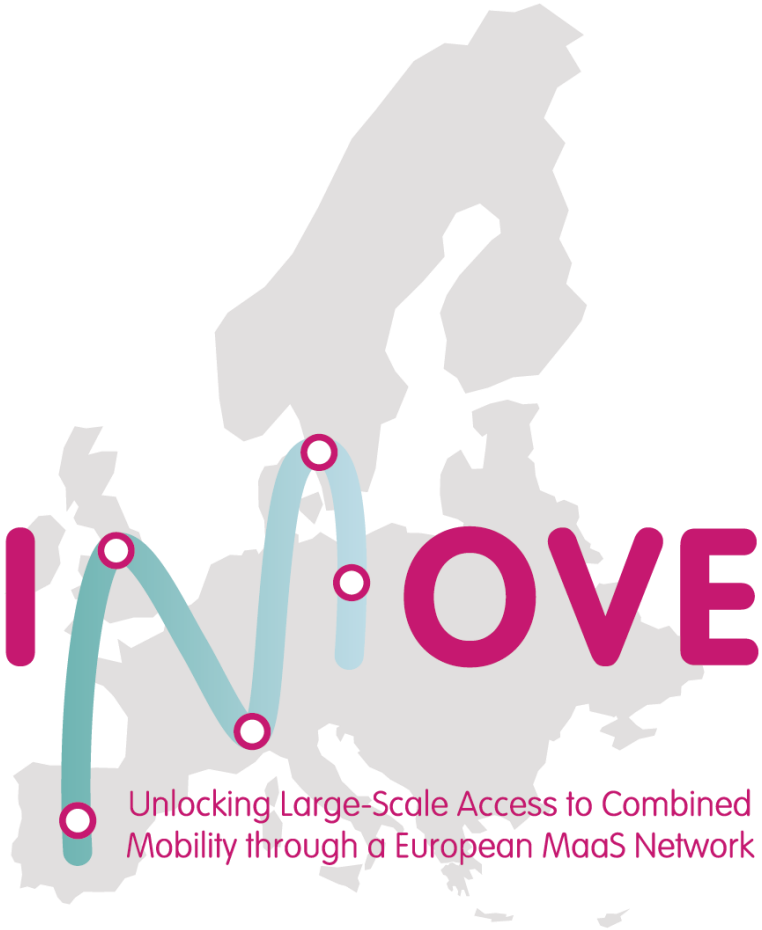

UNLOCKING LARGE-SCALE ACCESS TO COMBINED MOBILITY THROUGH A EUROPEAN MAAS NETWORK.

Deliverable D3.3
Ethics Compliance Report Final Version

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

The content of this report reflects only the authors' view. The Innovation and Networks Executive Agency (INEA) is not responsible for any use that may be made of the information it contains.

Deliverable D3.3
Ethics Compliance
Report Final Version

Due date of deliverable: 30/11/2019

Actual submission date: 29/11/2019

Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/06/2017 Duration: 30 months

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

Document Control Sheet

Deliverable number:	**D3.3**
Deliverable responsible:	Vectos (South) Limited
Work package:	WP3
Main editor:	Paul CURTIS

Editor name	Organisation
Paul CURTIS	Vectos (South) Limited
Laurie PICKUP	Vectos (South) Limited

Document Revision History			
Modifications Introduced			
Version	**Date**	**Reason**	**Editor**
1.0	30/04/2018	First Draft	Paul CURTIS
1.1	30/04/2018	Review	Vassilis PSALTOPOULOS
1.2	02/05/2018	Second Draft	Paul CURTIS
1.3	03/05/2018	Review	Laurie PICKUP
1.4	31/05/2018	Third Draft – following input from telco with WP3 partners	Paul CURTIS
1.5	31/05/2018	Review	Vassilis PSALTOPOULOS
2.0	25/10/2019	Final Draft	Paul CURTIS
2.1	04/11/2019	Final Draft – internal review	Laurie PICKUP
2.2	06/11/2019	Final Draft – release for external review	Paul CURTIS
2.3	25/11/2019	Final Version – following review and input from Living Lab partners	Paul CURTIS

Legal Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability to third parties for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. © 2017 by IMOVE Consortium.

This report is part of a project that has received funding by the European Union’s Horizon 2020 research and innovation programme under grant agreement number 723314.

Executive Summary

This Deliverable provides guidance to partners on the main requirements of the General Data Protection Regulation (GDPR). It also serves as a management tool through which partners can plan and deliver systems such that they adhere to the regulation's needs.

It contains checklists which should be reviewed by partners to see where procedures need to be put in place and where roles such as Data Protection Officers should be appointed.

The first draft was circulated to partners in May 2018 to equip them with the knowledge to put in place data protection measures. Section 7.1 has been updated in this final draft to include details of the ways in which GDPR compliance has been reached, the specific data handled, consent from users obtained and personal information kept private. It constitutes a selection of good practice examples which can be applied in other RIA and IA projects.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

Abbreviations and Acronyms

AB	Advisory Board
CA	Consortium Agreement
DDP	Deliverable Development Plan
DoA	Description of Action
EB	Executive Board
EC	European Commission
EoI	Expression of Interest
ERB	Ethics Review Board
GA	Grant Agreement
IPR	Intellectual Property Rights
LL	Living Lab
OSS	Open Source Software
PC	Project Coordinator
P/M	Person/Month
PMR	Periodic Management Report
PO	Project Officer
QMR	Quarterly Management Report
WP	Work Package

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

Table of Contents

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

List of Figures

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

List of Tables

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

INTRODUCTION

What is IMOVE?

Mobility as a Service (MaaS) is the future for urban transport. IMOVE aims to move the industry forwards into this future. Following recent mega-trends in the mobile and sharing economy and thanks to the latest ITS developments, MaaS schemes seek to solve how citizens move themselves and their goods. The wave will burst borders between different modes of transport, offering customers combined mobility packages as an alternative to own mobility and car ownership. A single subscription will deliver this door-to-door service, doing away with pockets full of tickets for the bus, train or other transport.

MaaS offers a mobility distribution model in which a single integrated service provider meets a passenger's individual needs with a customised service. The provider combines transportation infrastructure, travel information, payment services through one application. Today, MaaS schemes are disruptors with great potential, but a series of factors have hindered industry-wide take-off. So far, challenges have included public/private mobility integration, information handling and sharing, alongside service interoperability and scalability requirements. We now need specific action to usher in the future for transport. This is where IMOVE comes in.

Purpose of Ethics Compliance Report

To provide IMOVE partners with the information they need to understand what comprises personal data and the ways in which to ensure data privacy and protection during the project and hence compliance with the General Data Protection Regulation 2016/679. It was a working document which was initially circulated to partners in draft form in May 2018 in order to provide important guidance on how to proceed with the handling of data and putting in place measures to ensure GDPR adherence.

In this final version it also contains a summary of how the project adhered to the requirements of GDPR, especially noting the activities of the Living Lab partners where personal data was relevant. It includes details of the specific data handled (identified in the Local Data Management Plans), the systems set up to protect data and how permissions from users were sought and obtained.

It contains broader guidance for beneficiaries on GDPR.

The document is based on academic and regulatory sources as documented in the text and in the references. This reference to authoritative sources has been as comprehensive as possible and it represents the current state of best practice to the best of our knowledge.

The research ethics materials provided in this document relate to research across the whole of the project, the Pan-European inventory and the 'common information space'. They provide an account of the motivations, protocols and guides for an ethically sound research methodology and practice, as well as documents designed to obtain informed consent.

The document is written and compiled for the IMOVE project team, the European Commission, and relevant national Data Protection Authorities.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

1 EU LEGAL FRAMEWORK

1.1 HORIZON 2020 MAIN ETHICAL PRINCIPLES

All the research and innovation activities carried out under Horizon 2020 must comply with ethical principles and relevant national, EU and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection.

As such, projects will conduct research following these principles:

- Respect human dignity and integrity;
- Ensuring honesty and transparency towards research subjects - free and informed consent (as well as assent whenever relevant);
- Protect vulnerable persons;
- Ensure privacy and confidentiality;
- Promote justice and inclusiveness;
- Minimise harm and maximising benefit;
- Share benefits with disadvantaged populations, especially if the research is being carried out in developing countries;
- Respect and protect the environment and future generations;
- Follow highest standards of research integrity (i.e. avoid fabrication, falsification, plagiarism, double funding, etc.).

1.2 EU GENERAL DATA PROTECTION REGULATION

1.2.1 OBJECTIVES

It is billed as the most important change to data privacy regulation in 20 years. After four years of debate, the EU General Data Protection Regulation (GDPR) was approved by the European Parliament on 14 April 2016 and enforcement commenced in 25 May 2018. From this date, those organizations who do not comply may face the prospect of heavy fines.

The GDPR aims to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that had changed immeasurably from the time in which the preceding 1995 Directive was established, when online services for example were still in their infancy.

The GDPR replaces the Data Protection Directive 95/46/EC and is designed to:

- harmonize data privacy laws across Europe;
- protect and empower all EU citizens' data privacy; and

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

- reshape the way organizations across the region approach data privacy.

Two-thirds of Europeans, according to a recent Eurobarometer survey, stated they are concerned about not having complete control over the information they provide online. Seven Europeans out of ten worry about the potential use that companies may make of the information disclosed. The data protection reform will strengthen the right to data protection, which is a fundamental right in the EU, and allow them to have trust when they give their personal data. The new rules address these concerns by strengthening the existing rights and empowering individuals with more control over their personal data.

1.2.2 GLOSSARY OF KEY TERMS

- **Data Subjects** - natural persons whose personal data is processed by a controller or processor
- **Data Controller** - the entity that determines the purposes, conditions and means of the processing of personal data. They are responsible for ensuring appropriate security of the personal data and compliance with article 5 of the GDPR
- **Data Processor** - the entity that processes data on behalf of the Data Controller
- **Data Protection Officer** (DPO) - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR
- **Data Protection Authority** (DPA) - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the EU
- **Personal Data** - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person
- **Core Activities** – Primary business activities of an organisation, such that if it is necessary to process personal data to achieve key objectives, this is a core activity, and hence a DPO should be appointed.

1.2.3 MAIN CHANGES WITH PREVIOUS DIRECTIVE

Increased Territorial Scope

It applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location or where the processing takes place. The GDPR will also apply to the processing of personal data of data subjects in the EU by a data controller or data processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20m (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors - meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened such that the requests must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

and distinguishable from other matters, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

1.2.4 DATA SUBJECT RIGHTS

Right to access

Part of the expanded rights of data subjects is the right for them to obtain from the data controller confirmation whether their personal data is being processed and for what purpose. The controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Data Protection Officers

Under the GDPR, you must appoint a Data Protection Officers (DPO) if:

- you are a public authority (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

Even if you are not obliged to appoint a DPO, you may chose to do so in order to provide staff with ongoing support on compliance with legal requirements.

DPOs:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices;
- May be a staff member or an external service provider/ shared with other organizations;
- Contact details must be provided to the relevant DPA;
- Must be independent, an expert in data protection, adequately resourced, and report to the highest management level;
- Must not carry out any other tasks that could results in a conflict of interest.
- Tasks of the DPO:

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

- DPOs are tasked with monitoring compliance with the GDPR and other data protection laws, internal data protection policies, awareness-raising, training, and audits;
- DPOs act as a contact point for the Data Protection Authority.

Table 1. Checklist for DPO appointment

Check list item
☐ We are a public authority and have appointed a DPO (except if we are a court acting in our judicial capacity).
☐ We are not a public authority, and the nature of our processing activities does not require the appointment of a DPO. We have recorded this decision to help demonstrate compliance with the accountability principle.
☐ We have appointed a DPO based on their professional qualities and expert knowledge of data protection law and practices.
☐ We aren't required to appoint a DPO under the GDPR but we have decided to do so voluntarily, under the same duties and responsibilities.
☐ Our DPO has sufficient resources, is easily accessible as a point of contact for our employees, individuals and the Data Protection Authority. ☐ We have published the contact details of the DPO and communicated them to the Data Protection Authority.

Further info on DPOs from UK Data Protection Authority (ICO)

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

Breach Notification

Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach, this must be done within 72 hours. Will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals".

Privacy by Design

Privacy by design has existed for years but it is a legal requirement with the GDPR. It calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing. Additionally, data should only be stored for a strictly minimum period of time which is required to fulfil the task.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

2 AVOIDING HARM IN RESEARCH

2.1 AVOIDING HARM

Research should be conducted in a way that avoids harm to the data subject. This can be achieved through a detailed consent procedure and by adopting risk minimisation strategies. Informed consent form template is found in Annex 2 of Del 3.1.

One way of responding to the possibility of harming data subjects is by incorporating in the planning and running of the research, members of the public who are the focus of the work. A key barometer is to ensure participants are not worse off as a result of their involvement in the research, and to deliver research responsibly.

Research should also be designed in a way that maximises its relevance and benefit to society.

One must ensure that data subjects are protected from undue intrusion, distress, indignity, physical discomfort, personal embarrassment, legal exposure or psychological harm.

- **Legal Harm** – if you are likely to gather information about an individual's illegal behaviour, confidentiality is even more crucial.
- **Physical Harm** – for some research, the participants' health may be a factor to consider before including in a pilot for instance.
- **Psychological Harm** – data subjects may sometimes feel they are put in an uncomfortable situation to take part in the research. This can be overcome through an appropriate consent procedure, including a debriefing after the study.
- **Environmental Harm** – research should not have a detrimental impact on the environment, this can include measures to travel sustainably or minimise printing.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

3 ETHICS SELF-ASSESSMENT

3.1 HUMAN BEINGS

For the purposes of the IMOVE project, the area of ethical concern relates to human beings (data subjects) and the handling of their personal data, specifically that which emanates from the Living Labs. As a result, the principles for adhering to ethical standards are embedded in the GDPR.

Ethical principles provide the basis for conducting the action at city and project levels. The obligation on all beneficiaries is to ensure that the project completes its work without breaching the integrity of the research: for example, that the evidence produced is based on sound analysis and rational argument, that the work was conducted in a professional and fair manner, that the evidence was not biased and that there was no misconduct in the way the research was undertaken.

Ethical legislation at national, European and international levels will provide the basis for any research activities in IMOVE. Necessary consent and approvals will be obtained prior to any research on humans being undertaken in the IMOVE Living Labs.

The Charter of Fundamental Rights of the EU states (legally binding since 2009) the fundamental rights of humans protected in the EU: Dignity, Freedoms, Equality, Solidarity, Citizens' Rights, and Justice. The Charter is a very modern codification and includes 'third generation' fundamental rights, such as data protection. This right to data protection builds on Article 8 of the Convention for the protection of rights defining respect for privacy and Article 2 of the respective Protocol defining the right to freedom of movement. The project will ensure full compliance with the Charter.

3.2 PERSONAL DATA

Living Labs manage personal data related to the final users (profile, preferences, user patterns, subscription and tariff scheme, etc.) and data related to the services offered (mobility offer, timetables, vehicles availability, etc.). It is the data regarding the users which is of highest sensitivity, such as from mobile phone apps.

The precise types of data to be collected and processed are presented in the Data Management Plan (D3.1) and the subsequent Local Data Management Plans.

Primary data used for sampling for quantitative analysis should ensure that the approach can generate a sample that is random and of a size that can be analysed with the ability to make statistical inference for the overall sample and for the most significant sub-sample breakdowns; in order to ensure accuracy and integrity.

Secondary data sources are primarily collected for public use and for multiple uses – such as local population census material. The city authority collects other data for local planning purposes, for example travel pattern data; which are for multiple uses within the city authority, but which require permission for wider use. These data will be essential for establishing the local contexts within which the IMOVE measures will be implemented. They can provide essential data for sampling people to ensure a full cross-section of city areas or types of people are surveyed.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

3.3 ENVIRONMENT, EMPLOYMENT, HEALTH AND SAFETY

Central features which guide the sustainable mobility objectives in all of the Living Labs are to use mobility to provide greater access to jobs and services, improve health and enhance environmental quality for a better quality of life.

3.4 SOCIETAL IMPACTS

Where possible the project will manage data in a way that furthers more inclusive mobility. Specific attention will be given to understand the user needs of vulnerable groups, women and older people which could provide valuable insight into the way in which MaaS services can be designed and delivered to ensure accessibility for all. MaaS services should seek to avoid discriminatory impacts against certain groups of the community.

3.5 POTENTIAL MIS-USE OF RESEARCH RESULTS

The risk of potential misuse of research results can be substantially minimised by recognising risks in good time and taking adequate measures. The main areas of concern regarding potential misuse to the IMOVE project include:

- research involving the development of surveillance technologies that could result in negative impacts on human rights and civil liberties;
- research on minority or vulnerable groups and research involving the development of social, behavioural or genetic profiling technologies that could be misapplied for stigmatisation, discrimination, harassment or intimidation;
- research providing knowledge, materials and technologies that could be adapted for criminal/terrorist activities.

There are various ways to mitigate risk, depending on the planned activity beneficiaries may choose to:

- take additional security measures, e.g. physical security measures, classification of certain deliverables, compulsory security clearance for those involved in project;
- take additional safety measures, e.g. compulsory safety training for personnel;
- adapt the research design: e.g. use dummy data;
- limit dissemination: e.g. partial publication of the research results, regulating export.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

4 ETHICS CHECK

4.1 ETHICS SELF-ASSESSMENT

At the application stage, IMOVE declared that the research would involve **personal data collection** and/ or processing; specifically that it will involve tracking or observation of participants as well as processing of previously collated personal data (secondary use).

The EC provides an Ethics Self-Assessment checklist to help beneficiaries deal with ethical issues taking preventative or corrective measures. This can also act as a useful 'Ethics Check' indicating areas of a project to be monitored with consents and certificates needed to be evidenced to show compliance to the GDPR.

The details gathered will form part of the final version of this report Del 3.3 and so it is important that the suggested documents to be evidenced are sourced at an early stage. This underlines the importance of assigning the roles of Data Protection Officer, Data Processor and Data Controllers. More details (including templates for consent form and participant information sheets) are found in Del 3.1.

Table 2. Ethics Self-Assessment checklist – Personal Data Protection

PERSONAL DATA QUESTION	Y/N	If Y: Information to be provided	If Y: Documents to be provided/kept on file
Does your research involve personal data collection and/or processing?		Details of your procedures for data collection, storage, protection, retention, transfer, destruction or re-use (including, collection methodology (digital recording, picture, etc.), methods of storage and exchange (LAN, cloud, etc.), data structure and preservation (encryption, anonymisation, etc.), data merging or exchange plan, commercial exploitation of data sets, etc.). Details of your data safety procedures (protective measures to avoid unforeseen usage or disclosure, including mosaic effect, i.e. obtaining identification by merging multiple sources). Confirm that informed consent has been obtained. Details of data transfers to non-EU countries (type of data transferred and country to which it is transferred).	Copies of notifications / authorisat-ions for collecting and/or processing the personal data (if required). Copies of procedures Informed Consent Forms + Information Sheets + Other consent documents (opt-in processes, etc.) (if relevant). Copy of authorisation for data transfer to non-EU country (if required)
Does it involve the collection or processing of sensitive personal data (e.g. health,			Copy of notification/authorisation for processing sensitive data (if required)

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?			
Does it involve tracking or observation of participants (e.g. surveillance or localization data, and Wan data, such as IP address, MACs, cookies etc.)?		Details of methods used for tracking or observing participants.	Copy of notification/authorisation for tracking or observation (if required).
Does your research involve further processing of previously collected personal data ('secondary use') (including use of pre-existing data sets or sources, merging existing data sets, sharing data with non-EU MS)?		Details on the database used or of the source of the data. Details of your procedures for data processing. Details of your data safety procedures (protective measures to avoid unforeseen, usage or disclosure, including mosaic effect, i.e. obtaining identification by merging multiple sources). Confirm that data is openly and publicly accessible or that consent for secondary use has been obtained (and details of how this consent was obtained (automatic opt-in, etc.)). Confirm permissions by the owner/manager of the data sets.	Evidence of open public access (e.g. print screen from website). Informed Consent Forms + Information Sheets + other consent documents (opt in processes, etc.). Copies of permissions (if required).

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

5 ETHICS AUDIT

5.1 AUDIT REQUIREMENTS

It should be noted that if ethical principles are substantially breached, the Commission reserves the right, as per the terms of the Grant Agreement, to conduct an 'Ethics Audit' during the project whereby, if concluded to be necessary:

- The Grant Agreement may be amended;
- The Grant may be reduced;
- The Grant may be terminated; and
- Other appropriate measures may be implemented, in accordance with Grant Agreement.

In order to comply with the Grant Agreement, beneficiaries must ensure that persons carrying out research tasks:

- present their research goals and intentions in an honest and transparent manner;
- design their research carefully and conduct it in a reliable fashion, taking its impact on society into account;
- use techniques and methodologies (including for data collection and management) that are appropriate for the field(s) concerned;
- exercise due care for the subjects of research — be they human beings, animals, the environment or cultural objects;
- ensure objectivity, accuracy and impartiality when disseminating the results;
- allow — in addition to the open access obligations under Article 29.3 as much as possible and taking into account the legitimate interest of the beneficiaries — access to research data, in order to enable research to be reproduced;
- make the necessary references to their work and that of other researchers;
- refrain from practicing any form of plagiarism, data falsification or fabrication; and
- avoid double funding, conflicts of interest and misrepresentation of credentials or other research misconduct.

The beneficiaries must respect the highest standards of research integrity — as set out, for instance, in the European Code of Conduct for Research Integrity. This implies notably compliance with the following essential principles:

- honesty;
- reliability;
- objectivity;
- impartiality;
- open communication;
- duty of care;
- fairness; and
- responsibility for future science generations.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

6 IMOVE ETHICS

6.1 IDENTIFICATION OF ANY POTENTIAL ETHICAL ISSUES

This section presents the specific types of data handled in the project, the procedure for data collection and how this process complied with GDPR requirements.

The specific data types being handled during the project are presented in the Local Data Management Plans. The Living Labs in WP4 handled the most sensitive data types which required careful management.

It includes the main findings and recommendations to INEA on forward strategies for addressing the ethical dimension of the Horizon Programme, and to the IMOVE cities.

IMOVE Ethics Compliance Table

The data types listed in the Local Data Management Plans were considered by the Data Manager, and those that were of a personal nature were flagged to put in place procedures to ensure GDPR adherence.

The draft D3.3 was circulated to partners in May 2018 in order to provide guidance on GDPR compliance from the outset. This included the example Ethics Compliance Table which was used to by city partners to develop the local data management plans, and to identify specific data they plan to handle. The table below shows an example table which was presented to partners during the Ethics Review Board meeting to raise understanding of the types of data that would require mitigation measures to ensure protection and privacy.

Table 3. Ethics Compliance Table - example

Type of data	Procedure for data collection	Data management / storing	Who else has access to data?	How comply with GDPR?
Passenger names, credit cards, addresses, age	Online / app registration	Public Transport Authority Database	n/a	Data anonymized
Passenger modal choice	Entries and exits of public transport	Public Transport Authority Database	IMOVE beneficiaries	Data anonymized
Passenger attitudes and travel behaviour	Questionnaires	Stored in office / Database	IMOVE beneficiaries	Informed consent forms. DPC

During the project the Ethics Review Board, convening at project meetings, supported project partners through presentations and discussions in determining where and how data should be handled in a way consistent to the GDPR.

6.1.1 TURIN

Specific types of data handled in the project

From the outset, 5T and Urbi identified a variety of personal data including:

- passenger personal information (name, address, phone number, email);
- public transport purchases;
- car sharing and taxi reservations and trips made;

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

- bike sharing trips;
- mobility subscription information;
- payment and billing information;
- company profiles;
- lifestyle and travel habits of participants before and after the Living Lab trials.

The procedure for data handling

The way in which such data was collected was primarily through the use of the mobile phone application. This includes the registration form and then subsequently via tracking of entry and exit of public transport services. This also includes the user surveys by participating company staff at General Motors workplace.

Urbi was responsible for the collection and storing of passenger personal information from the app, whereas public transport and other mobility companies were jointly responsible for data pertaining to use of their services, such as boarding and alighting from bus or using car sharing. 5T was responsible for the collection, processing and storing of data emanating from the user surveys.

How this process complied with GDPR requirements.

The purposes for data sharing were to understand and compare the travel habits of citizens (employees) and before and after the Living Labs. To ensure adherence with GDPR, data is generally stored with suitable protections on the servers and cloud servers of the mobility providers, the local authority, 5T and the living lab operator Urbi. Data is anonymised before sharing.

A procedure was put in place to allow the user to request the deletion of data at any time.

With regards to the sensitivities of participant journeys and modal choices being tracked by the app, the pilot workplace General Motors is not allowed by labour law to track such employee movements. This meant they were able to naturally comply with GDPR. As such Urbi was responsible for user tracking and only shared with General Motors the rankings of the users so that awards could be made. In terms of the employee surveys of travel options, neither General Motors nor Urbi were permitted access to the primary data: instead 5T shared the data in an aggregated and anonymous format to ensure protection.

Examples of policies and procedures, informed consent, anonymising etc

With regards to the user survey completed by participating staff members, they were invited to complete the questionnaire online via http://www.5t.torino.it/imove/index.php/851323?lang=it-informal then after logging in (with username and password) the following message informs the user of the nature and scope of the survey:

- *"The questionnaire intends to investigate the mobility habits of the participants at the IMOVE Living Lab in Turin with General Motors. This information will be used for statistical purposes and will be shared anonymously between the IMOVE project partners. For more information on data processing, refer to the privacy policy attached to the application for participation in the IMOVE trial (compliant with European Regulation n. 2016/679)."*

It continues:

- *"ATTENTION: To register for the Living Lab, the application must be submitted to GM's Mobility Manager. The compilation of the survey is essential to access the established awards but its compilation DOES NOT CONSTITUTE adhesion to the IMOVE Living Lab. The user may at any time happen the rights provided for by the articles from 15 to 22 of the EU regulation 679/2016 (Right of access by the data subject, Right to rectification, Right to erasure, Right to restriction of processing, Notification obligation regarding rectification or erasure of personal data or restriction of processing, Right to data portability, Right to object and automated individual decision-making)"*

The diagram below illustrates the procedure for data handling and GDPR compliance.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

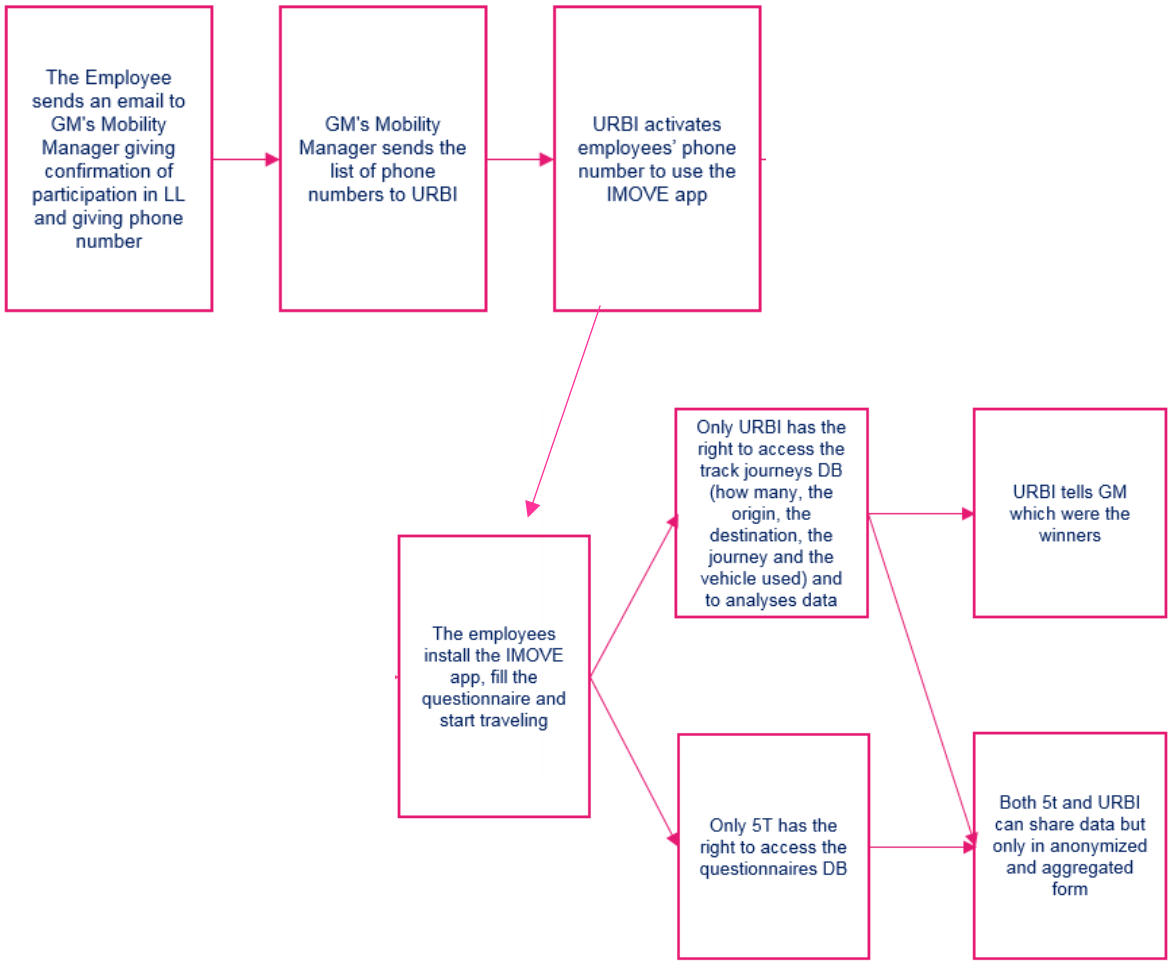

Figure 1. Data handling procedure: adhering to GDPR

Conclusions

Urbi's previous experience in data privacy through the app meant the policies and understanding were in place to ensure adherence to GDPR. The existing national policies on data protection – such as companies not being able to track the movements of their employees – acted as a support to this adherence.

6.1.2 MANCHESTER

Specific types of data handled in the project

From the outset, TfGM identified a variety of personal data including:

- passenger personal information (name, address, phone number, email)
- public transport purchases
- car sharing and taxi reservations and trips made
- bike sharing trips
- mobility subscription information
- user origin and destination data

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

- payment and billing information
- lifestyle and travel habits of participants before and after the Living Lab trials
- personal travel behaviour

The procedure for data handling

The way in which data was collected and processed was primarily through the Mobilleo mobile phone application. For example, passengers tapping in and out of a mobility service, making bookings and the geo-location services of the app. The registration and booking form was also accessible via the Mobilleo website. Such information falls primarily under the responsibility of Mobilleo (the mobility operator and app developer) in terms of data management, but also with car club and taxi companies as participating mobility service providers.

In addition, the screening questionnaire was sent to 200 users to capture travel behaviour information. TfGM are the responsible body for collecting and processing this data and it is stored on the TfGM local server.

How this process complied with GDPR requirements

TfGM undertook a Data Protection Impact Assessment internally to understand the data being collected during the project and how it was being shared with the service providers and project partners.

Regarding the information on individual travel behaviour, TfGM ensures that all data is anonymised by removing unique identifiers and that each user is assigned with a unique user ID. Once anonymised the data is saved in a password protected file and can be shared with other project partners with no exposure to risk.

Mobilleo and participating car share, ride hailing and taxi companies are also fully compliant to GDPR and other data security standards as is part of their terms of reference.

Information sharing agreements and terms and conditions have been set up between TfGM, Mobilleo and the participating mobility operators, specific to the IMOVE trials, setting out how data will be used and protected as well as defining the specific procedures for data sharing between different entities.

Examples of policies and procedures, informed consent, anonymising etc

As a public transport authority, TfGM has an appointed Data Protection Officer in place who was consulted as part of this process including conducting a compliance check and completion of a Data Protection Impact Assessment.

As part of the survey process, TfGM issued a Privacy Notice which clearly sets out the purposes for data collection and methods of processing.

Mobilleo's terms and conditions clearly set out the definition of Personal Data namely:

- *"Personal Data" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard, to the processing of personal data and on the free movement of such data, in this instance in relation to Travellers; and from 24th May 2018 will reflect the General Data Protection Regulations;*

Mobilleo's privacy policy enshrines the components of GDPR such as the rights to data erasure, the right to be informed about the purpose of data collection and that no data will be shared without prior permission being granted.

Conclusions

As a public transport authority TfGM has well established procedures in place for protecting personal data and was supported closely with their in-house DPO to ensure GDPR compliance.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

6.1.3 BERLIN

Specific types of data handled in the project

In the same way as the other living labs, there was a variety of personal data identified from the outset including:

- passenger personal information (name, address, phone number, email);
- public transport purchases;
- car sharing and taxi reservations and trips made;
- bike sharing trips;
- mobility subscription information;
- mobility preferences;
- payment and billing information;
- personal travel behaviour.

The procedure for data handling

Data collection is derived from entry and exit of public transport modes, usage of the app and completing the registration form online or on the app.

There are a number of responsible organisations for the collection and processing of data. namely: public transport operators, shared mobility providers, taxi companies, the local authority and Urbi the MaaS provider. In terms of data management and storage, this is the role of Urbi.

Surveys were delivered by Urbi to capture the travel behaviour of participating individuals, the data from which is stored on their cloud servers and is only accessible by them.

How this process complied with GDPR requirements

The surveys only collect phone numbers in order to associate the results to specific travel behaviours (i.e. the rest of the actual mobility data collected during the pilot)

Examples of policies and procedures, informed consent, anonymising etc

The app gives users an “in-app data cancellation request” allowing them to withdraw their consent at any time and for their data to be deleted. The Privacy Policy is made available on the app. See foot of images below.

This report is part of a project that has received funding by the European Union’s Horizon 2020 research and innovation programme under grant agreement number 723314.

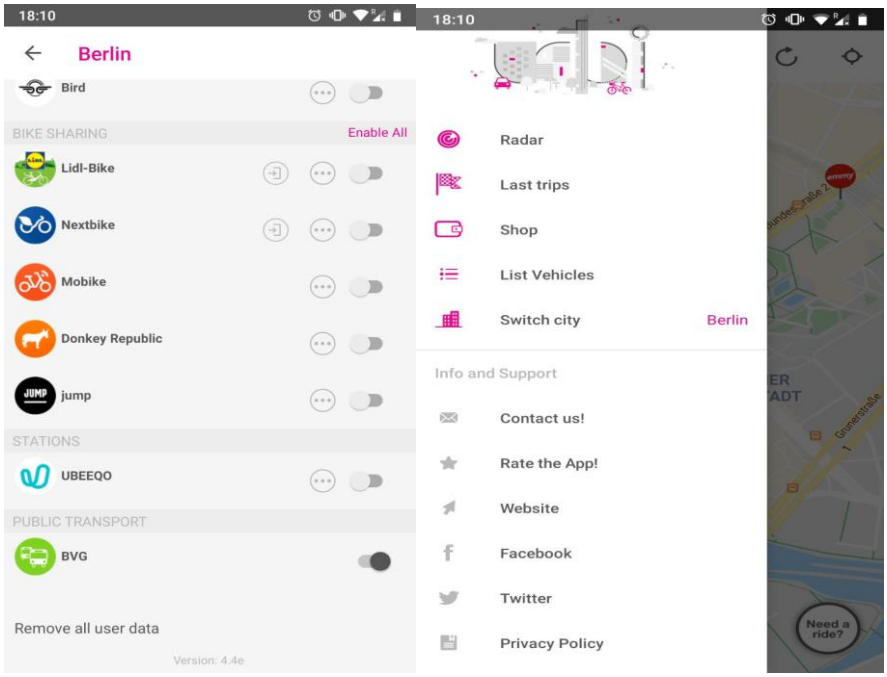

Figure 2. Privacy policy and right to withdraw consent functions on the application

The survey is subject to the same privacy policy of the app, since the responsible for data management is the same (Urbi). The terms and conditions plus the privacy policy is presented to the user is located at https://www.urbi.co/privacy/ and acceptance is undertaken upon registration (see image below).

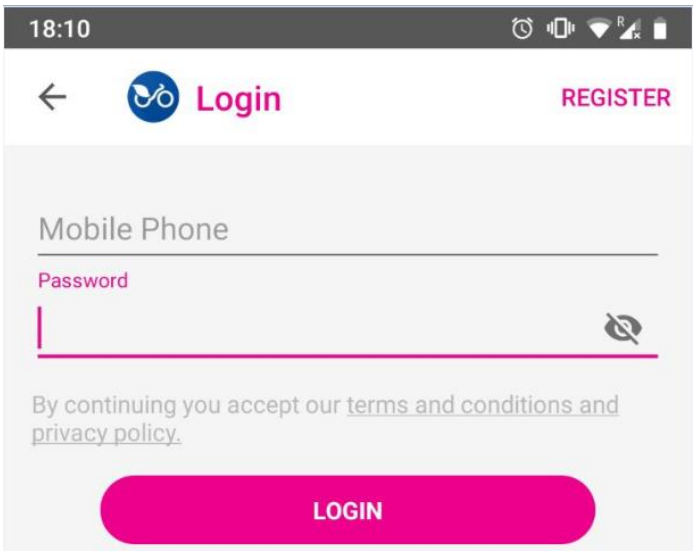

Figure 3. Gaining consent from the user to participate as per the Terms, Conditions and Privacy Policy

The survey, via the phone number (the only sensible information collected) is associated with the relative Urbi user account and therefore subject to the same data retention policies. If the user will request cancellation of its account from the platform, the survey data will be deleted together with mobility data.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

Conclusions

The presentation of data protection policies in prominent locations on the application gives participants clear information which was easy to find, ensuring their consent was suitably gained.

6.1.4 GOTHENBURG

Specific types of data handled in the project

The following types of personal data were identified by the Gothenburg Living Lab as being relevant for their pilot activities:

- passenger personal information (name, address, phone number, email);
- public transport purchases;
- car sharing and taxi reservations and trips made;
- bike sharing trips;
- mobility subscription information;
- mobility preferences;
- payment and billing information;
- personal travel behaviour.

The procedure for data handling

With regards to public transport tickets, Västtrafik records the number of purchases made by third party resellers. These resellers monitor public transport ticket sales via their own apps and database. As such Västtrafik, Trivector, Smartresenär and P-bolaget are responsible for data collection, processing, management and for storing it on their own databases.

User travel patterns are monitored through the KOMPIS framework namely through before and after surveys of individual users. Local business trip data has been collected by RISE whereas information pertaining to the residential pilot was collected by a researcher from Chalmers via interviews, in collaboration with Trivector.

In both cases, the data is managed and stored on the KOMPIS database managed by RISE and steps taken to ensure data is aggregated before sharing with other projects. Every pilot owner (i.e. the organisation managing and running the pilot) is responsible for ensuring that data security procedures comply with GDPR.

How this process complied with GDPR requirements.

It is possible to trace individual public transport tickets but there is no personal information attached such as passenger names or contact details. Rather, each ticket has a digital ID and thus eliminates any potential risk of data privacy.

The results of the customer survey indicating mobility preferences will be made public, but no data will be traceable to individual users and so will be GDPR compliant.

On the whole, Västtrafik gains access to aggregated statistics.

Examples of policies and procedures, informed consent, anonymising etc

The terms of use for EC2B are clearly set out with contact details for more information clearly presented.

Conclusions

From the outset, protocols were agreed between Västtrafik and the two organisations collecting survey information (RISE and Trivector) to ensure that data was normally aggregated before sharing with Västtrafik. This was a successful approach to ensuring adherence to data protection

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

6.1.5 MADRID

Specific types of data handled in the project

The Madrid Living Lab identified the following areas of personal data handled in the pilot:

- Cable car service;
- Fast EV CPs;
- GPS tracks MaaS users;
- BiciMad;
- Bus Madrid Validations;

The procedure for data handling

As leader of the pilot, EMT is responsible for data collection with support from Mosaic Factor. Data is stored securely on servers from both organisations comprising both local and the cloud.

The app was developed by an external company (IECISA). This meant that agreements were made with EMT to ensure their data protection policy was fit for purpose.

How this process complied with GDPR requirements

EMT paid careful consideration to issues surrounding data protection especially regarding the potentially delicate issue of GPS tracking of MaaS application users. This fed into the design specification of the application. In this case including a tick box for the users to select to declare that they accepted to be tracked as part of the pilot. Due to unforeseen difficulties in the development of the preproduction version of the app (Beta version), which was initially estimated to be delivered by 25/09/2019, and the subsequent delay in the final production version, together with last minute issues regarding the General Data Protection Regulation (GDPR) internal EMT procedures, the final testing has been carried out by using only internal resources (EMT and IECISA employees).

Users were recruited via email. They were provided with instructions and an anonymous survey to fill in. The result was 20 users agreeing to these terms and therefore enabling EMT to handle the ensuing data.

Examples of policies and procedures, informed consent, anonymising etc

When registering on the EMT user ID manager platform (EMTing), users are requested to accept the terms and conditions "*Acceptar términos y condiciones de uso*". Following this step, users chose whether or not they wish to have their journeys monitored "*Registrar mis recorridos*" or "*Recibir comunicaciones de EMT*", in both cases, followed by the double acceptance indicated by the GDPR.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

This is illustrated in the images below from the application.

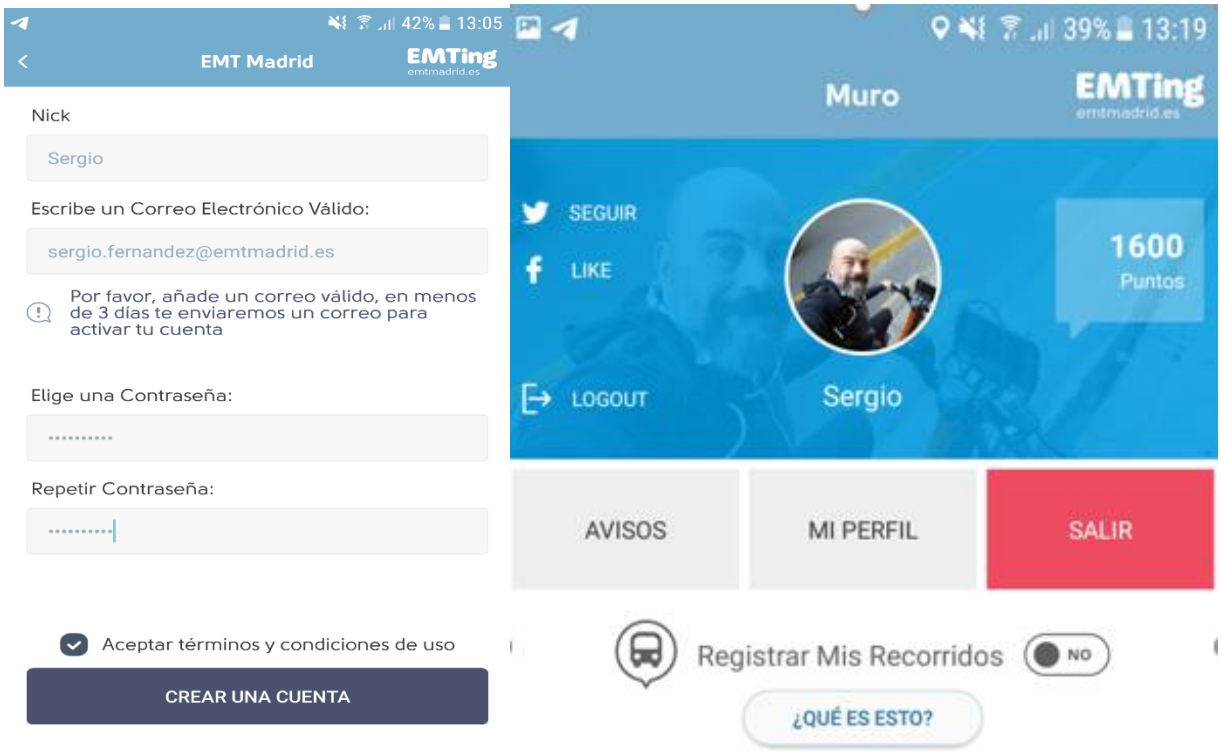

Figure 4. Informed Consent Procedure

The terms and conditions if accepting to be tracked are clearly set out, whereby upon opening the app, journeys will be tracked for the first 90 minutes.

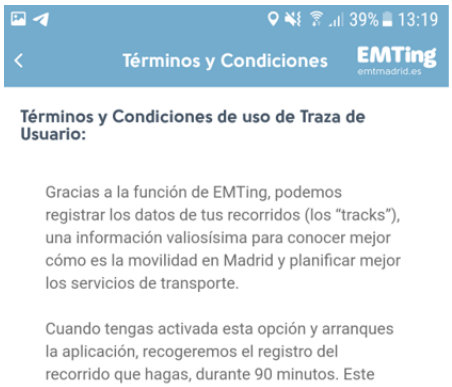

Figure 5. User terms and conditions

In addition, the usage of MaaS Madrid is subject to the following Privacy Policy (link[1]) which is available in the "*Acerca de*" section of the app and EMT website, and adheres to GDPR principles.

[1] https://www.emtmadrid.es/Elementos-Cabecera/Enlaces-Pie-horizontal/Privacidad-y-cookies

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

6.2 HANDLING OF ETHICAL ASPECTS

All beneficiaries should consider - where relevant - assigning the roles of Data Controller and Data Processor within their organizations, and whether they require appointing a Data Protection Officer. This is likely to be most relevant for the Living Lab partners, but all beneficiaries who have a role to process and analyse data collated for other parts of the project should also consider these requirements. Guidance is provided in Section 2 above and further advice in national languages can be sought from relevant National Data Protection Authorities[2].

The first source should always be with one's own organisation. The EC recommends that at the first instance, beneficiaries seek advice from colleagues with expertise in the ethics of research, such as:

- specialised ethics departments;
- relevant managers in your university/research organisation;
- hospital research ethics committees;
- ethics advisers in your company;
- data protection officers.

They should be able to provide you with information appropriate to your specific needs and legal environment.

6.3 ADDRESSING ETHICAL ASPECTS IN SUFFICIENT DETAIL

Local Data Management Plans will contain all types of data to be handled, collated, analysed or stored. The IMOVE Data Manager (Jose Fernandez, MOSAIC) will review these and flag to the sites and the Ethics Review Board where measures should be taken to ensure adherence to the GDPR. For example, obtaining Consent Forms, Data Protection Certificates or seeking advice from Data Protection Authorities. It is the role of the Ethics Review Board to ensure these permissions are sought in a timely fashion.

[2] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

7 IMOVE ETHICS REVIEW BOARD

7.1 ETHICS REVIEW BOARD

- Implement and refine the Ethics Compliance Report as drafted and updated during the project.
- Ensure that all necessary national, EU and international ethics approvals and opinions are obtained in all pilot countries prior to the commencement of the work, during the planning phase (for example national data protection authorities or under GDPR).
- Mentor all project beneficiaries on the ethical obligations of the project, including at subsequent consortium meetings.
- Conduct periodic reviews of ethics in preparation for EC ethical audits and produce full documentation for INEA observation.
- Periodic reporting to INEA on ethics compliance and issues that have arisen and been addressed, plus anticipated issues for later in the project as part of the management reporting.

The ERB is composed of the Chair, one representative from the Living Labs, the WP leaders, the Coordinator and the Data Manager, hence: VECTOS (Chair), SOFTECO, MOSAIC (Data Manager), UITP, ICCS, 5T, TFGM, VASTTRAFIK, URBI, VIKTORIA.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

CONCLUSIONS

The experience of the Living Labs has provided insight into common and less common issues arising regarding GDPR and how adherence is achieved.

In Turin Urbi's previous experience in data privacy through the app meant the policies and understanding were in place to ensure adherence to GDPR. The existing national policies on data protection – such as companies not being able to track the movements of their employees – acted as a support to this adherence.

As a public transport authority in Manchester, TfGM has well established procedures in place for protecting personal data and was supported closely with their in-house DPO to ensure GDPR compliance.

In Berlin, the presentation of data protection policies in prominent locations on the application gives participants clear information which was easy to find, ensuring their consent was suitably gained.

In Gothenburg, from the outset, protocols were agreed between Västtrafik and the two organisations collecting survey information (RISE and Trivector) to ensure that data was normally aggregated before sharing with Västtrafik. This was a successful approach to ensuring adherence to data protection

In Madrid, EMT ensured adherence to GDPR principles, notably for gained consent for journeys to be tracked, thanks to a well-defined app specification, provide to the developer so that it was integrated into the service from the outset. This was a successful approach.

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement number 723314.

REFERENCES

[1] Gorini, Marco, Freixanet, Josep, Fernandez, José. “D7.1 - Project Handbook”. *IMOVE project deliverable*, released 31/08/2017.

[2] GDPR 2018: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en

[3] Ethics Audit: http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm

[4] Avoiding Harm: http://dissertation.laerd.com/principles-of-research-ethics.php#first

[5] Avoiding Harm: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[6] Data types: https://keydifferences.com/difference-between-primary-and-secondary-data.html#KeyDifferences

[7] Data types: https://www2.le.ac.uk/offices/red/rd/research-methods-and-methodologies/intrepid-researcher/methods/2010-11/combining-primary-and-secondary-data-opportunities-and-obstacles

[8] Potential mis-use of data: https://ec.europa.eu/research/participants/portal/doc/call/h2020/fct-16-2015/1645168-explanatory_note_on_potential_misuse_of_research_en.pdf

[9] European Code of Conduct for Research Integrity: http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

[10] Information Commissioner’s Officer: https://ico.org.uk/

This report is part of a project that has received funding by the European Union’s Horizon 2020 research and innovation programme under grant agreement number 723314.