free, non-exclusive, Europe-wide, revocable, non-sub-licensable, non-transferrable and non-assignable licence for the duration of the Term to use the MyCorridor Platform and the Service Registration Tool, as necessary for the Service Provider's performance of its obligations under this Agreement.

8.6 The Service Provider grants the MyCorridor Consortium a royalty-free, non-exclusive, Europe-wide, revocable, non-sub-licensable, non-transferable, and non-assignable licence for the duration of the Term to use the Service Provider Platform and API, as necessary for the purposes of this Agreement.

8.7 Clauses 8.1-8.4 (inclusive) shall survive termination of this Agreement.

9. **Intellectual Property claims**

9.1 The Service Provider shall immediately notify the Lead Contact, and the Lead Contact (or any of the MyCorridor Technical Partners) shall immediately notify the Service Provider, in writing if it receives any challenge, complaint, claim, demand, action or other communication relating to any infringement or alleged infringement of any third party's Intellectual Property Rights (**"IPR Claim"**).

9.2 In the event of an IPR Claim relating to the Background and Foreground Intellectual Property of a party (the **"IPR Owner"**), the party receiving the IPR Claim shall shall: (i) notify the IPR Owner in accordance with clause 10.1; (ii) not make any admission, compromise or settle the IPR Claim without the prior written consent of the IPR Owner; (iii) allow the IPR Owner, in its absolute discretion, to decide what action, if any, to take and to control and conduct the IPR Claim; (iv) provide the IPR Owner with all assistance as it may reasonably require in the conduct of the IPR Claim.

9.3 In the event of an IPR Claim, the IPR Owner shall: (i) decide what action, if any, to take and to control and conduct the Claim; (ii) keep the other party reasonably informed of the conduct and development of the IPR Claim; and at its own expense and option either:

(a) procure the right for the other party to continue using MyCorridor Platform or Service Provider Platform (as applicable) and the infringing part; or

(b) make such alterations, modifications or adjustments to the MyCorridor Platform or Platform (as applicable) or that infringing part so that it becomes non-infringing without incurring a material diminution in performance, capacity or functionality; or

(c) replace the MyCorridor Platform or Service Provider Platform (as applicable) or that infringing part with non-infringing substitutes provided that such substitutes do not entail a material diminution in performance, capacity or functionality of the MyCorridor Platform or Service

Provider Platform (as applicable) reimbursing the other party for their reasonable costs associated with such substitution.

9.4 Any IPR Claim resulting from a party's Background or Foreground Intellectual Property shall be deemed to be a material breach of a condition of this Agreement and shall entitle the other party to terminate this Agreement immediately upon written notice.

10. **Confidentiality**

10.1 Each party shall:

(a) keep confidential all Confidential Information disclosed by or on behalf of one party (the **"Disclosing Party"**) to the other party (the **"Receiving Party"**) during the course of this Agreement; and

(b) only disclose the Disclosing Party's Confidential Information as necessary and only to those employees, directors, officers, subcontractors and agents that need to know, for the purposes of performing its obligations or exercising its rights under this Agreement.

10.2 The Service Provider shall not disclose to third parties without the express prior written consent of the Lead Contact the results of work performed as part of the MyCorridor Project or any other information relating to the MyCorridor Project.

10.3 Each party shall procure that the obligations in this clause 10 are observed by its employees, directors, officers, subcontractors and agents who have access to Confidential Information in accordance with clause 10.1(b) and by any other third party who is granted access in accordance with clause 10.2.

10.4 The Receiving Party shall notify the Disclosing Party immediately if it becomes aware of any disclosure in breach of the obligations set out in this clause 10, and at the request of the Disclosing Party the Receiving Party shall immediately take all such steps as are necessary to prevent any further disclosure.

10.5 The provisions of this clause 11 shall not apply to:

(a) any information which is in the public domain at the date of this Agreement or which subsequently comes into the public domain other than by breach of this Agreement or any other confidentiality agreement; or

(b) any information already in the possession of the Receiving Party at the date of this Agreement, other than under an obligation of confidentiality; or

(c) any information obtained by the Receiving Party without any obligation of confidence from a third party that is not in breach of a confidentiality agreement with the Disclosing Party concerning the information obtained.

10.6 The provisions of this clause 10 shall be deemed effective from the date first contacts were established between the parties with respect to the subject matter of this Agreement and shall remain in full force and effect for a period of four (4) years following termination of this Agreement.

11. **Data Protection**

Each party shall comply with the Data Processing Agreement at Annex 1 to this Agreement.

12. **Warranties**

12.1 Each party warrants and represents that it has full power and authority under its constitution, has taken all necessary actions and has obtained all authorisations, licences, consents and approvals to execute and perform this Agreement.

12.2 Each party warrants and represents that it has, and will continue to have, all necessary rights in and its Intellectual Property or any other Intellectual Property or other materials made available by it to the other party under this Agreement.

12.3 Each party warrants and represents that it has not, prior to the Effective Date, entered into any agreement, arrangement, joint venture, collaboration, competitive project or other dealing with any other person or body which would or might affect, conflict with or prejudice this Agreement or the rights of the other party under it, or which would or might prejudice the objectives of the MyCorridor Project, and that none of its employees, officers, agents or other persons engaged by a party has done so.

13. **Term and termination**

13.1 This Agreement shall commence on the Effective Date and, subject to earlier termination in accordance with this clause 13, shall continue for a fixed term until 31 May 2020 unless terminated in accordance with this clause 13 (the **"Term"**).

13.2 The MyCorridor Technical Partners may by written notice sent to the Service Provider by the Lead Contact immediately terminate this Agreement and/or access to the MyCorridor Platform if:

(a) the Project Funding is suspended, materially reduced or if the Grant Agreement is terminated;

(b) any of the MyCorridor Technical Partners are no longer a member of the MyCorridor Consortium; or

(c) the Service Provider is in breach of any of its confidentiality obligations under clause 10.

13.3 Either the Service Provider or the MyCorridor Technical Partners may terminate this Agreement immediately by written notice to the other party (which in the case of the MyCorridor Technical Partners shall be sent by the Lead Contact), if at any time:

(a) the other party commits a material breach of this Agreement which (in the case of a breach capable of a remedy) it does not remedy within 30 days of receiving written notice of the breach; or

(b) the other party suffers an Insolvency Event, or is likely to do so in the reasonably opinion of the terminating party.

14. **Consequences of termination**

14.1 Within 10 days of termination of this Agreement, the Service Provider shall, at its own expense, safely return to the MyCorridor Technical Partners (or at a MyCorridor Technical Partner's direction, destroy and irrecoverably delete) all documents and materials, including Confidential Information, (and any copies) in its possession or control.

14.2 Where a MyCorridor Technical Partner directs the Service Provider to destroy and irrecoverably delete all documents and materials under clause 14.1, the Service Provider shall, within 48 hours of destroying and irrecoverably deleting all such documents and materials, confirm to that MyCorridor Technical Partner in writing that it has complied with clause 14.1.

14.3 In respect of any Intellectual Property, made available by a MyCorridor Technical Partner to the Service Provider under or in connection with this Agreement, on termination of this Agreement, the Service

Provider shall cease using such Intellectual Property and take all reasonable steps to delete and render inaccessible any copies of or access to the same.

14.4 Termination shall be without prejudice to the accrued rights of either party at the termination date.

15. Liability

15.1 The parties acknowledge and agree that this is a collaboration agreement for the purposes of conducting research in furtherance of the MyCorridor Project. Accordingly, subject to clause 15.2, to the fullest extent permitted by law, the MyCorridor Technical Partners exclude all liability to the Service Provider, whether in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising out of or in connection with the performance or contemplated performance of this Agreement, including for (without limitation):

(a) all losses including any special, indirect, or consequential or pure economic loss, costs, damages, charges or expenses;

(b) any loss of profits, loss of business, loss of revenues, loss of anticipated savings, loss of sales, loss of opportunity, depletion or loss of goodwill or damage to reputation or similar losses;

(c) loss of use, loss or corruption of data, software, or information, damage to or loss of use of computer equipment;

(d) any failure to provide the MyCorridor Platform;

(e) any failure to meet the obligations under this Agreement; and

(f) any and all warranties, conditions, undertakings, terms and obligations implied by law (whether by statue, common law or otherwise).

15.2 Nothing in this Agreement shall limit or exclude the liability of either party for:

(a) death or personal injury caused by its negligence;

(b) fraud or fraudulent misrepresentation; and

(c) any other liability which cannot be limited or excluded by applicable law.

15.3 The Service Provider shall be solely and fully liable for any damage, loss, cost, expense, claim or other liability relating to Participants arising from or connected to the Service Provider's provision of the Services.

15.4 The Service Provider acknowledges and agrees that the MyCorridor Technical Partners shall not have any responsibility or liability to Travellers with respect to the transportation services being provided by the Service Provider for a Booking or Journey, whether under this Agreement or otherwise.

15.5 The Service Provider acknowledges and agrees that the MyCorridor Technical Partners shall be jointly and severally liable for their obligations under this Agreement, and no other member of the MyCorridor Consortium shall have any liability under this Agreement.

16. **Insurance**

16.1 The Service Provider shall take out and maintain insurance cover at its own cost with a reputable insurance company to cover its potential liabilities arising under or in connection with this Agreement to such extent as would be reasonably expected to be taken out and maintained by an experienced, reasonable and prudent provider of services which are the same or similar to the Services.

16.2 This clause shall survive termination of this Agreement, howsoever arising.

17. **Dispute resolution**

17.1 A party shall not commence court proceedings (except proceedings seeking interlocutory relief) in respect of a Dispute arising out of or in connection with this Agreement unless it has complied with this clause 18.

17.2 If any Dispute arises out of or in connection with this Agreement, the Lead Contact of the party raising the Dispute shall provide written notification to the other party setting out the details of the Dispute (a **"Dispute Notice"**).

17.3 Within five (5) Business Days of a party receiving a Dispute Notice from the other party, the Lead Contact shall commence discussions in an attempt to settle the Dispute amicably.

17.4 If the Dispute cannot be resolved within thirty (30) Business Days following the commencement of discussions between the parties the Dispute is not resolved, or if discussions do not commence in accordance with clause 17.3, the Dispute shall be finally settled by binding arbitration under the Rules of Conciliation and Arbitration of the International Chamber of Commerce by two arbitrators appointed in accordance with the said Rules. The language of arbitration shall be English and the arbitration shall take place in London or such other place as the MyCorridor Technical Partners and the Service Provider shall agree in writing. Payment of associated costs shall be determined by the arbitrators appointed under this clause 18.

18. **Force majeure**

Neither party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure result from events, circumstances or causes beyond its reasonable control. In such circumstances the affected party shall be entitled to a reasonable extension of the time for performing such obligations. If the period of delay or non-performance continues for fifteen (15) Business Days, the party not affected may terminate this Agreement by giving seven (7) Business Days' written notice to the affected party.

19. **Assignment and other dealings**

19.1 Subject to clause 19.2, this Agreement is personal to the parties and neither party shall assign, transfer, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any of its rights and obligations under this Agreement, without the other party's prior written consent, not to be unreasonably withheld or delayed.

19.2 Notwithstanding clause 19.1, the MyCorridor Technical Partners may, in whole or in part, assign or subcontract this Agreement to another member of the MyCorridor Consortium Member where necessary.

20. **No partnership or agency**

Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other.

21. **Notices**

21.1 Any notice required or authorised to be given under this Agreement will be in writing to the Lead Contact of the recipient party and may be served by (i) personal delivery; (ii) first class post; or (iii) email.

21.2 Notices shall be deemed served (i) in the case of a notice delivered by hand, at the time of delivery; (ii) in the case of a notice sent by post, on the second Business Day after the day of posting; and (iii) subject

to condition 21.3, in the case of a notice sent by email, one hour after transmission or, if not sent on a Business Day, on the next Business Day.

21.3 Notice will be valid if served by email provided that the notice is expressly acknowledged by the recipient by return email (as the case may be) or other written acknowledgement. For this purpose, any automated response, including error messages and "out-of-office" responses to an email will not be treated as acknowledgement for the purposes of this clause 21.

21.4 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

22. **Variation**

22.1 No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

22.2 Both parties shall, at all times, remain willing to discuss possible contractual variations that have been prompted by technical, Project Funding or other factors, although neither party shall have any obligation to agree to any such variation proposed.

23. **Waiver**

A failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this Agreement shall prevent or restrict the further exercise of that or any other right or remedy.

24. **Governing law**

This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

25. **Jurisdiction**

Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

26. **Severance**

26.1 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Agreement.

26.2 If any provision or part-provision of this Agreement is deemed deleted under clause 26.1, the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

27. **Entire Agreement**

27.1 Save as expressly stated otherwise in this Agreement, this Agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

27.2 Each party acknowledges that in entering into this Agreement it does not rely on, any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement.

27.3 Each party agrees that it shall have no claim for innocent or negligent misrepresentation based on any statement in this Agreement.

27.4 Nothing in this clause shall limit or exclude any liability for fraud.

28. **Survival**

Provisions of this Agreement which are either expressed to survive its termination or, from their nature or context, are apparently intended to survive such termination shall remain in full force and effect notwithstanding termination.

29. **Further assurance**

Each party shall, and shall use all reasonable endeavours to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may reasonably be required for the purpose of giving full effect to this Agreement.

30. **Third Party Rights**

This Agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

This Agreement has been duly executed by the parties.

Signed for and on behalf of

Signature: ……

Name:

Position:

Date: ……

Signed for and on behalf of

[●]

Signature: ……

Name: ……

Position: ……

Date: ……

Schedule 1

Project description

MYCORRIDOR PROJECT

The aim of the MyCorridor Project (Project ID: 723384) is to develop an innovative platform, offering a one-stop-shop for Travellers, based on ITS. These ITS technologies will include, without limitation, interactive traffic management, extending the current capability of TM 2.0, to make MaaS a sustainable reality, seamlessly integrating public and private transport systems as needed, into a cross-border travel chain. The unique focus of the MyCorridor Project is to facilitate personalised, sustainable travel in urban and interurban areas across the EU, in an ITS-facilitated, multi-modal, integrated MaaS chain.

This Schedule sets out a summary of the MyCorridor Project's objectives, but a more detailed description can be found at Annex 2.

MyCorridor Project objectives

The MyCorridor Project objectives include (without limitation):

(a) collaborating with service providers, providing the opportunity to bring together MaaS aggregators, conventional transport operators and infomobility services, using a single access digital platform;

(b) conducting Pilots, to receive feedback from Participants and the Service Provider's to test and evaluate the user experience of the MyCorridor Platform;

(c) developing a multi-faceted evaluation framework for the testing and evaluation of the MyCorridor Platform and its potential as a possible ecosystem, by:

  (i) receiving and evaluating Participant and the Service Provider feedback (through various mediums, including , without limitation, face-to-face interviews, feedback forms and focus groups) relating to the usefulness and usability of the MyCorridor Platform and the user experience of Participants and the Service Provider in using the MyCorridor Platform;

  (ii) receiving and evaluating the Service Provider's feedback (through various mediums, including, without limitation, face-to-face interviews, feedback forms and focus groups), providing information relating to, for example, the Service Provider's integration of, and Participant's experience of, the Services and the Service Provider's experience with the Service Registration Tool;

  (iii) evaluating the user experience of the MyCorridor Platform in real-life Pilots; and

  (iv) receiving and evaluating user's acceptance and Participant's feedback relating to their willingness to pay for a MaaS service, changes in their habits/attitudes following the switch to the MyCorridor One-Stop-Shop system, as well as the impacts on local businesses, organisations and society as a whole.

(d) conducting meta-evaluation, to further provide valuable data about the real value of MaaS concept and technologies in different European countries, taking into consideration cultural, literacy, behavioural aspects of the Travellers.

(e) optimising the MyCorridor Platform and the One-Stop-Shop;

(f) developing an impact assessment to assess future opportunities and possible success rate of transportation and market penetration of the MyCorridor One-Stop-Shop and MyCorridor Platform; and

(g) publication of the MyCorridor Project's research results, through an open-source model.

Schedule 2

Services

Categories of information to be provided by the Service Provider

- **Name**: The name of the service
- **Cluster**: The cluster to which the service belongs
- **Subcluster**: The subcluster to which the service belongs
- **Mobility Product**: The mobility product offered by the service
- **Location**: A set of locations (cities, countries, or both) where the service operates
- **Time Period**: A set of time periods (i.e. day plus time period within day) when the service operates
- **Cost**: It denotes if the service is provided for a fee or free of charge
- **API**: It denotes the availability of an existing API providing business information of the service (e.g. timetables for a public transport service)
- **API URL**: The base URL of the API
- **API Response Type**: The response type (i.e. JSON, XML [5] or both) of the web API
- **Booking API**: It denotes the availability of an API providing booking functionalities for the service (e.g. booking a seat for a coach)
- **Booking API URL**: The base URL of the Booking API
- **Booking API Response Type**: The response type (JSON, XML or both) of the Booking API
- **Business rules**: General, business rules of the service that may affect the passengers (e.g. discount policies)
- **Comments**: Additional comments/remarks of Service Provider in relation to the operation of the service
- **API documentation**: A file (in PDF format) describing in detail both the API and the booking API of the service

Schedule 3

Additional information relating to the Services

MyCorridor Service Category - Clustering	
Mobility services cluster: Services related to the online purchase of *Mobility Products*, which are available for purchase via the MyCorridor one-stop-shop. **In this cluster, any informatory service part met is because it is part of a Mobility Product. For example, the informatory part of a PT service is clustered here, only if it can finally lead to ticket booking and/or purchase. If it is decoupled and is merely an informatory service (upon payment or not), it belongs to the infomobility services cluster below.**	**Vehicle related services**: MyCorridor services supporting purchase of *Mobility Products* for private use of cars (i.e. parking, rental, etc.).
	Vehicle (car/bike/ecar/ebike/ride) sharing/pooling: MyCorridor services supporting purchase of sharing/pooling *Mobility Products*.
	Public transport: MyCorridor services supporting purchase of Public Transport *Mobility Products (urban, interurban)*.
	Public Transport (Para transit): MyCorridor services supporting purchase of para transit *Mobility Products* (i.e. taxi services, demand-responsive transport services).
	Tourist: Services targeting specifically at tourism.
	Vehicle related/Public Transport: Services combining vehicle and PT services (i.e. ferry services).
Traffic management services cluster: Services related to the online purchase of Traffic Management related *Mobility Products* and/or the use of advanced Traffic Management concepts in the MaaS framework. **Can be TM2.0 enabled or not. TM2.0 for MyCorridor stands for the integration of data coming from several sources (i.e. TomTom) feeding the original service.**	**Advanced traffic management services** (i.e. real time traffic state and forecast, event management, etc.)
	Access control & Tolling: MyCorridor services supporting purchase of traffic/demand management products (such as tolls, urban congestion pricing, zone access control).
	C-ITS enabled traffic management services (i.e. traffic lights control and forecasting, etc.).
Infomobility services cluster: Services related to the information and real-time support of the user in *pre-trip phase* (trip planning, support in decision of what *Mobility*	**Multimodal**: MyCorridor service combining multi modal information/route planning/guidance into a **single feedback** to the user.
	Public Transport: MyCorridor services supporting use of Public Transport *Mobility Products*, prior or after their purchase, related to real time info, timetables, etc.

MyCorridor Service Category - Clustering	
Product to purchase), *on-trip phase (*and *after trip phase* if applicable*)*. They can be related to *Mobility Products* sold by MyCorridor or for any other mobility service/product not currently supported by MyCorridor. In the latter case, the user just gets information/guidance without the possibility to buy those mobility services.	**Park & Ride**: MyCorridor services supporting use of Park & Ride *Mobility Products* (i.e. real-time information for parking availability and PT estimated time of arrival).
Added Value services cluster: Services giving added value to the user and enhancing user experience. **Could be closely associated to mobility or not.**	**Touristic/Entertainment**: Services related to supply of touristic/cultural/entertainment information.
	Synthetic: Services that result as a synthesis of independent services.

MaaS Ecosystem stakeholder cluster	PART A Indicative stakeholders	PART B Stakeholders profile/ responsibilities
Mobility/MaaS operator *or* MaaS aggregator *or* Maas Issuer *(the term MaaS Aggregator will be used from now on in the current document)*	• MaaS company • Traffic Management or City agency • Public transport operator • PPP • E – marketplace business entity • An alliance of mobility operators, etc.	• Combines the transport services (*mobility products*), infomobility services and other ICT services into a single application. • Provides personalised travel solutions. • Responsible for customer service and user experience • Basically a business role; could be coupled with a technical role. • *Could be one entity, an alliance of entities or roaming businesses following the telecom world paradigm. As seen in previous column, this role could be played – depending the business model – by various entities.*
Transportation Service Provider/Operator (supplier of mobility products)	• Public transport operators (all modes) • Vehicle (car/bike/...) sharing/pooling/rental service provider (public or private) • Parking operators • Road operators (tolls) • Taxi operators • Coach buses operators	• Transport operator providing schedules, fares as covered by Ticketing, offer fares and real-time information, vehicle information, booking information, availability, locations (e.g. bikes and docking stations). • Multi modal or road management.

MaaS Ecosystem stakeholder cluster	PART A Indicative stakeholders	PART B Stakeholders profile/ responsibilities
	• Traffic Management operator	• Running ITS applications for management, control and passenger information purposes. • Could provide also transport content (i.e. drivers and rides database).
Infomobility, added value and Mobile Service / Technology providers *(for convenience, the shortened term to be used will be Mobile Service Providers from now on)*	• Infomobility services providers • Dynamic navigation service providers • Mobile application providers • Telecom providers • Financial services providers • Trusted 3rd parties • Technology (ICT, ITS) providers • *Other/Local MaaS aggregators*	• Provide infomobility related services (i.e. information services, value-added services, etc.). • Provides key enabling technology and services (e.g. mobile ticketing, payment) and ICT infrastructure. • Providing ITS infrastructure.

Key Definitions of Service Registration Tool	
Name	The name of the service
Cluster	The cluster to which the service belongs
Subcluster	The subcluster to which the service belongs
Mobility Product	The mobility product offered by the service
Location	The location (city) where the service operates
Service starting time	The start time of a service session
Service ending time	The end time of a service session
Business rules	General, business rules of the service that may affect the passengers (e.g. discount policies)
API availability	The availability of an existing web API
API type	The response type (JSON, XML or both) of the web API
API URL	The base URL of the web API
Booking API availability	The availability of an existing web API through which the service is booked by the Traveller
Booking type	The response type (JSON, XML or both) of the Booking API
Booking API URL	The base URL of the Booking API
Comments	Additional comments/remarks of the Service Provider in relation to the operation of the service

Schedule 4

Lead Contact details

MyCorridor Technical Partners Lead Contact

Name:

Email address:

Service Provider Lead Contact

Name:

Email address:

Schedule 5

MyCorridor Consortium Technical Partners

Annex 1

Data Processing Agreement

Definitions

"Data Protection Legislation" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of personal data including: (i) the General Data Protection Regulation (EU Regulation) 2016/679 (the **"GDPR"**); (ii) any laws or regulations ratifying, implementing, adopting, supplementing or replacing the GDPR; and (iii) any laws and regulations implementing or made pursuant to EU Directive 2002/58/EC (as amended by 2009/136/EC); in each case, as updated, amended or replaced from time to time.

The terms **"Data Controller"**, **"Data Processor"**, **"Data Subject"**, **"Joint Controllers"**, **"Personal Data"**, **"process"** and **"processing"** shall have the meanings set out in the GDPR.

1. **Data protection**

1.1 The parties shall, at all times, comply with the provisions and obligations imposed by the Data Protection Legislation and the data protection principles set out therein when storing and processing Personal Data in respect of the types of Personal Data, categories of Data Subjects, nature and purposes, and duration, set out in paragraph 1.6 of this Annex 1.

1.2 To the extent that one party provides Personal Data to the other to process on its behalf, the party providing the Personal Data shall act as Data Controller and the receiving party shall act as Data Processor.

1.3 Each party shall maintain records of all processing operations under its responsibility that contain at least the minimum information required by the Data Protection Legislation, and shall make such information available to any competent supervisory authority on request.

1.4 To the extent that either party acts as a Data Processor in respect of any Personal Data that it receives from the other party (and in respect of which the other party is the Data Controller), the Data Processor shall:

(a) process such Personal Data only in accordance with the Data Controller's instructions from time to time (including those set out in this Agreement), and only for the duration of this Agreement;

(b) not process the Personal Data for any purpose other than those expressly authorised by the Data Controller;

(c) take reasonable steps to ensure the reliability of all its employees who have access to the Personal Data, and ensure that any such staff are committed to binding obligations of confidentiality;

(d) implement appropriate technical and organisational measures and procedures to protect Personal Data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of Personal Data;

(e) not transfer the Data Controller's Personal Data outside the European Economic Area without the prior written consent of the Data Controller, and if the Data Controller so consents, take such steps as are required by the Data Controller to ensure that the relevant transfer, access or processing complies with the Data Protection Legislation;

(f) promptly, and in any event, within 24 hours, inform the Data Controller if any of the Data Controller's Personal Data (that is in the Data Processor's possession or control) is lost or destroyed or becomes damaged, corrupted, or unusable. The Data Processor shall restore such Personal Data at its own expense where data loss or destruction is for reasons attributable to the Data Processor;

(g) notify the Data Controller within two (2) Business Days if it receives a request from a Data Subject for access to that person's Personal Data;

(h) provide the Data Controller and any supervisory authority with full co-operation and assistance in relation to any request made by a Data Subject to exercise its rights under the Data Protection Legislation;

(i) only appoint a sub-processor of Personal Data with the prior written consent permission of the Data Controller, and notwithstanding such appointment, the Data Processor shall be liable for the acts and omissions of any such third party as if they were the acts and omissions of the Data Processor;

(j) not disclose any Personal Data to any Data Subject or to a third party other than at the written request of the Data Controller or as provided for in this Agreement;

(k) hand over all personal data to the Data Controller, or, at the Data Controller's request, delete all Personal Data, on termination or expiry of this Agreement and not make any further use of such Personal Data (except to the extent applicable law requires continued storage of the Personal Data by the Data Processor, and the Data Processor has notified the Data Controller accordingly, in which case the provisions of this paragraph 1.4 shall continue to such Personal Data);

(l) make available to the Data Controller and any competent supervisory authority all information necessary to demonstrate or ensure compliance with the obligations laid down in this paragraph 1 and/or the Data Protection Legislation;

(m) permit the Data Controller or its representatives to access ay relevant premises, personnel or records of the Data Processor on reasonable notice to audit and otherwise verify compliance with this paragraph 1.

(n) take such steps as are reasonably required to assist the Data Controller in ensuring compliance with the obligations set out in Articles 30 to 34 (inclusive) of the GDPR.

1.5 If either party receives any complaint, notice or communication which relates directly or indirectly to the processing of Personal Data by the other party or to either party's compliance with the Data Protection Legislation, it shall as soon as reasonably practicable notify the other party and it shall provide the other party with reasonable co-operation and assistance in relation to any such complaint, notice or communication.

1.6 Processing of Personal Data under this Agreement shall be in respect of the following:

Categories of Data Subjects	
Types of Personal Data	

Purpose and nature of processing	
Duration	

Annex 2

[Detailed description of the MyCorridor Project and objectives]

Annex IIB. MyCorridor Platform terms and conditions for external service providers

1. **Our Agreement**

1.1 These terms and conditions (the "**Terms**") are the terms on which the technical partners within the MyCorridor consortium, as defined below, provide you, as a service provider, with access to the MyCorridor platform (which includes any services, features, content and interfaces provided through the platform) (the "**Platform**").

2. **About us**

2.1 MyCorridor is a consortium of partners, carrying out the MyCorridor research project, funded by the European Union's Horizon 2020 initiative, project ID: 723384 (the "**MyCorridor Project**"). The consortium includes the technical partners listed in Annex 1 to these Terms, who are responsible for bringing you the MyCorridor Platform and associated services (together the "**MyCorridor Technical Partners**" "**we**", "**us**", "**our**").

2.2 Subject to these Terms, you are invited to register your transport-related services (the "**Services**") via the Platform using our registration tool (the "**Registration Tool**"), to make your Services available to users of the Platform ("**Users**"), for the purposes of the MyCorridor Project's research.

2.3 Please read these Terms carefully. By ticking the box confirming that you accept these terms, or otherwise by offering your services via our Platform, you represent to us that:

(a) you have read and understood these Terms;

(b) you agree to be bound by these Terms without modification in relation to the Platform;

(c) you have the power, capacity and authority to enter into these Terms;

2.4 We may amend these Terms from time to time in order to reflect changes to the Platform and for legal, regulatory or security reasons. We will give you reasonable notice by email of any material changes to these Terms.

2.5 If you have any questions, complaints or comments about the Platform, the Registration Tool or these Terms, please contact us at mycorridor@certh.gr.

3. **The Platform**

3.1 The Platform is made available free of charge via the mobile application developed by us, for the purposes of the MyCorridor Project's research.

3.2 The Platform is designed to enable you to integrate your Services into the Platform, using the Registration Tool, to make your Services available to Users of the Platform, for the purposes of the MyCorridor Project's research trials.

3.3 You acknowledge and agree that we provide the Platform on an 'as-is' basis for the purposes of evaluation and testing as part of the MyCorridor Project and we do not warrant or guarantee that the Platform will be always be available, uninterrupted or fault free and we do not accept any liability for any errors or omissions.

3.4 We do not make any statement (express or implied) that your use of the Platform will produce and/or generate any particular outcome (whether in relation to (without limitation) the Platform's functionality,

success or volumes of trips booked) and, save as set out in these Terms, we do not make any other representations, warranties, conditions or endorsements of any kind whatsoever (express or implied) about the Platform, including, but not limited to, any implied term, condition, representation or warranty of satisfactory quality or fitness for a particular purpose.

3.5 We are constantly looking for ways to improve and expand the Platform. You agree that you shall provide feedback to us, as and when requested by us, to assist with the development and optimisation of the Platform.

3.6 We may improve, update or change our Platform or Registration Tool from time to time, in line with one of the MyCorridor Project's objectives, which is to optimise this Platform and the Registration Tool. We will try to give you reasonable notice of any major updates or changes that may affect you and your provision of the Services.

3.7 We assume no responsibility for the contents of any other websites linked to the Platform. Where the Platform does contain links to other websites and resources provided by third parties, these links are provided for information only. The use of a third party website may be subject to separate terms and conditions.

3.8 You are also responsible for ensuring that all persons who access the Platform through your internet connection are aware of these Terms and the other applicable terms and conditions listed above, and that they comply with them.

3.9 We may suspend or terminate the Platform (or your access to it) without notice or liability to you at any time if we feel this is necessary (for example for improvements, maintenance or upgrades), but will use reasonable endeavours to notify you of the same in advance.

4. Registration Tool

4.1 In order to use the Platform you are required to be a registered service provider. You shall complete the registration process using the Registration Tool or, in the event that the Registration Tool is faulty, or where we otherwise direct, using such other means as may be agreed between you and us in writing.

4.2 In order to become a registered service provider, you will be asked to provide your company name, the link to your company's website offering the Services, and to set up a password and username. You are responsible for maintaining the confidentiality of your password and username and are responsible for all activities that are carried out under them. We will not be responsible for losses suffered by you where your password or user name is used by someone else. You agree to notify us immediately by email to mycorridor@certh.gr if you become aware of or suspect any unauthorised use of your password or username.

4.3 By registering, you agree that you are fully responsible for all activities that occur under your username and password. We may assume that any communications we receive under your account have been made by you.

5. Your use of the Platform

5.1 *Your promises to us*

You represent and warrant that:

(a) you will comply at all times with all applicable laws in force from time to time;

(b) all information and details provided by you to us (including on registration) are true, accurate and up to date in all respects and at all times;

(c) you will only use the Platform and make your Services available to Users on these Terms and in accordance with the MSA; and

(d) you will at all times comply with any guidelines provided to you by us from time to time.

5.2 ***Your conduct***

You agree that you will not:

(a) use ideas, formats, concepts, themes, excerpts or any other aspects of other content you may view on the Platform in order to create (or authorise the creation of) any material similar in nature to, or derived from, that content;

(b) use the Platform for any unlawful or unauthorised purpose;

(c) use the Platform in any way that interrupts, damages, impairs or renders the Platform less efficient;

(d) claim to have any rights, other than those set out in these Terms or the MSA to use any Application Programming Interface (the "**API**") provided by us;

(e) breach section 6 'We are not responsible for viruses and you must not introduce them';

(f) authorise, encourage or assist any other person to copy, modify, reverse-engineer, decompile, disassemble, alter or otherwise tamper with any software (including source code), databases and other technology that forms part of the Platform;

(g) access or attempt to access the accounts of other users or penetrate or attempt to penetrate the Platform's security measures.

6. **We are not responsible for viruses and you must not introduce them**

6.1 We do not guarantee that the Platform will be secure or free from bugs or viruses. You are responsible for configuring your information technology, computer programmes and computer platform in order to access the Platform. You should use your own virus protection software. We will not be liable for any losses which you sustain as a result of any virus, Trojan, worm, logic bomb, denial-of-service attack, or other malicious or technologically harmful material that may infect your computer equipment, computer programs, data or other proprietary material (each a "**Virus**") due to use of the Platform.

6.2 You must not:

(a) transfer files that contain Viruses or otherwise knowingly introduce any Viruses into the Platform;

(b) attack (or instigate or facilitate the attack of) the Platform via a denial-of-service attack or a distributed denial-of-service attack;

(c) attempt to gain unauthorised access to the Platform, the server on which the Platform is stored or any server, computer or database connected to the Platform; or

(d) use the Platform for any purpose which is unlawful, abusive, libellous, obscene or threatening.

6.3 By breaching the above provisions, you may commit a criminal offence under the Computer Misuse Act 1990. We will report any such breach to the relevant law enforcement authorities and we will co-operate with those authorities by disclosing your identity to them. In the event of such a breach, your right to use the Platform will cease immediately.

7. **Intellectual Property**

7.1 All rights, title, interest and intellectual property (including patents, trade-marks, design rights, copyrights, database rights, trade secrets, rights in confidential information and all rights of equivalent nature anywhere in the world (whether registered or not), together with any applications or rights to apply for the foregoing) ("**IPR**") in the Platform and the Registration Tool, including their respective design, text and graphics, selection, arrangement and underlying source code and software, belong to the MyCorridor Project consortium entities or their licensors.

7.2 Subject to these Terms, we grant you, solely for purposes relating to your provision of the Services via the Platform:

(a) a revocable, non-exclusive, non-transferable and non-sublicensable licence to download and or receive the API provided by us to you, for the sole purpose of the integration of your Services with the Platform;

(b) a revocable, non-exclusive, non-transferable and non-sub licensable licence to access and use the Platform (and any development versions thereof) for the purpose of providing and managing the provision of your Services, in accordance with these Terms.

7.3 In circumstances where you provide the API to enable your Services to be integrated into the Platform, you provide us with an irrevocable, non-exclusive licence to use the API as necessary, for us to assist you with your integration of the Services into the Platform.

7.4 You agree to compensate and defend us fully against any claims or legal proceedings (including any costs or losses we incur or suffer related to these) brought against us by any other person as a result of your breach of this section 7 (Intellectual Property) (including if you are unable to validly grant us the rights you agree to grant).

7.5 Access to or use of the Platform or the Registration Tool does not grant you any ownership right in the Platform or the Registration Tool.

7.6 This section 7 (Intellectual Property) shall survive termination of your provision of Services via the Platform or any termination of these Terms.

8. **Confidentiality**

8.1 You shall treat as confidential and shall not (other than where permitted or compelled to do so by any applicable law) use or disclose to any person (nor permit the disclosure of) any of our confidential information which shall include any information (in whatever form) which is not publicly known and which is disclosed to, or otherwise learnt by, you in connection with your use of the Platform and your discussions with us regarding the MyCorridor Project.

8.2 This section 8 (Confidentiality) shall survive any termination of these Terms.

9. **Fees**

9.1 The Platform is provided by us to you free of charge for you to provide your Services via the Platform for the purposes of the MyCorridor Project's research objectives.

9.2 You acknowledge and agree that we shall act as an interface between you and the Users and where a User makes a Booking for your Services via the Platform, our registered payment services provider will accept such payment from the User on your behalf, and shall transfer such payment to you, as agreed in writing.

9.3 You acknowledge that we may, at our discretion, offer financial incentives to Users to encourage them to participate in a research trial for the purposes of the MyCorridor Project. Any such financial incentives shall not affect any payments owed to you in accordance with this section 9 (Fees).

10. **Term and Termination**

10.1 These Terms come into force on the date you begin the process of integrating your Services into the Platform and shall continue in force until terminated in accordance with these Terms or until you otherwise stop providing your Services via the Platform.

10.2 Termination for convenience: You or we may terminate the integration of your Services, your access to the Platform and these Terms at any time on not less than one month's prior written notice.

10.3 We may terminate your access to the Platform and these Terms on written notice to you with immediate effect if:

(a) the MyCorridor Project's funding is suspended, materially reduced or if the MyCorridor Project's funding agreement is terminated;

(b) any of the MyCorridor Technical Partners is no longer a consortium member of the MyCorridor Project;

(c) you commit a breach of these Terms which is capable of remedy and is not remedied within 30 days of written notice from the other; or

(d) you commit a material breach of these Terms which is not capable of remedy; or

(e) you make an arrangement with or assignment in favour of a creditor, go into liquidation or administration or a receiver or manager is appointed to manage your business or assets, or any analogous insolvency event occurs in the territory where you are located (if such termination is permitted by applicable law).

10.4 On any termination of these Terms your right to use the Platform shall cease and you shall not make (or attempt to make) any further use of it.

10.5 Termination (for whatever reason) of these Terms shall not affect:

(a) any rights, liabilities or obligations which accrued before such termination;

(b) any of these Terms that are intended to continue to have effect after such termination.

11. **Liability**

11.1 Your use of the Platform is for the purposes of the MyCorridor Project's research trial only. Subject to section 11.2 below, to the fullest extent permitted by law, we exclude all liability to you, whether in contract, tort (including negligence and breach of statutory duty), misrepresentation, restitution or otherwise, arising out of or in connection with the performance or contemplated performance of this Agreement, including liability for (without limitation):

(a) all losses including any direct, indirect or consequential losses;

(b) any loss of profits, loss of business, loss of agreements or contracts, loss of revenues, loss of opportunity, loss of anticipated savings, loss of use or corruption of software, data or information, loss of or damage to goodwill or reputation;

(c) any failure to provide the Platform or the Registration Tool;

(d) your use of, or inability to use, our Platform;

(e) any business interruption;

(f) any failure to meet our obligations under these Terms; and

(g) any and all warranties, conditions, undertakings, terms and obligations express or implied by law (whether by statue, common law or otherwise).

11.2 Nothing in this Agreement shall limit or exclude the liability of either party for:

(a) death or personal injury caused by its negligence;

(b) fraud or fraudulent misrepresentation; and

(c) any other liability which cannot be limited or excluded by applicable law.

11.3 You shall be solely and fully liable for any damage, loss, cost, expense, claim or other liability relating to other users of the Platform, arising out of or in connection with your provision of the Services and your use of the Platform.

12. **Data Protection**

For the purposes of this section 12 (Data Protection):

"**Data Protection Laws**" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of personal data including: (i) EU Regulation 2016/679 ("GDPR"); (ii) any laws or regulations ratifying, implementing, adopting, supplementing or replacing the GDPR; and (iii) any laws and regulations implementing or made pursuant to EU Directive 2002/58/EC (as amended by 2009/136/EC), in each case, as updated, amended or replaced from time to time; and

the terms "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**processing**", "**technical and organisational measures**" and "**transfer**" (in the context of transfers of Personal Data) shall have the meanings set out in the GDPR.

12.1 You acknowledge and agree that you and we are each acting as independent Controllers in respect of any Personal Data transferred under these Terms. Notwithstanding any other provision of this Terms, in exercising our respective rights and performing our respective obligations under these Terms you and we shall each act, to the extent necessary, at all times comply with the Data Protection Laws and shall not do or omit to do anything which has the effect of placing the other party in breach of any such laws or regulations.

12.2 To the extent you receive from us, or process any Personal Data on our behalf, you shall:

(a) process such Personal Data (i) only in accordance with our written instructions from time to time (including those set out in these Terms), and (ii) only for the duration that these Terms remain in force;

(b) not process such Personal Data for any purpose other than those set out in these Terms or otherwise as expressly authorised by MyCorridor;

(c) take reasonable steps to ensure the reliability of all your personnel who have access to such Personal Data, and ensure that any such personnel are committed to binding obligations of confidentiality when processing such Personal Data;

(d) implement and maintain technical and organisational measures and procedures to ensure an appropriate level of security for such Personal Data, including protecting such Personal Data against the risks of accidental, unlawful or unauthorised destruction, loss, alteration, disclosure, dissemination or access;

(e) not transfer, access or process such Personal Data outside the European Economic Area without our prior written consent (and, if we so consent, take such steps as we reasonably require to ensure that the relevant transfer, access or processing complies with the Data Protection Laws);

(f) promptly inform us if any such Personal Data is (while within your or your subcontractors' possession or control) subject to a personal data breach (as defined in Article 4 of GDPR) or is lost or destroyed or becomes damaged, corrupted or unusable;

(g) only appoint a third party (including any subcontractors) to process such Personal Data with our prior written consent, and notwithstanding any such appointment by you, you shall be liable for the acts and omissions of any such third party as if they were your acts and omissions;

(h) not disclose any Personal Data to any Data Subject or to a third party other than at our written request or as expressly provided for in these Terms;

(i) irretrievably delete, or where we so request return, all Personal Data on termination or expiry of these Terms, and not make any further use of such Personal Data (except to the extent applicable law requires your continued storage of the Personal Data, in which case you shall notify us accordingly and the provisions of this section 12 (Data Protection) shall continue to apply to such Personal Data);

(j) provide us and any DP Regulator with all information and assistance necessary or desirable to demonstrate or ensure compliance with the obligations in this section 12 (Data Protection) and/or the Data Protection Laws;

(k) permit MyCorridor or our representatives to access any relevant premises, personnel or records of yours on reasonable notice to audit and otherwise verify compliance with this section 12 (Data Protection);

(l) take such steps as are reasonably required to assist us in ensuring compliance with our obligations under Articles 30 to 36 (inclusive) of GDPR;

(m) notify us within two (2) Business Days if you receive a request from a Data Subject to exercise its rights under the Data Protection Laws in relation to that Data Subject's Personal Data; and

(n) provide us with your full co-operation and assistance in relation to any request made by a Data Subject to exercise its rights under the Data Protection Laws in relation to that Data Subject's Personal Data.

12.3 If either party receives any complaint, notice or communication which relates directly or indirectly to the processing of Personal Data by the other party or to either party's compliance with the Data Protection Laws, it shall as soon as reasonably practicable notify the other party and it shall provide the other party with reasonable co-operation and assistance in relation to any such complaint, notice or communication.

13. **Assignment/transfer**

13.1 We may assign or otherwise transfer all or any of our rights, liabilities and obligations under these Terms to any third party. We will notify you of any such assignment or transfer.

13.2 We may delegate the provision of the Platform or the performance of any obligation or function relating to the Platform and reserve the right to use any agents on such terms as we may think fit.

13.3 You shall not assign or transfer (or purport to assign or transfer) or otherwise deal with (including through the declaration of a trust) in whole or in part, your rights or obligations under these Terms without our prior written consent.

14. **Tax**

You are responsible for reporting, remittance, withholding and payment to the relevant tax authorities (as applicable) of the relevant taxes in relation to your provision of the Services. We are not responsible for determining whether taxes apply to any transaction, or for reporting or remitting any taxes arising from any transaction.

15. **General**

15.1 These Terms and, where you have entered into a master services agreement with us governing the integration of your Services into the Platform ("**MSA**"), that MSA, constitute the entire agreement and understanding between you and us relating to these Terms and supersede any previous agreement or understanding between you and us in relation to the same. Where applicable, if there is any conflict between these Terms and the MSA, the MSA shall prevail. Neither you nor we have relied on any statement, representation, warranty, understanding, undertaking, promise or assurance (whether negligently or innocently made) of any person that is not set out in these Terms or, where applicable, the MSA.

15.2 If we delay exercising or fail to exercise or enforce any right available to us under these Terms, this does not constitute a waiver of that right or any other rights under these Terms. A waiver by us of any default shall not constitute a waiver of any subsequent default. No waiver by us shall be effective unless it is expressly stated to be a waiver and is communicated to you.

15.3 If any part of these Terms is disallowed or found to be ineffective by any court or regulator, the other provisions shall continue to apply.

15.4 These Terms shall be construed and controlled by the laws of England and Wales and each party further consents to the exclusive jurisdiction of the courts of England and Wales.

15.5 These Terms are not intended to give rights to anyone except you and us. This Agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

15.6 You acknowledge that these Terms will not create any partnership, joint venture or trust relationship between you and us.

Thank you for using our Platform.

Annex 1

The MyCorridor Technical Partners

Centre for Research and Technology Hellas ("CERTH")

CERTH Hellenic Institute of Transport

CERTH Informatics and Telematics Institute

Italia TTS Association

AMCO Inspired Technologies

Viva Payments Services S.A

Salzburg Research SRFG

MAP Traffic Management B.V.

Swarco Mizar S.r.l

TomTom Location TechnologyGermany GMBH

Chaps spol sro

Annex IIC. MyCorridor consumer terms of supply

Introduction

The MyCorridor one-stop-shop mobile travel application (the "Platform"), is brought to you by the technical partners of the "**MyCorridor**" research consortium listed in Annex 1 to these Terms of Supply (the "**MyCorridor Technical Partners**", "**MyCorridor**", "**we**", "**us**", "**our**"), each a "**MyCorridor Technical Partner**".

Who we are and how to contact us

The MyCorridor Technical Partners form part of the MyCorridor consortium, carrying out the MyCorridor research project, funded by the European Union's Horizon 2020 initiative, project ID: 723384.

You can contact the MyCorridor Technical Partners at mycorridor@certh.gr.

These Terms of Supply

These Terms of Supply (the "**Terms**") set out the terms on which MyCorridor agrees to make the Services available to you via the Platform, including for the purposes of the Pilots (defined below).

Please read these Terms carefully. By using our Platform, you confirm that you accept these Terms and that you agree to comply with them. If you do not agree to these Terms, you must not use our Platform.

We recommend that you save and/or print a copy of these Terms for future reference when making a Booking.

1. **Definitions and scope**

1.1 ***Definitions***

The following definitions have the same meaning whether they are singular or plural.

"Booking" means any order for Services placed via our Platform.

"Journey" means a door-to-door travel solution, incorporating one or more Services, redeemable via one electronic ticket, accessible to you via the Platform after a Booking is made.

"Phase 1" means the first phase of the Pilots, with recruited users, in a controlled environment, for the purposes of testing and evaluating the Platform, without real-life travel.

"Phase 2" means the second phase of the Pilots, with recruited users, testing the Platform through real-life application, including actual travel and payment.

"Pilot" means the testing and evaluating of the Platform through Phase 1 and Phase 2. "**Pilots**" shall be construed accordingly.

"Supplier's Terms and Conditions" means the terms and conditions applicable to the Supplier(s) with whom you have concluded a separate contract by making a Booking for Services via the Platform.

"Service" means a transport service provided by a Supplier and offered via the Platform as part of a Journey, such as a flight, taxi, train or car hire. "**Services**" shall be construed accordingly.

"Supplier" means a supplier of Services, such as an airline, car hire company, train operator or other transport operator.

"Terms of Use" means the terms governing your use of the Platform, which supplement these Terms.

1.2 ***Scope***

The MyCorridor Platform is a one-stop shop, helping you to find door-to-door travel solutions and to make the necessary reservations for a Journey, redeemable via one electronic ticket ("**e-ticket**"), accessible via the Platform.

MyCorridor acts merely as an intermediary for the booking of Services. The Services in your Booking are governed by a contract between you and the relevant Supplier and MyCorridor is not responsible for any delays, cancellations or disruptions to any Service. Please refer to the relevant Supplier's Terms and Conditions before finalising a Booking.

These Terms only apply to you as a consumer or Pilot participant. If you are a Supplier or other service provider, please refer to our Service Provider Platform Terms and Conditions available here mycorridor@certh.gr.

MyCorridor may amend these Terms at any time without prior notice. Any such amendments to these Terms will not apply to Bookings that have already been accepted by MyCorridor, on behalf of the Supplier(s) concerned.

Other terms that apply to you

These Terms refer to the following additional terms, which also apply to your use of our Platform:

- our Terms of Use policy , which sets out the permitted uses and prohibited uses of our Platform. When using our Platform, you must comply with our Terms of Use policy;
- our Privacy Policy ;
- our Cookie Policy , which sets out information about the cookies we use; and
- the relevant Supplier's Terms and Conditions, which you'll find a link to in your Booking confirmation email, within the Platform itself or via the relevant Supplier's website.

2. **The Booking Process**

2.1 ***Your legal authority***

You must be at least 18 years old and legally authorised to enter into contractual obligations and, where relevant, have the requisite consent or authority to act for or on behalf of any persons included in a Booking.

2.2 ***The Booking process***

(a) *How to book*

The Platform will display one or more Journey suggestions, consisting of door-to-door travel solutions (including cross-border travel solutions), which may include more than one Service, in response to your search criteria. The Journey suggestions offered on the Platform specify the individual Services included in that Journey, together with the total price, a breakdown of the proposed itinerary, and a breakdown of the prices for each Service included in that Journey. Prices are shown in EUR.

Once you have selected your preferred Journey, payment will be requested via the Platform and processed by MyCorridor's Payment Services Provider, Viva Payments Services S.A ("VivaWallet"), in accordance with the 'Prices and Payment' section of these Terms below, to complete your Booking. Where your participation in the Pilot includes real-life testing conditions,

such as real-life travel, you will be required to pay for your travel ticket yourself. Where you are taking part in Phase 1 of the Pilots, which does not include real-life travel, no actual payment will be processed.

Please note that you may require other documentation or approval for travel to your destination. It is your responsibility to ensure that you carry all necessary documentation. We advise that you check with the relevant Supplier or passport office, prior to completing your Booking, whether there are any particular requirements for your Journey.

Suppliers (or related authorities) may require passenger information to be submitted to them prior to travel. We therefore reserve the right to request this information from you (which may include copies of your passport), to verify this information on behalf of Suppliers or authorities that require it.

(b) *Prices and payment*

MyCorridor acts as an interface between you and the Supplier. By making a Booking via the Platform, you authorise MyCorridor to act as your representative during the Booking process, and for our Payment Services Provider, VivaWallet, to accept the required payment from you and transfer it to the Supplier in your name and on your behalf. As stated in section 2.2.1, where you are participating in a Phase 1 Pilot, which does not require you to pay for the Services, this section 2.2.2, does not apply to you.

To enable your Booking to be finalised, you will be required to provide the details of your payment card via the Platform, and VivaWallet will often have to verify: (i) the validity of the payment card; and, (ii) the availability of funds on the payment card (to be confirmed by the bank issuing your card).

(c) *Pre-authorisation*

When you make a Booking we may need to take a pre-authorisation, which is a hold of a specified amount on your credit or debit card for a Booking to be finalised. If a pre-authorisation is required, you will be notified of the pre-authorisation amount at the time of making your Booking. This guarantees to us that the funds are available for you to pay for your Journey and for any additional charges which may be incurred during your Journey. Please note that this is not a charge and no funds will actually be debited from your account as part of this pre-authorisation process.

The amount of the pre-authorisation will depend on the Services in your Booking, and this amount will be notified to you at the time you make your Booking.

VivaWallet, as our Payment Services Provider, is responsible for the pre-authorisation process. If you have any questions regarding your pre-authorisation, please contact VivaWallet here https://www.vivawallet.com/en-gb/.

Once your Journey is completed, the final fare for that Journey will be debited from the credit or debit card you provided to us on making your Booking. Where the pre-authorisation amount was greater than the final fare for your Journey, any additional pre-authorisation amount will be released in accordance with your relevant credit or debit card's terms and conditions. Please note that it is your issuing bank which holds the pre-authorisation, and therefore if you have any questions relating to when your pre-authorisation will be released, please contact your issuing bank.

(d) *Additional payment terms*

Occasionally technical errors do occur, and we reserve the right to cancel any transaction in which a Service or Journey has been sold at an incorrect value.

We do not take third party payments. Therefore, the card holder must be one of the travellers.

Air miles and vouchers from loyalty programmes are not valid for Bookings via the Platform. If you are entitled to benefit from a discount, the associated special fares will be shown on the Platform during the Booking process, before you confirm the Booking.

(e) *Confirmation of Booking*

Once your Booking has been processed and accepted, you will receive a confirmation message via e-mail and your e-ticket via the Platform or via email, which will cover all the Services included in your Journey. The confirmation message and the Platform will provide details of your itinerary, the amount paid and instructions on how to use your e-ticket. On receipt of this confirmation message, your contract with the relevant becomes directly enforceable against that Supplier, without any intervention by MyCorridor.

Please ensure that you enter your email address carefully when you make a Booking. If your contact details subsequently change, please let us know straight away by contacting us at mycorridor@certh.gr, so we can make sure you don't miss any important messages, such as any changes to your itinerary.

Unfortunately, we're not responsible if anything goes wrong with your Booking or Journey because you gave us an inaccurate email address.

If you do not receive a confirmation message within 24 hours of placing the Booking, you should contact MyCorridor at mycorridor@certh.gr.

(f) *Your right to cancel or amend a Booking*

This section 2.2.4 only applies to you if you are booking real-life travel, which requires actual payment by you, (whether or not as a Pilot participant). Where you are participating in Phase 1 of the Pilot, you are not entitled to cancel or amend a Booking, unless you are doing so under, and in accordance with, our specific instructions, as part of the Pilot.

Your rights to cancel or amend a Booking will be subject to the relevant Supplier's Terms and Conditions. Where you consider you are eligible to cancel or amend a Booking, please contact MyCorridor at least 48 hours prior to commencing your Journey, at mycorridor@certh.gr.

A fee may be imposed by the applicable Supplier in the event of your cancellation or amendment to a Booking. Please refer to the relevant Supplier's Terms and Conditions.

(g) *Reimbursements and refunds*

This section 2.2.5 only applies to you if you are booking real-life travel, which requires actual payment by you (whether or not as a Pilot participant).

(i) *Reimbursements*

If you are participating in a Pilot, you may be entitled to a full or partial reimbursement of the amount paid by you for your Booking, if this has been agreed between you and us prior to your participation in the Pilot. If you are eligible for a reimbursement, this will be transferred directly to you by the relevant MyCorridor Technical Partner managing the Pilot. The Supplier is not responsible for any such reimbursement. If you have any queries relating to your entitlement to a reimbursement, please contact the MyCorridor Technical Partner in charge of the Pilot. If you are not sure which MyCorridor Technical Partner to contact, please contact mycorridor@certh.gr.

(ii) *Cancellations and delays by Suppliers*

In the event of a delay or cancellation to one of the Services in your Booking, or if a Supplier causes you to miss a connecting Service forming part of your Journey, you may be entitled to a refund or compensation from the Supplier (less any payment processing charges). Any right you may have to a refund (in whole or in part) or to any compensation, and the extent of any such refund or compensation, will depend on the Supplier's Terms and Conditions. Please contact the relevant Supplier if you consider you may be entitled to a refund or to compensation. Not all taxes are refundable and any card charges are not refundable.

(iii) *Cancellations and amendments by MyCorridor*

As a Pilot participant, you acknowledge that we will be testing and evaluating the Platform, and that therefore there may be occasions where we need to cancel or amend your Booking. Where we are required to cancel your Booking, we shall provide you with advance written notice of the cancellation via your account on the Platform or using the email address you provided to us when you signed up to the Pilot, and we shall issue you a refund for your Booking, or the part of the Booking which was cancelled, unless an amendment can be made.

In the event we propose an amendment to your Booking, we shall provide you with advance notice and details of an alternative proposed Service or Journey via your account on the Platform or using the email address you provided to us when you signed up to the Pilot (an "**Amendment Notice**"). If you are unable to accept the alternative Service or Journey proposed by us, you must notify us of this within 24 hours of receiving the Amendment Notice, using the contact details provided in the Amendment Notice.

For any cancellation, amendment or refund related enquiries, please contact us at mycorridor@certh.gr.

3. Your personal information

We will only use your personal information as set out in our privacy policy available here [*Insert link to privacy policy*].

4. The Services

4.1 *Supplier's Terms and Conditions*

This section 4 does not apply to you if you are taking part in Phase 1 of the Pilot, where you are not participating in real-life travel.

As a reminder, MyCorridor only acts as an intermediary for the booking of any Services. This means that the Services in your Booking are governed by a contract between you and the relevant Supplier and MyCorridor is not responsible for any delays, cancellations or disruptions to any Service. When you make a Booking via the Platform, MyCorridor makes the Booking on your behalf and these Terms are subject to each relevant Supplier's Terms and Conditions.

The Supplier's Terms and Conditions will set out what rights you have against the relevant Supplier and will explain their liability to you in the event of anything going wrong.

On making a Booking you automatically accept, and agree to comply with, the relevant Supplier's Terms and Conditions. You acknowledge that breaching the Supplier's Terms and Conditions could result in cancellation of your Booking, removal of any MyCorridor benefits offered to you, and additional charges.

We have no control over Suppliers or their respective websites, terms and conditions and policies. It is your responsibility to read and ensure you fully understand the relevant Supplier's Terms and

Conditions. In instances where a Supplier's Terms and Conditions are not accessible via a link on the Platform, please refer to the relevant Supplier's website. Following a request by you addressed to MyCorridor at mycorridor@certh.gr, we shall provide you with that Supplier's contact details so you can contact them directly to obtain a copy. Please ensure that you refer to the applicable Supplier's Terms and Conditions for any applicable cancellation or amendment charges and other important terms and conditions.

In particular, you acknowledge and agree that:

- MyCorridor has no control over the allocation of seats on any transport, even if pre-booked, and does not guarantee that any specific seats will be available on a journey;
- MyCorridor has no control over any indications of the journey times which are provided by the Supplier of the relevant Service and which are given for guidance only and are subject to alteration and confirmation by the Supplier;
- it is your responsibility to check and comply with the relevant Supplier's policies and Terms and Conditions. For example, (without limitation) on the carriage of pregnant women and children.
- additional charges may be imposed by some Suppliers for extras such as, (but not limited to), additional stops, meals, luggage, preferred seat selection or seat upgrades and access to Wi-Fi. Certain Services, e.g., car rentals, may also require additional charges to be paid locally, such as refuelling, additional driver charges, young driver surcharge and delivery and collection fees. Please refer to the relevant Supplier's Terms and Conditions for further information. You acknowledge that MyCorridor is not responsible for such charges and any information on such charges which may be shown on the Platform are for information only and may be amended by the relevant Supplier at any time. Queries or complaints relating to any such charges must be addressed directly with the relevant Supplier;
- a ticket may only be used by you or by the person in your travel group on whose behalf you bought the ticket;
- if you are making the Booking, you must be at least 18 years old; and
- although MyCorridor may provide information about disruption to a journey (such as line closures and bus replacement services), to the extent that such information is made available to MyCorridor by the relevant Supplier, it is your responsibility to check with the relevant Supplier directly if you are concerned about any possible planned or unplanned disruptions to your Journey.

4.2 *EU Community list*

In accordance with EU regulations, details of air carriers that are subject to an operating ban within the European Community are available at http://ec.europa.eu/transport/modes/air/safety/air-ban/index_en.htm.

4.3 *Accessibility*

If you require assistance relating to a disability or reduced mobility during your Journey, you should directly contact the Supplier with whom you will be travelling in accordance with the relevant Supplier's Terms and Conditions, to request such assistance. We recommend that you contact the relevant Supplier as soon as reasonably practicable after making your Booking.

4.4 ***Insurance***

The prices quoted on the Platform do not include travel insurance. You are therefore advised to take out insurance that covers the consequences of certain cases of cancellation and an additional policy that provides cover for certain special risks such as the cost of repatriation in the event of an accident or illness. It is your responsibility to ensure any insurance policy is adequate to cover your requirements.

5. **Service and the handling of complaints**

If you have a query, request for information, or complaint relating to a Service, you must first contact us at mycorridor@certh.gr. We shall initially process any query, request for information, or complaint you may have on behalf of Suppliers. However, where appropriate, you may subsequently be advised to contact the Supplier directly. You are encouraged to bring forward any complaint within 30 days of the end of a Journey.

If a complaint has arisen during the Journey, we recommend that you address the complaint directly with the relevant Supplier, so that measures can be taken to resolve the problem efficiently and limit the damage suffered by you.

The European Commission's Online Dispute Resolution Platform is available at http://ec.europa.eu/odr.

6. **MyCorridor's liability**

You accept that MyCorridor acts as an interface between you and the Suppliers and we will under no circumstances be liable with respect to any Service provided by a Supplier or for the acts or omissions of any other third party.

In rare circumstances out of our control such as, but not limited to, natural disasters, terrorist attacks and war ("force majeure" events), we or the relevant Supplier may be prevented from providing services to you. In such circumstances, we're exempt from our legal responsibilities and any other non-compliances that result from that event happening.

MyCorridor is not liable if and insofar as you are able to claim for damages under an insurance policy such as travel insurance.

The exclusions and limitations contained in this clause apply only to the extent permitted by applicable law.

7. **Law and jurisdiction**

These Terms are governed by the laws of England and Wales. You agree that the English Courts shall have jurisdiction to hear and determine any dispute arising from the interpretation of these Terms. However, you may choose the law and jurisdiction of the country in which you reside.

8. **General**

We may transfer our rights and obligations under these Terms to another organisation. You may only transfer your rights or your obligations under these Terms to another person if we agree to this in writing.

These Terms, together with any others incorporated or referred to in these Terms, constitute the entire agreement between you and us relating to their subject matter, and supersede all previous understandings and agreements (whether oral or written) relating to the subject matter.

If MyCorridor does not invoke one of the provisions of these Terms at any one moment, this must not be interpreted as a cession of the right to invoke it at a later date.

Each of the paragraphs of these Terms operates separately. If any court or relevant authority decides that any of them are unlawful, the remaining paragraphs will remain in full force and effect.

These Terms are a legally binding contract between you and us. No other person shall have any rights to enforce any of its terms.

These Terms come into force on 17 February 2020.

Annex 1

MyCorridor Technical Partners

Centre for Research and Technology Hellas ("CERTH")

CERTH Hellenic Institute of Transport

CERTH Informatics and Telematics Institute

Italian TTS Association

AMCO Inspired Technologies

Viva Payments Services S.A

Salzburg Research SRFG

MAP Traffic Management

Swarco Mizar S.r.l

TomTom Location TechnologyGermany GMBH

Chaps spol sro

Annex IID. MyCorridor consumer terms of use

Who we are and how to contact us

The MyCorridor one-stop-shop mobile travel application (the "**Platform**"), is brought to you by the technical partners of the "**MyCorridor**" research consortium listed in Annex 1 to these Terms of Supply (the "**MyCorridor Technical Partners**", "**MyCorridor**", "**we**", "**us**", "**our**"), each a "**MyCorridor Technical Partner**".

Who we are and how to contact us

The MyCorridor Technical Partners form part of the "**MyCorridor**" consortium, carrying out the MyCorridor research project, funded by the European Union's Horizon 2020 initiative, project ID: 723384 (the "**MyCorridor Project**").

You can contact the MyCorridor Technical Partners at mycorridor@certh.gr.

Definitions

"**Booking**" means the process of selecting and booking travel in accordance with our Terms of Supply.

"**Journey**" means a door-to-door travel solution, incorporating one or more Services, redeemable via one electronic ticket accessible to you via the Platform after a Booking is made.

"**Phase 1**" means the first phase of the Pilots, with recruited users, in a controlled environment, for the purposes of testing and evaluating the Platform, without any actual travel.

"**Phase 2**" means the second phase of the Pilots, with recruited users, testing the Platform through real-life application, including actual travel and payment by the user.

"**Pilot**" means the testing and evaluating of the Platform through Phase 1 and Phase 2. "Pilots" shall be construed accordingly.

"**Service**" means a transport service provided by a Supplier and offered via the Platform as part of a Journey, including (but not limited to) a flight, taxi, train or car hire. "**Services**" shall be construed accordingly.

"**Supplier**" means a supplier of Services, such as an airline, car hire company, train operating company, insurance provider or other transport or Service provider.

"**Terms of Supply**" means the terms of supply governing a Booking made by you via the Platform, accessible here [include link to Terms of Supply].

1. **Use of our platform**

1.1 By making a Booking via our Platform, browsing or otherwise using our Platform as a consumer or Pilot participant, you acknowledge and agree to have read and understood these Terms of Use (these "**Terms**"), and you confirm that you accept and agree to comply with them.

1.2 If you do not agree to these Terms, you must not use the Platform.

1.3 We recommend that you print a copy of these Terms for future reference.

1.4 The MyCorridor Platform is operated by the MyCorridor Technical Partners.

1.5 You declare that you are an adult (at least 18 years of age) with the legal capacity to be bound by these Terms and to use our Platform in accordance with these Terms. Further, you declare that all information you provide to access our Platform is true, complete and accurate and you agree to keep it updated.

2. There are other terms that may apply to you

The following additional terms also apply to your use of the Platform:

(a) Our Privacy Policy [*insert link to MyC's privacy policy*], which sets out the terms on which we process any personal data we collect from you, or that you provide to us during your use of the Platform. By using the Platform, you consent to such processing and you warrant that all data provided by you to us is accurate; and

(b) our Cookies Policy [*insert link to MyC's cookie policy*], which sets out information about the cookies on the Platform.

If you make a Booking via our Platform, whether or not as a participant in a Pilot, our Terms of Supply [*insert link to Terms of Supply*] will apply to the Booking.

3. **We may make changes to these Terms**

We amend these Terms from time to time. Every time you wish to use our Platform, please check these Terms to ensure you understand the terms that apply at that time. These Terms were most recently updated on 17 February 2020.

4. **We may make changes to the Platform**

4.1 We may update and change the Platform from time to time, to reflect changes to the Services, our users' needs and our business priorities.

4.2 You acknowledge that the Platform is made available to you for the MyCorridor Project's research purposes. We do not guarantee that the Platform or any content on it will always be available or be uninterrupted. We may suspend or withdraw or restrict the availability of all or any part of the Platform at any time. We will try to give you reasonable notice of any suspension or withdrawal.

4.3 You are responsible for ensuring that all persons who access our Platform through your internet connection are aware of these Terms and other applicable terms and conditions, and that they comply with them fully.

5. **You must keep your account details safe**

5.1 Once you are provided with or create a user identification code, password or any other piece of information as part of our security procedures, you must treat such information as confidential. You must not disclose it to any third party.

5.2 Each user identification code is only permitted to be used by one individual. Only MyCorridor has the right to re-allocate user identification codes to new users.

5.3 We have the right to disable any user identification code or password, whether chosen by you or allocated by us, at any time, if in our reasonable opinion you have failed to comply with any of the provisions of these Terms.

5.4 If you know or suspect that anyone other than you knows your user identification code or password, you must promptly notify us at mycorridor@certh.gr.

6. **How you may use material on the platform**

6.1 We are the owner or the licensee of all intellectual property rights in our Platform, and in the material published on the Platform.

6.2 In consideration of you agreeing to abide by these Terms, we grant you a revocable, non-transferable, non-sublicensable, non-exclusive licence to access and use the Platform for your own personal, non-commercial purposes, relating to your browsing and Booking of Services, and for no other purpose.

6.3 You shall not copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any or all of the source code.

6.4 We may stop providing the Platform at any time and upon any termination, (a) the rights and licenses granted to you in these Terms will end; (b) you must stop using the Platform, and delete access to it from your device.

7. **Do not rely on information on this site**

Although we make reasonable efforts to update the information on the Platform, we make no representations, warranties or guarantees, whether express or implied, that the content on the Platform is accurate, complete or up to date.

8. **We are not responsible for websites we link to**

8.1 Where our Platform contains links to other sites and resources provided by third parties, these links are provided for your information only. Such links should not be interpreted as approval by us of those linked websites or information you may obtain from them.

8.2 We have no control over the contents of those sites or resources.

9. **Our responsibility for loss or damage suffered by you**

9.1 We do not exclude or limit in any way our liability to you where it would be unlawful to do so.

9.2 Different limitations and exclusions of liability will apply to liability arising as a result of the supply of the Services to you, which will be set out in our Terms of Supply.

9.3 Please note that we only provide the Platform for domestic and private use. You agree not to use our Platform for any commercial or business purposes, and we have no liability to you for any loss of profit, loss of business, business interruption or loss of business opportunity.

10. **We are not responsible for viruses and you must not introduce them**

10.1 We do not guarantee that our Platform will be secure or free from bugs or viruses.

10.2 You are responsible for configuring your information technology, computer programmes and platform to access our Platform. You should use your own virus protection software.

10.3 You must not misuse our Platform by knowingly introducing viruses, Trojans, worms, logic bombs or other material that is malicious or technologically harmful. You must not attempt to gain unauthorised access to our Platform, the server on which the Platform is stored or any server, computer or database connected to our Platform. You must not attack the Platform via a denial-of-service attack or a distributed denial-of service attack. By breaching this provision, you would commit a criminal offence under the Computer Misuse Act 1990. We will report any such breach to the relevant law enforcement authorities and we will co-operate with those authorities by disclosing your identity to them. In the event of such a breach, your right to use the Platform will cease immediately.

11. **Governing law and jurisdiction**

As a consumer or Pilot participant, these Terms are governed by the laws of England and Wales. You agree that the English Courts shall have jurisdiction to hear and determine any dispute arising from the interpretation of these Terms. However you may choose the law and jurisdiction of the country in which you reside.

Annex 1

MyCorridor Technical Partners

Centre for Research and Technology Hellas ("**CERTH**")

CERTH Hellenic Institute of Transport

CERTH Informatics and Telematics Institute

Italian TTS Association

AMCO Inspired Technologies

Viva Payments Services S.A

Salzburg Research SRFG

MAP Traffic Management

Swarco Mizar S.r.l

Chaps spol sro