SHared automation Operating models for Worldwide adoption

SHOW

Grant Agreement Number: 875530

D3.5: Final SHOW Ethics manual & Data Protection Policy and Data Privacy Impact Assessment

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 875530

Legal Disclaimer

Executive Summary

The SHOW project aims to support the migration path towards effective and persuasive sustainable urban transport through technical solutions, business models and priority scenarios for impact assessment, by deploying shared, connected, electrified fleets of automated vehicles in coordinated Public Transport (PT), Demand Responsive Transport (DRT), Mobility as a Service (MaaS) and Logistics as a Service (LaaS) operational chains in real-life urban demonstrations. Demonstration and evaluation activities will be done in 11 Mega and Satellite sites throughout Europe (smaller scale trials are also targeted in some of the follower sites in addition). SHOW is a user-oriented project where the participation of humans is essential for a successful outcome. A sound and correct ethical treatment of participants and their safety is therefore of great importance for SHOW. Along with that, compliance with GDPR principles, on project level but also on local site level, is also mandatory.

This deliverable is the final version of the Ethics Manual and Data Protection Policy for SHOW and constitutes an update of the former version, D3.4.

To assure continuous monitoring and control in the project, a living Ethics Board (EB) has been established from the start of the project, led by VTI, including the Local Ethics Representatives assigned at test site level.

The objective with this final update of the Deliverable is to provide the final version of the Ethics Manual and Data Protection Policy for the SHOW project. With respect to the previous version, the questionnaire on ethical and legal issues - formalised as a process since the beginning of the project for the sake of ethics monitoring across the test sites – has been completed for the test sites of SHOW in view of the “final demo phase” upcoming (in the former D3.4 version, the same questionnaire had been completed in view of the “pre-demo” phase). In addition, the central to the project Data Privacy Impact Assessment (DPIA) has been updated, whereas the need for conducting local DPIAs at the test sites, in accordance with GDPR, has been recognised and discussed in a new section. It is recommended that the DPIA part of the current Deliverable is read in conjunction with the also updated in this period Data Management Plan of the project (the so-called *D14.3: DMP – final version*).

Document Control Sheet

Start date of project:	01 January 2020
Duration:	48 months
SHOW Del. ID & Title:	Deliverable 3.5: Final SHOW Ethics manual, Data Protection Policy and Data Privacy Impact Assessment
Dissemination level:	PU (for Public)
Work package:	WP3
Lead authors:	Anna Anund (VTI)
Other authors involved:	Louise Dahlgren (VTI), Maria Gkemou (CERTH/HIT), Ma Loukea (CERTH/HIT),
Internal Reviewers:	Nikos Tsampieris, ERTICO Maria Gkemou, CERTH/HIT
External Reviewers:	NA
Due submission date:	31/12/2021
Actual submission date:	16/02/2022
Status:	SUBMITTED
File Name:	SHOW_D3.5_SHOW Final Ethics manual_SUBMITTED

Document Revision History

Version	Date	Reason	Editor
0.1	14/11/2021	First draft ready Requests for ethics questionnaire update & local DPIAs	Anna Anund (VTI) Maria Gkemou, Matina Loukea (CERTH/HIT)
1.0	14/12/2021	First consolidation upon results, central to the project DPIA update	Maria Gkemou, Matina Loukea (CERTH/HIT), Alexis Papadopoulos (CERTH/ITI)
1.1	31/01/2022	Version sent for peer review	Anna Anund (VTI)
2.0	16/02/2022	Final version sent for submission	Anna Anund (VTI), Matina Loukea, Maria Gkemou, (CERTH/HIT)

Table of Contents

List of Tables

List of Figures

Abbreviation List

Abbreviation	Definition
ADAS	Advanced Driver Assistance Systems
AEE	Advisory Ethical Expert
CCAV	Collaborative Connected Autonomous Vehicle
CEN	European Committee for Standardization
DMP	Data Management Plan
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPP	Data Protection Policy
DRT	Demand Responsive Transport
EB	Ethics Board
ECHR	European Court of Human Rights
EEA	the European Economic Area
EGE	European Group on Ethics in Science and New Technologies
EM	Ethical Manager
ETSC	European Telecommunications Standards Institute
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Counc 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation)
ICO	Information Commissioner's Office
ID	Identification
IF	Incidental Findings
ISO	International Organization for Standardization
IT	Information Technologies
ITS	Intelligent Transport System
KPI	Key Performance Indicator
LaaS	Logistics as a Service
LER	Local Ethics Representatives
MaaS	Mobility as a Service
OEM	Original Equipment Manufacturer
PIA	Privacy Impact Assessment
POPD	Protection Of Personal Data
PT	Public Transport
QM	Quality Manager
SES	Socio Economic Status
SME	Small and Medium-sized Enterprise
SSL	Secure Sockets Layer
TC	Traffic Control
UC	Use Cases
UN	United Nations
VEC	Vehicle Electric Centre

1 Introduction

1.1 Purpose and structure of the document

The final Ethics Manual, here named *D3.5: Final SHOW Ethics manual, Data Protection Policy and Data Privacy Impact Assessment* describes the Ethical Code of Conduct for all actions and activities related to evaluations within SHOW.

Although the current version stands for the final official version of the Ethics Manual, the Ethics Manual is still intended to be a "living document" to which references can be made throughout the duration of the project. The specific objective is to provide any updated related to the established principles, processes, mechanisms and bodies synthesis and to provide the status of the ethics controlling towards the final pilot round of the SHOW test sites as well as to recognise and discuss the need for local Data Privacy Impact Assessments (DPIAs) at the test sites. In the later sense, it is recommended to be read with the final update of the DMP (D14.3).

A sound and correct ethical treatment of participants is of great importance for SHOW, any relevant processes and administered documents are monitored and managed by the SHOW Ethics Board (EB).

The Data Protection Policy describes how data in general terms are supposed to be handled within SHOW. The policy focuses mainly on compliance with mandatory Data protection regulation regarding personal data such as the GDPR and complimentary local Data protection obligations. The aim is to make sure a sound and correct ethical treatment of participants that will be involved in the evaluation activities at the test sites, but, also, beyond that in any project activity involving humans.

Data Controllers or Data Processors must know when and how to carry out a Data Privacy Impact Assessment (DPIA). The Data Protection Policy provides guidance correspondingly, quoting also a template for carrying out the assessment successfully.

After a brief overview of the project and the ethical process (Chapter 1) the ethics manual is described (Chapter 2). The Ethics Manual describes the Ethical Code of Conduct for all actions and activities within SHOW. The updated summary of the ethics controlling process of the project is provided in Chapter 3. The Data Protection Policy (Chapter 4) describes how data is supposed to be processed within SHOW. The Data Protection Policy focuses mainly on compliance with mandatory data protection regulation. The Data Protection Policy also contains the guidelines and template for carrying out the DPIA (Chapter 5).

The central to the project DPIA has been updated in Chapter 5, on the basis of the knowledge and elaboration of work in this respect of the previous period, whereas the need and justification for local DPIAs at test site level is discussed.

Annex I provides an Ethics checklist for Ethics responsible partners at each test site to ensure that all necessary steps are taken to abide with the SHOW Ethics policy, Annex II provides the SHOW questionnaire on ethical and legal issues serving for the ethics controlling process across the project, Annex III includes the Data Privacy Impact Assessment (DPIA) template and Annex IV provides the living Ethics Board of the project.

1.2 Intended Audience

This deliverable addresses the members of the Consortium of SHOW and the third parties involved in the project, as well as the European Commission and other external participants that have an interest in conducting ethics and GDPR compliant large scale evaluation in CCAM.

1.3 Interrelations

The document is the Ethical manual for SHOW and together with EC Ethics requirement described in D18.1 (POPD – H – Requirement No. 1) that is about informed consent and information to participants and D18.2 (POPD – Requirement No. 3) that is about Data Protection Officer details, but also point at issues related to the "data minimisation" principle, security measures and informed consent procedures, it sets the basic for the work in pre-pilots (WP11) and Demonstration (WP12) and the closely related evaluation activities, but also in other project activities were humans are involved. The following diagram (Figure 1) presents the most distinct interrelations. Connections between other WP activities imply communication and sharing of data, results, and reports. The work related to services (WP5 and WP6), vehicle systems (WP7) and infrastructure (WP8) are not directly related to the Ethics, however, any conduct with external service providers should remain ethical and any data provision for the functioning of the systems should comply with the data protection policy of the project. The same holds true with the internal sharing of data, namely with WP10 and WP13.

The early connection to the Data Management Plan (D14.2; D14.3) and the technologies for large-scale data collection (WP5) in Figure 1 allows for harmonization of efforts. Apart from the tests with humans, it sets the foundation for any type of interaction with humans inside and outside to the project to be ethical (e.g. collection of input during dissemination activities, WP1 survey, social media feedback). It also identifies any data collection processes and activities within the project and pinpoints that the SHOW Ethical policy applies to them.

These user and stakeholder groups have been identified and is defined in D1.1 and in D1.2 'SHOW Use Cases' (M9), where the Use Cases (UCs) have been described.

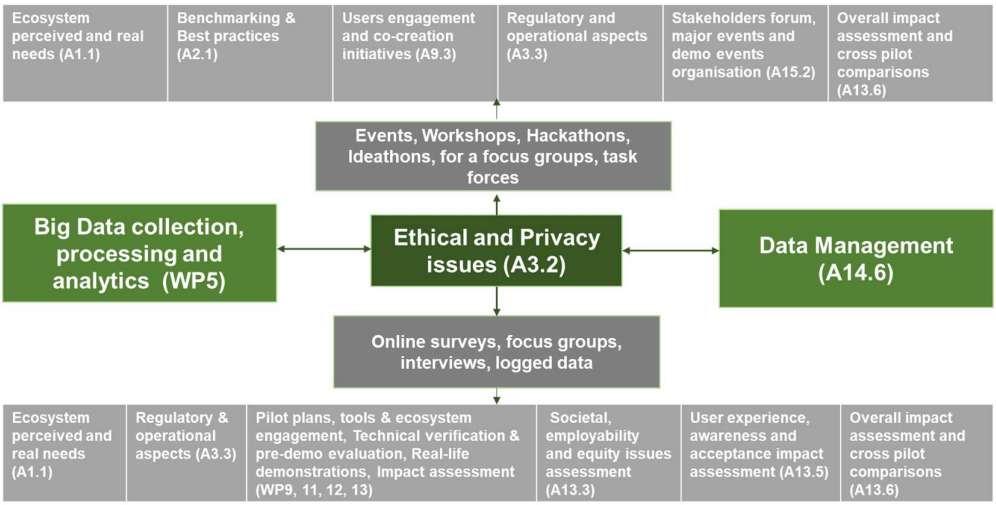

Figure 1: SHOW Ethical and Privacy issues interrelationships.

1.4 About SHOW

The SHOW project aims to support the migration path towards effective and persuasive sustainable urban transport through technical solutions, business models and priority scenarios for impact assessment, by deploying shared, connected, electrified fleets of automated vehicles in coordinated Public Transport (PT), Demand Responsive Transport (DRT), Mobility as a Service (MaaS) and Logistics as a Service (LaaS) operational chains in real-life urban demonstrations.

SHOW aims to demonstrate and evaluate a complex System of Systems (SoS). The SHOW ecosystem includes system and services as: Traffic Management Control (TMC) controlling

AV fleet, Advanced Logistic vehicles, Connected bike sharing, Automated charging and parking depot, Roadside charging, Automated MaaS, Automated Maas Stations, Automated DRT.

Comprehensive frameworks to be used for evaluations of such an ecosystem, with layers of safety, energy and environmental impact, societal impact, logistics and user experience, awareness and acceptance are not yet available. Especially when taking into consideration several stakeholder perspectives, described in SHOW D1.1: "Ecosystem actors' needs, wants & priority users experience exploration tools". The list of stakeholders for SHOW consists of the following key groups:

- Vehicle users (end users, drivers, and remote operators)
- Public interest groups and associations
- Decision-making authorities or regulators
- Operators (e.g., public transport operators, private fleet operators)
- Mobility service providers
- Industry (e.g., AV manufacturers)

The generic aim with the ethics manual is to make sure SHOW partners have a sound and correct ethical treatment of participants across all relevant activities of the project.

1.4.1. The Pilot Sites

In total 13 countries and 20 cities will be involved in Demonstrations activities. The following table (Table 1) presents the countries and cities included in the Mega, the Satellite and the Follower sites. In addition, Ispra site will serve for dedicated technical validation activities.

Table 1: Countries and cities per Site type.

Mega	Satellite	Follower
• France: Rouen and Rennes[1] • Spain: Madrid • Austria: Graz, Salzburg, Carinthia[2] • Germany: Karlsruhe, Monhe and Aachen[4]. • Sweden: Linköping and Gothenburg[5]	• Finland: Tampere • Denmark: Copenhagen • Italy: Turin • Greece: Trikala • Netherlands: Eindhoven (Brainport) • Czech Republic: Brno	• Belgium: Brussels • Greece: Thessaloniki • Switzerland: Geneva

[1] To be replaced by another City; subject to Amendment.

[2] As a replacement for Vienna, subject to Amendment.

[3] As a replacement for Mannheim, subject to Amendment.

[4] To be replaced, subject to Amendment.

[5] Replacing Kista, part of Amendment.

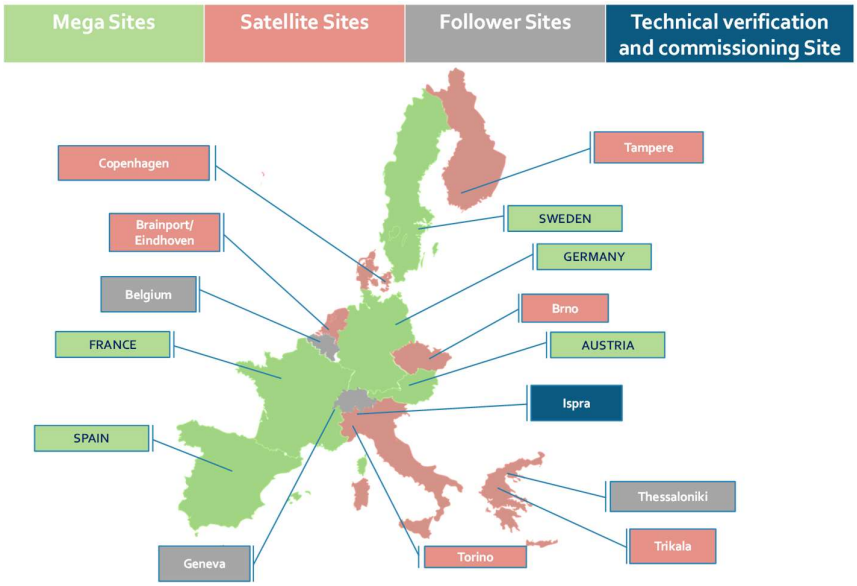

Figure 2: Mega Sites, Satellites and Follower sites in SHOW.

All countries abide to relevant EU legislation, directives, and guidelines (see Chapter 2). There might also be certain test site specific regulations that needs to be applicable.

The evaluations are divided into two phases. The pre-demonstration where no end users from general public are involved in general; still, participants from the SHOW Consortium will be involved and provide feedback in real life condition field trials, serving as rehearse trials in view of the final field trials. For the evaluation during the final demonstration phase, public citizens will be targeted.

1.4.2. End users and stakeholders

SHOW targets a wide variety of stakeholders and end users, as follows:

Stakeholders:

- Vehicle users (end users, drivers, and remote operator)
- Public interest groups and associations
- Decision-making authorities or regulators
- Operators (e.g., public transport operators, private fleet operators)
- Mobility service providers
- Industry (e.g., AV manufacturers)

End users:

- All types of travellers using public and private transport. Target groups at sites: commuters, residents, students, children, elderly, tourists/ visitors, Vulnerable Road Users (VRUs), Persons with reduced Mobility (PRM).
- SHOW beneficiaries employees at pilot sites (for pre-demo activities), clustered to one of more of the above categories.

2 Ethics Manual

2.1 Aim

The current deliverable (D3.5) is an update of *D3.4: SHOW updated Ethics manual & Data Protection Policy and Data Privacy Impact Assessment*.

The established Ethics Board (EB) is provided at Annex IV of the current document. The Ethics Manual gives further clarifications about the inner workings of the EB and the relations between the local ethics representatives, the partners of SHOW and the EB.

The Ethics Manual touches upon issues concerning ethics in relation to children, incidental findings, incentive schemes and gender.

Furthermore, the updated Ethics Manual takes the Covid-19 pandemic into account when it comes to health and safety procedures.

2.2 Regulations

In Annex 4 of Grant Agreement the legislation and non-binding instruments to be considered by SHOW's Ethics Board are described. Specific Laws and Directives to be considered per area are summarised in Table 2.

Table 2: Legislation and non-binding instruments to be considered by SHOW's Ethics Board.

Ethical & social issue	Ethics area	Law/directive
Human Dignity and integrity of user	*Human rights*	• Universal Declaration of Human Rights (United Nations) • Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe) • European Charter of Fundamental Rights • Draft recommendation of the Council of Europe on the promotion of the human rights of older persons • European Charter of the Rights of Older People in need of Long-term care and assistance
Privacy	*Data protection*	• The Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) (replacing the Directive 95/46/EC of the European parliament and the Council (1995)), on the protection of individuals about the processing of personal data and on the free movement of such data. • Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. • Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector. Take into account developments of Reform of the legislative framework

Ethical & social issue	Ethics area	Law/directive
		for personal data protection (In January 2012, the European Commission proposed a reform of the Directive 95/46/CE, which constituted until now the basic instrument for personal data protection, in the form of a global Regulation on data protection 2012/001 (COD), supplemented by Directive 2012/0010 (COD) concerning the processing of personal in the area of police and judicial cooperation in criminal matters. • Art.29 Data Protection Working party: Working Document on Privacy on the Internet.
New Technologies	*Liability and Safety*	• Directive 85/374/EEC on liability for defective products as amended by Directive 1999/34/EC, hereinafter "the defective products Directive" • Directive 2011/24/EU on the application of patients' rights in cross-border healthcare • Directive 90/385/EEC on active implantable medical devices and Directive 93/42/EEC on medical devices and Directive 98/79/EC on in vitro diagnostic medical devices • RoHS Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment. • Directive 98/34/EC of the European Parliament and of the Council of 20 July 1998 amended by Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services.
Safety and Certification of Autonomous systems/ vehicles		• Existing technologies adhere to all current and relevant standards in the area (of Application Requirements and Services, ISO TC 204 - Intelligent transport systems CEN TC 278 - Intelligent transport systems, etc.). • All the technologies will be verified before actual implementation for the pilot activities.

2.3 Partners role and responsibilities

Within the project evolution the following regulations related to compliance, approvals, privacy, personal health information and collaboration should be applied for all partners involved in user related activities, such as evaluation activities, focus groups, surveys and data collection in general etc. (see also the project Consortium agreement):

1. Each party shall be responsible for ensuring its own compliance with all laws and regulations applicable to its activities. Such laws include, but are not limited to, those in respect of rights of privacy, intellectual property rights and healthcare.

2. Any party which provides any data or information to another party in connection with the project will not include any personal information relating to an identified or identifiable natural person or data subject.
3. To this end, the providing party will anonymise all data delivered to other parties to an extent sufficient to ensure that a person without prior knowledge of the original data and its collection cannot, from the anonymised data and any other available information, deduce the personal identity of individuals (see CA for further information).
4. Each party shall be solely responsible for the selection of specific database vendors/data collectors/data providers, and for their performance (see CA for further information).
5. Partners supplying special data analysis tooling, shall have the right on written notice and without liability to terminate the license that it has granted for such tooling to be used in connection with the project, if the supplying partner knows or has reasonable cause to believe that the processing of particular data through such tooling infringes the rights (including without limitation privacy, publicity, reputation and intellectual property rights) of any third party, including of any individual.

2.4 Ethics Code of Conduct

2.4.1 Code of Conduct for Research Integrity

ALLEA is the European Federation of Academies of Sciences and Humanities, representing more than 50 academies from over 40 EU and non-EU countries. ALLEA has created the European Code of Conduct for Research Integrity. The Code serves the European research community as a community as a framework for self-regulation [6]. The European Commission has recognised the Code as a reference document for research integrity for all EU-funded research projects and as a model for organisations and researchers across Europe.

The members and third parties of SHOW are therefore obliged to ensure that the conditions for research Integrity set out in the Code is fulfilled. The Code will be used as a framework for dealing with ethical and professional issues within SHOW.

Good research practices, according to the Code, are based upon the following fundamental principles of research integrity:

Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources.

Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.

Respect for colleagues, research participants, society, ecosystems, cultural heritage, and the environment.

Accountability for the research from idea to publication, for its management and organisation, for training, supervision, and mentoring, and for its wider impacts.

[6] https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf

2.4.2 Code of Conduct for various ethical issues

The procedures and criteria that will be used to identify/recruit participants will be kept on file and submitted on request. Furthermore, the informed consent procedures (see D18.1) that will be implemented for the participation of humans will be kept on file and submitted on request.

The members of SHOW shall especially focus on:

Abide to the Ethics Manual and Data Protection Policy of SHOW.

Protect private and sensitive information and ensure that participants will not be harmed during the pilots. The Data Protection Policy is found in Chapter 4.

Respect participant's free will and treat them as intelligent beings who decide for themselves about any type of gathered data that are indeed outcomes of their participation.

Inform in full about which data will be collected and how data will be collected, processed, shared, and disposed before signing the consent form. For informed consent and withdraw recommendations are made in D18.1.

Communicate ethical issues to the Ethics Board and the project management team to ensure these issues will be timely and effectively addressed, managed and resolved.

Ensure ethics approval (wherever is applicable) is obtained on time and relevant documents are shared with the EB.

Communicate results their findings through open-access journals to other researchers and academic communities (especially true if it is requested by the funder). Personal data, unless separately agreed with the person, will not be published.

Ethics control and monitoring within SHOW is carried out by the EB.

Incentive strategies (if any) have been decided and described within WP9 Deliverable 9.2 (and will be updated in D9.3).

Transparency at each Demonstration site should explain the following to recruited participants:

- general scope of SHOW and short reference to its objectives,
- scope and short description of the Pilot and the respective study,
- value of participation (benefits for the participant and the public in general),
- acknowledgement of research results, and
- role of participants in the Pilots.

Acknowledgement to the participants of SHOW studies will be done by the local to each site evaluation teams. The Evaluation team members will during testing ensure that the participants feel comfortable and not coerced or tired. Questions are allowed during testing, in designated times. Participants should be informed about this possibility beforehand. The contact person details will be provided to the participant along any information and contacts in case the participants have any questions after the end of the testing session.

Risk assessment See Chapter 2.7.

Communication with participants should abide with fundamental human rights principles. Participants should not feel coerced, threatened or stressed by researchers. The researchers must make sure that their behaviour towards participants is not deceitful and that the participants has been given sufficient information about the project. The concept of deception and debriefing is discussed below.

- **Deception.** Researchers do not deceive by any means prospective participants about research that is reasonably expected to cause physical pain or severe emotional distress. Researchers explain any deception that is an integral feature of the design and conduct of an experiment to participants as early as feasible, preferably at the conclusion of their participation, but no later than at the conclusion of the data collection, and permit participants to withdraw their data. No deception will take place in SHOW Demonstrations and the user will be informed at all evaluation stages about the objectives and the procedures related to the pilots and how their data will be handled, processed, and stored. In the case a functionality of a service is emulated, they will be informed beforehand (in the context of "Scope and short description of the Pilot and respective study"), but they will be asked to perform and react as the situation was real.
- **Debriefing.** Researchers provide a prompt opportunity for participants to obtain appropriate information about the nature, results and conclusions of the research, and they take reasonable steps to correct any misconceptions that participants may have of which the researchers are aware.

2.5 The SHOW Ethics Board

2.5.1 Overview

In general, the Consortium shall implement the research project in full respect of the legal and ethical national requirements and code of practice. The Local Ethics Representatives (LER) will be used as a contact point to achieve this aim.

Ethics Board (EB) consist of the Core Ethics Board (CEB) and the Local Ethics Representatives (LER), see Figure 3.

CEB is led by the Ethics Manager (VTI) in collaboration with the Coordinator (UITP), the Technical and innovation Manager (CERTH/HIT) and the WP9 leader (VTI).

All SHOW Pilot sites and cross-test site entities that will participate in the project have nominated a Local Ethics Representative that will be supervised by the Ethics Board of the project.

The name of the representatives in both CEB and LER are found in Annex IV and on the project Cooperative tool. Names and contact information are being continuously updated.

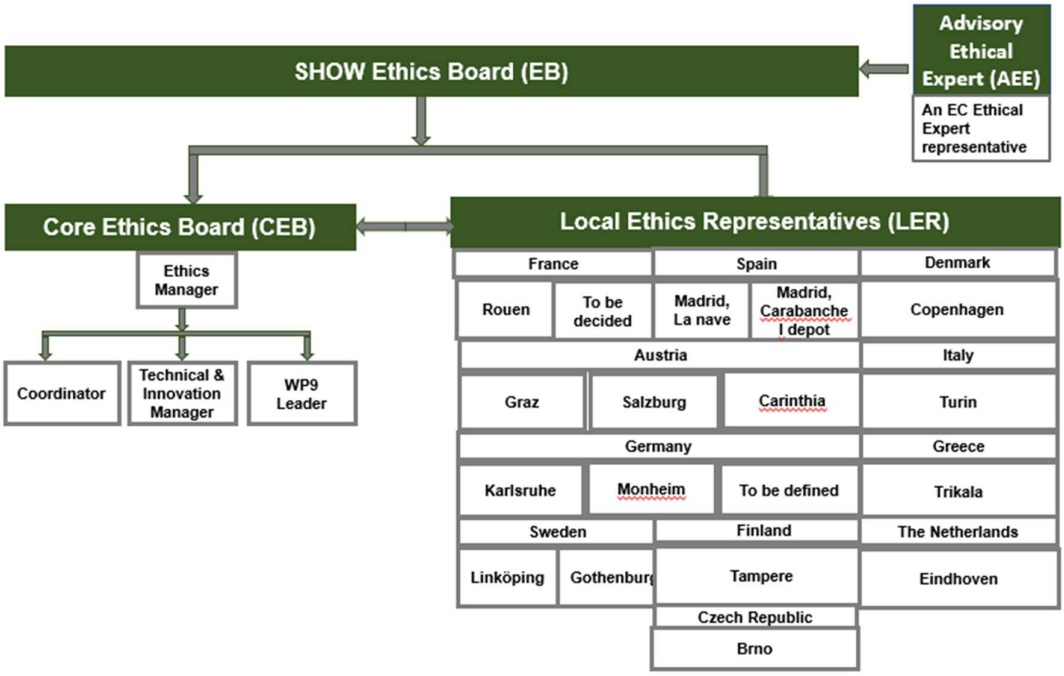

Figure 3: The Ethical board organisation.

2.5.2 Main responsibilities of the EB

The main responsibilities of the Ethics Board are as follows:

- Ensure the project's Ethics policy complies with European and national regulations.
- Ensure all project activities are conducted in line with SHOW Ethics Manual and Data Protection policy (this document).
- Resolute any potential ethics related conflicts and mitigate risks.
- Address any potential issues and risks.
- Raise any ethics issues related to automation and resolve in collaboration with pilot site responsible partners.

The SHOW Ethics Board (EB) will be responsible for the project's ethics management and will act as supervisors of the ethical activities of the project. They will do so considering both European and national ethical and legal requirements. They will also collaborate with external members (e.g. regional/municipality authorities) to ensure the Board is making decisions that are in harmony with the ethical profile and agenda of the cities and areas that will act as a Pilot sites.

The EB is obliged to obey the national and European legislation and code of practices and has to fully support and scrutinize any plans, operational documents, and research protocols to guarantee that the Ethics policy is applied in all activities and foremost when and where users are involved. Partners should ensure timely submission of research protocols based on their previous experience with relevant bodies to avoid any delays in the pilot's instantiation.

2.5.3 Local Ethics Representatives (LER)

The profile of a member of the LER is defined as follows:

- Responsible for a demonstration site;
- Experience in data collection and/or data management with humans involved;

- Experience in preparation and submission of ethical proposals and handling of approvals including compliance to GDPR in relation to vehicle testing.

The LER are required to report to the Ethics Board about all relevant activities, their compliance as well as any problems that may arise (see Annex I for support purposes and Chapter 2.6 in this document).

The means to do so will be the Ethics Controlling Reports, according to the template of Annex II, designed for this purpose. A summary of each pilot site will be obtained, and the information will become the Ethics profile of each pilot site. In addition to the SHOW Controlling Report, ethical approvals will be obtained in the test sites if they have obligation to do so.

The LER at each test site will be the main contact point for any ethics related issues (e.g. submission of research/test protocols for approval, by the Institutional/National Ethics Committees, GDPR, etc.) from the specific pilot site point of view. Their role will be to comply with the Ethics Manual (this document) and report back before and after each pilot round by means of an Ethics Controlling Report (see Annex II) across all issues defined by the EB and tackle with user involvement, ethical and data protection issues. In addition, one of the main tasks of the nominated persons will be to coordinate and be responsible for obtaining approval by the local/regional/institutional ethics and GDPR regulatory committee before any pilot related activities take place (e.g. even before recruitment starts), if needed. Any required or requested authorisations and approvals remain official project documents at any time.

2.5.4 The Advisory Ethical Expert

The role of the AEE is to support and provide input to the EB and to make sure that considerations made are in line with the work done by the dedicated EC Expert Group addressing specific ethical issues raised by driverless mobility, specifically connected and automated driving related to road transport (see https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3659).

The work of Ethics of Connected and Automated Vehicles and their recommendation has been used as a starting point in this work (https://ec.europa.eu/info/news/new-recommendations-for-a-safe-and-ethical-transition-towards-driverless-mobility-2020-sep-18_en).

2.6 Ethical Management in SHOW

The diagram in Figure 4 presents the procedure of ethical considerations from planning to realisation of a demonstration/evaluation activity. The LER of SHOW is the one responsible for keeping track of the process through a dedicated checklist (see Annex I).

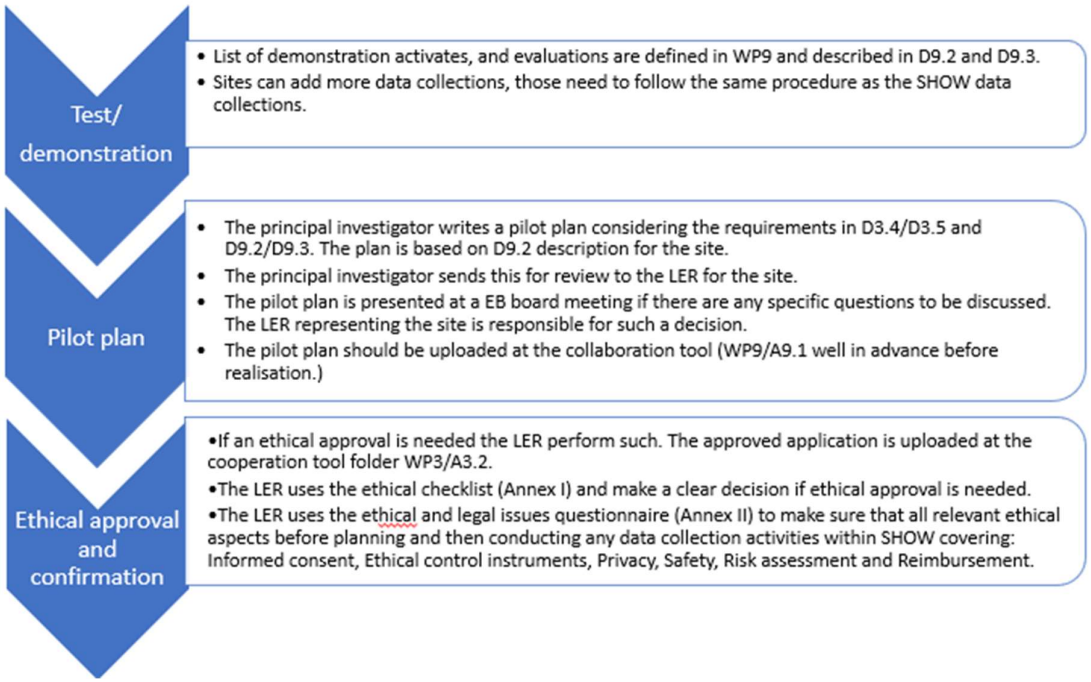

Figure 4: The procedure and flow of information from Ethics Board to Demonstration site.

2.7 Risk assessment and mitigation strategy

The risk assessment includes the plans to ensure no harm will be brought upon the participants and pre-testing activities will ensure that this will stay the case. None of the Pilot related tasks (either in pre-demo or Demonstration) is anticipated to have any (side-) effects on the physical or mental integrity or health of the participant, other than the ones existing in their everyday travelling activities. As diverse user groups are addressed (travellers including potentially disabled, older citizens, young people, and various stakeholders) all sites (have and) will internally review the Pilot plans and will reach a decision on the inherent risks for all possible addressed user groups.

To minimise risk, the LER ensure that the participants have received proper information. Also, when there are safety related issues (i.e. in-vehicle information and scenarios of use) all necessary precautions will be taken. In all cases, the test sites will abide with the internal and/or national safety regulations applying in their sites. All the test site leaders have established internal company quality assurance procedures, which will be adopted to guarantee high level quality in SHOW activities.

It is not possible to conceive a procedure, investigation, or process which would be without any risk. One of the most important factors in the assessment of risk is the perception of the prospective participant of the importance of risk. The participant's life situation may substantially influence the way in which a risk is perceived. The end point of the process is the consent given by the person to be part of the research project, having considered all aspects of the process and asked all relevant questions.

All relevant information will be given to the participants. This means that the project SHOW will be carefully explained. The choice that is made and the consent that is given will be without coercion or undue pressure being applied.

Categories of risk take into consideration:

- **Physical risks** stemming from traffic safety issues will be minimised and is expected to be at the same level as that experienced by the average traveller throughout their daily driving when in a hurry, fatigued, stressed, etc.
- **Psychological consequences** will be carefully examined and considered.
- **Social inconveniences** will be minimised (no additional stress or different from stress experienced during daily living/driving/travelling conditions, cost reimbursement for additional transport costs, etc.).

A risk analysis is presented in Table 3.

Table 3: Preliminary considerations regarding Ethical Risk Management in SHOW.

Ethical & Social risks	Description	Ethical Risk Management in SHOW
Application of overarching Ethical and legal framework	All relevant legislation, regulation and ethical codes will be considered; they are defined how they are met in terms of processes, timing and responsibilities.	SHOW EB will oversee the ethical concerns involved in the project and the ethics approval processes at project level. Annex I includes the information required to be addressed and included in an Ethics application form partners will be required to obtain prior any evaluation takes place.
Transparency and consent of the travellers	The informed consent administration ensures that the user accepts participation and is informed about the project and demonstration/evaluation objectives. Written consent, if needed, is obtained after travellers are informed. Information provided is clear and understandable about their roles (tasks and rights), research objectives and methods applied, duration of study and participation (if they differ), confidentiality, safety and risk related issues as well as the benefit for them and the project. These aspects are managed in the next column (on the right) and are depicted in the informed consent form template (annexed in D18.1).	The basic parts of the SHOW informed consent include: 1. The possibility to decline the offer and to withdraw at any point of the process (and without consequences) 2. Information about the data controllers, processors and data manipulation in general; 3. Identification of data controllers and processors; 4. Contact person identification.

Ethical & Social risks	Description	Ethical Risk Management in SHOW
Privacy and data protection	Only anonymised or pseudonymised data will be processed and used in the evaluations and, therefore, no personal data will be processed in relation to specific user. The name will not be connected to other characteristics (e.g. age, gender, nationality, health and/or mobility profile). To avoid risks related to the processing of personal data such as identity theft, discriminatory profiling or continuous surveillance, the principle of proportionality has to be respected. Data can be used only for the initial purpose for which they were collected. Anonymisation or pseudonymisation is a way to prevent violations of privacy and data protection rules. Processing has to be limited to what is truly necessary and less intrusive means for realising the same end have to be considered.	This is in detailed described in Chapter 3. In general, the project identifies which data protection rules apply and establishes a list of risks and potential solutions; taking due account of the following: - What kind of data will be processed? - What is the purpose of the processing? - Will the data exceed the purpose of the study? - Are there procedures ensuring that data is processed only for the originally identified purposes? - Who is the owner of the data? - Is data connected to other information? - Will data be commercially exploited? - What is the duration of the storage of the data? - Where will the data be stored and according to which national legislation? - Who will access the data? Are they secured? - Will the user be recorded? - Which metrics will be implemented? - Who will supervise the data protection? The collected information have consequently fed the data management process.
Safety & certification of autonomous systems/vehicles	Data collection and evaluation activities should not entail any undue risk for participants other than the ones they will encounter in their everyday travelling and living activities.	Existing technologies adhere to all current and relevant standards in the area (of ETSI TC ITS - Application Requirements and Services, ISO TC 204 - Intelligent transport systems CEN TC 278 - Intelligent transport systems, etc.) as they are collected and listed within A15.5. Further standardisation and certification aspects will be handled in the aforementioned activity.

Ethical & Social risks	Description	Ethical Risk Management in SHOW
		SHOW technologies will be verified, validated before actual deployment to pre- and final demonstrations within D11.1 'Technical validation protocol and results' and D11.2 'Demos safety, reliability and robustness validation and commissioning', respectively.
Participants' engagement	Evaluation is expected to be inclusive and representative of different traveller types, especially in a dynamically shaped real-life context. The selection and recruitment of participants is a crucial part of the involvement process, as it will impact on the quality of the outcomes and the sustainability of the research outcomes. At this stage a satisfactory number of users and combination of travellers' characteristics is sought (i.e. to reflect and accommodate the needs of the chosen UCs); gender balance and equality are addressed.	SHOW will target specific travellers' groups. Adequate number of travellers will ensure sample representativeness, even at pre-Demonstration level, including: i) different age groups, ii) balanced female/male ratio iii) various social, cultural, and socio-economic (SES backgrounds). Relevant reporting has and will take place at D9.2 and D9.3 respectively. The EB will oversee the selection of participants having been committed in the above Deliverables. Participant engagement will be governed by the guidelines defined by the Responsible Research and Innovation Framework*. *https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

Further criteria and procedures regarding participants' recruitment might apply depending on the elaborated pre-Demonstration plans. These further criteria and procedures have been described in detail in a dedicated chapter of *D9.2: Pilot experimental plans & impact assessment framework for pre-demo evaluation*, which will be respectively updated for the final demo phase in *D9.3: Pilot experimental plans, KPIs definition & impact assessment framework for final demonstration round.*

2.8 Health and safety procedures

For SHOW, it is of high importance that during evaluation and demonstration activities appropriate Health and Safety (H&S) procedures on departmental/institutional abut also on regional/national level are followed. This includes staff as well as external participants. The overview of the respective regulations for SHOW test sites is provided Chapter 5.1.5 of the Grant Agreement. It is up to each site to follow those regulations and provide evidence for thin upon request.

Due to the Covid-19 pandemic health and safety procedure must take local and national provisions and recommendations into account and adapt accordingly.

2.9 Ethics in relation to participants

All research should follow the Data Protection Policy of SHOW (see Chapter 4).

As SHOW demonstrations operate under real environments (with an estimated total of 1,500,000 passengers participating in them over the course of the 12 months, across all 20 cities in Europe), they cover the needs and consider the preferences of all types of travellers.

Nevertheless, specific use cases and test environments (around schools, universities, airports, warehouse depots, etc.) take place; thus, the objective is to research specifically the needs and wants of specific target user clusters, including among other commuters, tourists, students and the elderly and people with mobility restrictions. Finally, the integrated transportation chain nature of SHOW Pilots and their connections to major city hubs (rail stations, etc.) allow for proper coverage of multimodal travellers' needs.

Traveller groups and involved stakeholders will be recruited and invited, respectively to participate in dedicated and controlled activities during the conduction of the pre-demonstration tests, as they have been defined within D9.2/D9.3. All participants will have the competence to understand the informed consent information.

Recruitment of participants will take place during both pre-demonstrations and Demonstrations. Also, recruitment stands in both phases also for the vulnerable road users that will participate depending on the pilot plans, specifications, requirements and criteria, due to the nature of the evaluation (i.e. in some cases, specific connectivity equipment is required by the VRUs that participate in the interaction with AVs).

Vulnerable road users (VRUs) are considered "*by the amount of protection in traffic (e.g. pedestrians and cyclists) or by the amount of task capability (e.g. the young and the elderly). Vulnerable road users do not usually have a protective 'shell', and also the difference in mass between the colliding opponents is often an important factor. Vulnerable road users can be spared by limiting the driving speed of motorized vehicles and separating unequal road user types as much as possible"* (SWOV Vulnerable Road Users Fact Sheet, 2012).

Vulnerable users such as homeless, drug and alcohol users and abusers, immigrants, etc. will not be recruited to participate in any SHOW controlled demonstration evaluation across the test sites. However, during the final pilot round that will be open to public, participants will not be recruited (apart from the cluster of VRUs mentioned earlier), and people will freely use the vehicles, as they would normally do during their daily and/or frequent mobility activities. As such, the SHOW Consortium will have no control and will not be aware of who is using the vehicles; still, in any case, no personal data will be collected by the passengers. For real operation in the field trials, the same regulations that already stand and are applied by the operators (concerning the protection of human rights, etc.) will be also in force for the case of SHOW.

The substantial number of users will ensure a wide trial perspective, including: i) different age groups, ii) balanced female/male ratio, and iii) various social backgrounds. The EB of SHOW will oversee the selection of participants when it is applicable (i.e. in stakeholder interviews, in the specific cases that passengers will be recruited).

2.9.1 Ethics in research with children

According to the United Nations Convention on the Rights of the Child, the term child refers to every human being below the age of eighteen years unless under the law applicable to

the child, majority is attained earlier. The term child will have the same meaning in this document.

Children are addressed as a user group within SHOW, hence partners must familiarise with and abide ethical guidelines pertaining specifically to children, which have been developed by a number of organizations. These guidelines vary somewhat, depending on the value basis for the research in different organizations. The core principles are as follows:

- Having a commitment to children's well-being **(Beneficence)**;
- Having a commitment to doing no harm **(Non-Maleficence)**;
- Having a commitment to children's rights including the right of individuals to take responsibility for him or herself **(Autonomy)**;
- Being child-centred in its approach to research, listening to children, treating them in a fair and just manner **(Fidelity)**.

These principles have implications for decision-making in several key areas, including consent and confidentiality, but also in the general manner in which children are treated in any research encounter. D18.1 describes the procedure for information and consent regarding children.

2.9.2 Not included in SHOW

SHOW will not touch any of the following fields of research:

- research activity aiming at human cloning for reproductive purposes;
- research activity intended to modify the genetic heritage of human beings which could make such changes heritable;
- research activities intended to create human embryos solely for the purpose of research or for the purpose of stem cell procurement, including by means of somatic cell nuclear transfer.

Furthermore, SHOW does not include any research involving

- the use of human embryonic tissue, human foetuses, human foetal tissue, other human tissues;
- genetic information;
- pregnant women;
- animals.

2.10 Incidental findings

They are defined as the findings that maybe by-products or outcomes of the study that were not necessarily collected to answer the main research questions and objectives but could be of importance for the physiological, psychological and metal wellbeing of the participant. The number and type of incidental findings could be different for each site and valuable for both the person and the other stakeholder groups.

Any findings that are related to driver's traffic rules' violations during the tests will not be communicated to third parties (including insurances, authorities, etc.); as the driver is driving "as he/she will do when along" and assumes fully legal responsibility on his/her acts. Written exception will be made for deliberate criminal acts on behalf of the driver or/and related to an eventual accident during the tests.

Health decrements identified in a person during a test will be communicated in writing to the test participant and only, supporting them to contact medical support if needed.

2.11 Reimbursement

The participants may receive a reimbursement (incentive) as compensation for their participation. The incentive will be in line with the performing partners' general practice. Two levels of incentivisation are expected to be applied:

a) Incentives for real-life travellers, not specifically recruited by SHOW: Real-life travellers will be incentivised to use the services provided in SHOW through discounts that will be offered to them by the respective operators. This discount has been anticipated to be covered by the project, if wished by the test sites, in the sense of "compensation for evaluation activities' and has been allocated in the different pilot leaders of the corridor. Still, it might be the case that the different operators themselves may have planned to assume this at own cost.

b) Incentives for participants specifically recruited by SHOW: As commitment is essential for the success of the project, users might receive some form of reimbursement. In case of recruiting employees, incentives are not used as people are already paid for their time. Participants should be informed of the presence/absence of incentives when recruited and a statement needs to be added in the consent form. In case of legal restrictions or policies, the ethics responsible at each pilot site should inform the EB. An alternative to cash is using vouchers; sometimes it is easier for evaluation moderators to carry/use and they should be representative of the demographics (i.e. have an added value for older citizens). It is upon the discretion of each partner to decide the incentive scheme to use (if not to use). Other options include sharing the results of the study, making charitable donations, creating a prize draws and offer nonmonetary gifts.

Recruited participants in pre-demo activities as well as VRUs and stakeholders in both phases may receive an incentive as compensation for their participation. It will not be conditional based on performance or restricted to finalization of the actual test. In general, it is not envisaged to give money to the evaluation activities participants.

It is a fine line between creating a culture of incentives when recruiting people and the EB will oversee and approve (or not) the incentive schemes chosen by each pilot site, apart from the research protocol approval by the LER. Therefore, based on the evaluation plans appropriate incentives will be chosen.

2.12 Gender

The gender level of participation within the SHOW activities will be monitored. Equal opportunities and equal treatment between men and women will be guaranteed.

Over the years, the European Parliament has supported and called for measures to improve the position of women. This work continues through the activities of the Women's Committee. In detail, several specific European and UN Policies have been adopted to promote the equity of gender. Those will be fully respected within the project. The monitoring of the gender level of participation within the project activities is important for SHOW.

In more detail, there are several specific European and UN Policies that will be adopted to promote the equity of gender (i.e. Council Directive 75/117/EEC, etc.).

SHOW will ensure that during all its phases, and as much as possible equal gender participation will be maintained, this addresses research and development phases, as well as evaluation phases. The gender will be one of the Demonstrations and other test/evaluations participants' characteristics that will be tracked and statistically processed (to come up with any correlations if applicable). This is added in D9.3 for each demonstration site.

3 Data Protection Policy

Personal Data must be processed in compliance with applicable data protection laws. The exact requirements and due diligence for Processing Personal Data need to be scoped and defined within the relevant jurisdictions.

All parties and third parties to SHOW must comply with all applicable data protection laws and adapt routines continuously so that the Processing of Personal Data for which the parties are responsible does not violate the rights and freedoms of individuals. Each one is responsible for complying with SHOW Data Protection Policy (current Chapter).

Throughout this Data Protection Policy, a Party or third party to SHOW which are Processing Personal Data will be referred to as Controller and/or Processor.

There are checklists provided by the ICO throughout this Data protection policy, which are supposed to help the Controllers/Processors (see Chapter 4.1), to meet the obligations under the GDPR. In case of uncertainty concerning the Controllers/Processors ability to meet the requirements of the GDPR, it is recommended that the Controller/Processor use these checklists. Be aware that there might be other regulations to comply with as well, for example complimentary national regulations to the GDPR.

The Personal Data that is or will be processed with in SHOW will fall into one of the following categories:

- Personal Data collected in the context of participation in a research study,
- Contact information such as name, address, telephone number and email address,
- Banking and other financial information for payment or invoicing purposes,
- Information about how one uses websites, for the purpose of making them more user-friendly, for example via cookies,
- Information about participation in conferences or courses, and
- Personal Data needed for employment purposes.

The Data Management Plan for SHOW (D14.2; D14.3) further explains how the parties must process information to fulfil their obligations.

The following excerpt is from SHOW Consortium Agreement.

"*The Parties agree that any Background, Results, Confidential Information and/or any and all data and/or information that is provided, disclosed or otherwise made available between the Parties during the implementation of the Action and/or for any Exploitation activities ("Shared Information"), shall not include personal data as defined by Article 2, Section (a) of the Data Protection Directive (95/46/EEC) (hereinafter referred to as "Personal Data") or under Article 4.1 of the GDPR. Accordingly, each Party agrees that it will take all necessary steps to ensure that all Personal Data is removed from the Shared Information, made illegible, or otherwise made inaccessible (i.e. de-identify) to the other Parties prior to providing the Shared Information to such other Parties.*"

3.1 Terminology for Data Protection Policy

- Anonymisation means the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. Once data is truly anonymised and individuals are no longer identifiable, the data will not fall within the scope of the GDPR.
- Data Protection laws mean EU Data Protection regulations and, to the extent applicable, the data protection or privacy laws of the test site country.
- Data Protection Policy means this document (D3.5)
- DPO means Data Protection Officer
- DPIA means Data Protection Impact Assessment
- GDPR means the General Data Protection Regulation (EU) 2016/679
- ICO means Information Commissioner's Office
- Pseudonymisation means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.
- Special Category Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health (also known as Sensitive Data).

The terms, "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Third countries", "Processing", "Processor" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

A party Processing Personal Data will in this Data Protection Policy be referred to as a Controller or a Processor. The terms Controller and Processor will be used somewhat interchangeable in this Data Protection Policy depending on the regulation to which it refers to.

The initial letter of the terms defined in this paragraph (4.1.) will be written with a capital letter indicating the terms specific meaning.

3.2 Data Protection Officer

In general, each Controller/Processor is obliged to appoint a Data protection officer (DPO) unless the duty is not mandatory under the GDPR.

It is a necessity to appoint a DPO if a DPIA must be carried out before a lawful processing of Personal Data can begin. The list of DPO contact points per pilot site has been updated, see Table 6.

Position of the DPO
☐ Our DPO reports directly to our highest level of management and is given the required independence to perform their tasks.

☐ We involve our DPO, in a timely manner, in all issues relating to the protection of Personal Data.

☐ Our DPO is sufficiently well resourced to be able to perform their tasks.

☐ We do not penalize the DPO for performing their duties.

☐ We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

Tasks of the DPO

☐ Our DPO is tasked with monitoring compliance with the GDPR and other Data Protection Laws, our data protection policies, awareness-raising, training, and audits.

☐ We will take account of our DPO's advice and the information they provide on our data protection obligations.

☐ When carrying out a DPIA, we seek the advice of our DPO who also monitors the process.

☐ Our DPO acts as a contact point for the Supervisory Authority. They co-operate with the Supervisory Authority, including during prior consultations under Article 36, and will consult on any other matter.

☐ When performing their tasks, our DPO has due regard to the risk associated with Processing operations, and takes into account the nature, scope, context and purposes of Processing.

Accessibility of the DPO

☐ Our DPO is easily accessible as a point of contact for our employees, individuals and the Supervisory Authority.

☐ We have published the contact details of the DPO and communicated them to the Supervisory Authority.

3.3 Record of Processing activities

Unless the duty is not mandatory under the GDPR, each Controller/Processor is obliged to keep a record of Personal Data Processing activities under its responsibility. **The data should be stored 5 years after the end of the project closure.**

3.4 Rights for individuals

Rights for individuals under the GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict Processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Each Controller/Processor must ensure that the requirements regarding these rights are met, for example when Processing Personal Data related to participants.

3.5 Principles

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of each Controller´s/Processor´s approach to Processing Personal Data.

3.6 Lawfulness, fairness and transparency

Each Controller/Processor must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using Personal Data and ensure that there is not a breach of any other laws while Processing the data. Each Controller/Processor must use Personal Data in a way that is fair. This means not to use data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. Each Controller/Processor must be clear, open and honest with individuals from the start about how their Personal Data will be used.

Lawfulness

☐ We have identified an appropriate lawful basis (or bases) for our Processing.

☐ If we are Processing Special Category Data or criminal offence data, we have identified a condition for Processing this type of data.

☐ We don't do anything generally unlawful with Personal Data.

Fairness

☐ We have considered how the Processing may affect the individuals concerned and can justify any adverse impact.

☐ We only handle individual's data in ways they would reasonably expect, or we can explain why any unexpected Processing is justified.

☐ We do not deceive or mislead individuals when we collect their Personal Data.

Transparency

☐ We are open and honest and comply with the transparency obligations of the right to be informed. [7]

3.6.1 Purpose limitation

The Controller/Processor must from the start decide the purpose of processing is, keep a record of the purpose and specify the purpose in the Controller´s/Processor´s privacy information for individuals.

[7] Information Commissioner's Office, published at the ICO website 2020-02-28, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/, licensed under the Open Government Licence

It is only allowed to use the Personal Data for another purpose if either this is compatible with the original purpose, the Controller/Processor gets a consent, or there is an obligation or function set out in law.

3.6.2 Data minimisation

The Controller/Processor must ensure that the Personal Data that are being processed is adequate, relevant and limited to what is necessary. With "adequate" means that the data Processing is sufficient to properly fulfil the defined purpose of the Processing (see purpose limitation above). With "relevant" means that the data Processing has a rational link to the defined purpose for the Processing. With "limited to what is necessary" means that the Controller/Processor is not allowed to hold more Personal Data than is needed for the defined purpose for the Processing.

In addition, aggregated data and/or inferences-mainly related to consolidated estimations will be shared with researchers outside the SHOW-consortium only upon agreement to do so, as the project participates in the Open Research Pilot.

3.6.3 Accuracy

The Controller/Processor should take all reasonable steps to ensure the Personal Data that is processed is not incorrect or misleading as to any matter of fact and if deemed necessary keep the data updated.

☐ We ensure the accuracy of any Personal Data we create.

☐ We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.

☐ We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.

☐ If we need to keep a record of a mistake, we clearly identify it as a mistake.

☐ Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

☐ We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the Personal Data.

☐ As a matter of good practice, we keep a note of any challenges to the accuracy of the Personal Data. [8]

3.6.4 Storage limitation

The Controller/Processor must not keep Personal Data for longer than needed.

☐ We know what Personal Data we hold and why we need it.

☐ We carefully consider and can justify how long we keep Personal Data.

[8] Information Commissioner's Office, published at the ICO website 2020-02-28, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/, licensed under the Open Government Licence

☐ We have a policy with standard retention periods where possible, in line with documentation obligations.

☐ We regularly review our information and erase or anonymise Personal Data when we no longer need it.

☐ We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.

☐ We clearly identify any Personal Data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes. [9]

3.6.5 Integrity and confidentiality (security)

The Controller/Processor must ensure that there are appropriate security measures in place to protect the Personal Data that is being Processed. With security measures means technical and organisational actions. The security measures of the Personal Data include protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage. This means that each Controller/Processor must have proper security to prevent Personal Data to accidentally or deliberately be compromised.

The Controller/Processor must choose employees with relevant professional qualifications providing enough guarantees in terms of technical expertise and personal integrity to ensure such confidentiality.

Note that information security is more than just cybersecurity (the protection of your networks and information systems). It also covers, and therefore requires, other actions like physical and organisational security measures.[10]

☐ We undertake an analysis of the risks presented by our Processing and use this to assess the appropriate level of security we need to put in place.

☐ When deciding what measures to implement, we take account of the state of the art and costs of implementation.

☐ Where necessary, we have additional policies and ensure that controls are in place to enforce them.

☐ We understand that we may also need to put other technical measures in place depending on our circumstances and the type of Personal Data we process.

☐ We use encryption and/or pseudonymisation where it is appropriate to do so.

☐ We understand the requirements of confidentiality, integrity and availability for the Personal Data we process.

---

[9] Information Commissioner's Office, published at the ICO website 2020-02-28, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/, licensed under the Open Government Licence

[10] Information Commissioner's Office, published at the ICO website 2020-02-28, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ , licensed under the Open Government Licence

☐ We make sure that we can restore access to Personal Data in the event of any incidents, such as by establishing an appropriate backup process.

☐ We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.

☐ Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

☐ We ensure that any data processor we use also implements appropriate technical and organisational measures. [11]

Below are some examples of actions that each Controller / Processor should consider and, if necessary, implement.

Pseudonymisation and Encryption

- Encrypted data transfer through server (SSL)
- Pseudonymisation of personal data for both development, integration and testing
- Protective measures against infiltration
- Physical protection of core parts of systems and access control
- Logging of systems and mechanisms as well as appropriate auditing of the peripheral components

Confidentiality

- Access to data is restricted and password protected.
- Access is documented and system controlled with permission and with potential for access removal
- Anti-virus software protected with automated updates and firewalls usage of systems and solutions
- Automatically activated and password-protected computer locking
- Password-protected access to all data and to a limited number of partners
- Prevention of forced password entry attempts
- Restriction to account access
- Logging of all access attempts and those who are failed to data storage
- Separated data handling

Integrity

- Detailed tracking of accessing and interacting with data (e.g. uploads, changes, versions, access times, etc.)
- Frequent backups to ensure data is not corrupted
- Ensuring utilised S/W, applications, systems involved are regularly updated and properly configured

Availability and Resilience

- Deletion procedures are established and documented
- The controller has a clearly defined process of data handling

[11] Information Commissioner's Office, published at the ICO website 2020-02-28, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/, licensed under the Open Government Licence

Restoring data access

- Documented and regularly tested failover procedures

Evaluation of technical and organizational measures

- Ensuring partners are informed about the Data Protection Policy (this document)
- The EB supervises the partners of SHOW (See Chapter 2).

3.6.6 Accountability

The accountability principle requires the Controller/Processor to take responsibility for what is being done to Personal Data and how the Controller/Processor comply with the other principles. There must be appropriate measures and records in place to be able to demonstrate compliance.

Compliance

☐ We take responsibility for complying with the GDPR, at the highest management level and throughout our organisation.

☐ We keep evidence of the steps we take to comply with the GDPR.

Technical and organisational measures

☐ adopting and implementing data protection policies (where proportionate);

☐ taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our Processing operations;

☐ putting written contracts in place with organisations that process Personal Data on our behalf;

☐ maintaining documentation of our Processing activities;

☐ implementing appropriate security measures;

☐ recording and, where necessary, reporting Personal Data Breaches;

☐ carrying out data protection impact assessments for uses of Personal Data that are likely to result in high risk to individuals' interests;

☐ appointing a data protection officer (where necessary); and

☐ adhering to relevant codes of conduct and signing up to certification schemes (where possible).

☐ We review and update our accountability measures at appropriate intervals. [12]

3.7 Lawful processing

The Controller/Processor must have a valid lawful basis to Process Personal Data. Before collecting data the participants have the right to be informed about relevant lawful basis. It is good to know that the GDPR sets out six lawful bases (consent, contract, legal obligation,

[12] Information Commissioner's Office, published at the ICO website 2020-02-28, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/, licensed under the Open Government Licence

vital interest, public task and legitimate interest). At least one must be applicable whenever a Controller/Processor Process Personal Data. Most lawful bases require that processing is 'necessary' for a specific purpose. If the Controller/Processor can reasonably achieve the same purpose without the Processing, the Controller/Processor can't claim to have a lawful basis at hand. The Controller/Processor must determine which lawful basis is applicable before beginning Processing. The decision should be documented.

The lawful bases we need to follow in SHOW are the following:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

If the Controller/Processor are Processing Special Category Data, criminal conviction data or data about offences the Controller/Processor need to identify both a lawful basis for general Processing and an additional condition for Processing this type of data.

3.7.1 Consent

The GDPR sets a high standard for consent. But the Controller/Processor often won't need consent. If consent is difficult, it is recommended to look for a different lawful basis. If the Controller/Processor deems consent to be the best option for lawful basis, be aware of the strict requirement for the procedure.[13]

Asking for consent

☐ We have checked that consent is the most appropriate lawful basis for Processing.

☐ We have made the request for consent prominent and separate from our terms and conditions.

☐ We ask individuals to positively opt in.

☐ We don't use pre-ticked boxes or any other type of default consent.

☐ We use clear, plain language that is easy to understand.

☐ We specify why we want the data and what we're going to do with it.

☐ We give separate distinct ('granular') options to consent separately to different purposes and types of Processing.

☐ We name our organisation and any Third-party controllers who will be relying on the consent.

☐ We tell individuals they can withdraw their consent.

☐ We ensure that individuals can refuse to consent without detriment.

[13] Information Commissioner's Office, published at the ICO website 2020-03-03, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/, licensed under the Open Government Licence

☐ We avoid making consent a precondition of a service.

☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

☐ We keep a record of when and how we got consent from the individual.

☐ We keep a record of exactly what they were told at the time.

Managing consent

☐ We regularly review consents to check that the relationship, the Processing and the purposes have not changed.

☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.

☐ We make it easy for individuals to withdraw their consent at any time and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don't penalise individuals who wish to withdraw consent.[14]

Furthermore, the consent procedure for SHOW has been described in D18.1.

3.8 Pseudonymisation and Anonymisation

3.8.1 Pseudonymisation

Pseudonymising Personal Data aims to reduce the risks to the Data Subjects and helps the Controller/Processor to meet the data protection obligations. It is a form of security measure.

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual. Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. The Controller/Processor can tie that reference number back to the individual if the Controller/Processor have access to the relevant information. This additional information shall be held separately and under lock.

Pseudonymised Personal Data remains Personal Data and within the scope of the GDPR.[15]

To mitigate the risks involved with processing Personal data, Personal Data should be encrypted (i.e. pseudonymisation and coding) to the extent reasonably possible, so that

[14] Information Commissioner's Office, published at the ICO website 2020-03-03, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/, licensed under the Open Government Licence

[15] Information Commissioner's Office, published at the ICO website 2020-03-03, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/ licensed under the Open Government Licence

individual cannot be identified. Pseudonymisation is preserved by consistently coding participants with unique identification codes.

Only one person at each pilot site will have access to personal identifiers (if any). A Test ID will be issued for each of the participants, whereas the pilot site person that will collect and issue them will not have participated in the evaluation and will have not meet the test participants and their performance in the tests.

3.8.2 Anonymisation

Anonymisation is a method of limiting risk of Processing data. Anonymising data wherever possible is therefore encouraged.

The GDPR does not apply to Personal Data that has been anonymised, i.e. information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.

In order to be truly anonymised under the GDPR, the Controller/Processor, must strip Personal Data of sufficient elements that mean the individual can no longer be identified. However, if the Controller/Processor could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised.[16]

3.9 International Transfer of Personal Data

It might be necessary for a Controller/Processor to transfer Personal Data to a Third country, although it should be avoided if possible. Controller/Processor must make special care to ensure compliance with the GDPR before the transfer takes place. The transfer is not allowed if the Controller/Processor are unable to make the transfer in accordance with the GDPR

The GDPR primarily applies to Controllers and Processors located in the European Economic Area (the EEA) with some exceptions. Individuals risk losing the protection of the GDPR if their Personal Data is transferred outside of the EEA. On that basis, the GDPR restricts transfers of Personal Data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their Personal Data is protected in another way, or one of a limited number of exceptions applies. A transfer of Personal Data outside the protection of the GDPR (which we refer to as a 'restricted transfer'), most often involves a transfer from inside the EEA to a country outside the EEA.[17]

1. Are we planning to make a restricted transfer of Personal Data outside of the EEA?

If no, you can make the transfer. If yes go to Q2

2. Do we need to make a restricted transfer of Personal Data in order to meet our purposes?

If no, you can make the transfer without any Personal Data. If yes go to Q3

[16] Information Commissioner's Office, published at the ICO website 2020-03-03, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/ licensed under the Open Government Licence

[17] Information Commissioner's Office, published at the ICO website 2020-03-02, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/, licensed under the Open Government Licence

3. Has the EU made an 'adequacy decision' in relation to the country or territory where the receiver is located or a sector which covers the receiver?

If yes, you can make the transfer. If no go to Q4

4. Have we put in place one of the 'appropriate safeguards' referred to in the GDPR?

If yes, you can make the transfer. If no go to Q5

5. Does an exception provided for in the GDPR apply?

If yes, you can make the transfer. If no you cannot make the transfer in accordance with the GDPR.

If you reach the end without finding a provision which permits the restricted transfer, you will be unable to make that restricted transfer in accordance with the GDPR.[18]

3.10 Data Privacy Impact Assessment

A Data Privacy Impact Assessment (DPIA) is a process to help the Controller identify and minimise the data protection risks of a project. The DPIA helps identifying the risks, foresee problems and bringing forward solutions.

The Controller must conduct a DPIA if the Processing is likely to result in a high risk to individuals. It is also good practice to do a DPIA for any other major project which requires the Processing of Personal Data.[19]

In SHOW it is mandatory for all test sites to consider if a DPIA is needed, and if yes perform such. It might be the case that the controllers at SHOW demonstration sites might already have established a process within its organisation and access to relevant template to conduct a DPIA in a satisfying way. Otherwise, the requirement for the process is described below and a template is provided in Annex III. The specific status of the SHOW test sites with respect to the recognition of the need for a DPIA and the conduct of it is summarised in the following Chapter.

[18] Information Commissioner's Office, published at the ICO website 2020-03-02, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/, licensed under the Open Government Licence

[19] Information Commissioner's Office, published at the ICO website 2020-03-02, 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/, licensed under the Open Government Licence

DPIA awareness

☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving Personal Data.

☐ Our existing policies, processes and procedures include references to DPIA requirements.

☐ We understand the types of Processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.

☐ We have created and documented a DPIA process.

☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening

☐ We consider carrying out a DPIA in any major project involving the use of Personal Data.

☐ We consider whether to do a DPIA if we plan to carry out any other:

☐ evaluation or scoring;

☐ automated decision-making with significant effects;

☐ systematic monitoring;

☐ Processing of sensitive data or data of a highly personal nature;

☐ Processing on a large scale;

☐ Processing of data concerning vulnerable Data Subjects;

☐ innovative technological or organisational solutions;

☐ Processing that involves preventing Data Subjects from exercising a right or using a service or contract.

☐ We always carry out a DPIA if we plan to:

☐ use systematic and extensive profiling or automated decision-making to make significant decisions about individuals;

☐ process special-category data or criminal-offence data on a large scale;

☐ systematically monitor a publicly accessible place on a large scale;

☐ use innovative technology in combination with any of the criteria in the European guidelines;

☐ use profiling, automated decision-making or Special Category Data to help make decisions on someone's access to a service, opportunity or benefit;

☐ carry out profiling on a large scale;

☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;

☐ combine, compare or match data from multiple sources;

☐ process Personal Data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;

☐ process Personal Data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;

☐ process children's Personal Data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

☐ process Personal Data that could result in a risk of physical harm in the event of a security breach.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our Processing.

☐ If we decide not to carry out a DPIA, we document our reasons.

DPIA process

☐ We describe the nature, scope, context and purposes of the Processing.

☐ We ask our data processors to help us understand and document their Processing activities and identify any associated risks.

☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ We ask for the advice of our DPO.

☐ We check that the Processing is necessary for and proportionate to our purposes, and describe how we will ensure compliance with data protection principles.

☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

☐ We identify measures we can put in place to eliminate or reduce high risks.

☐ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

☐ We implement the measures we identified, and integrate them into our project plan.

☐ We consult the Supervisory Authority before Processing, if we cannot mitigate high risks.

☐ We keep our DPIAs under review and revisit them when necessary.[20]

[20] Information Commissioner's Office, published at the ICO website 2020-03-02, 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/, licensed under the Open Government Licence

4 Ethics compliance check at SHOW sites

4.1 Overview

During the preparation of the previous version of the SHOW Ethics Manual (D3.4) (in view also of the pre-demo phase launch), the "Questionnaire on ethical and legal issues" of Annex II was completed by each LER (Local Ethics Representative), responsible for conducting trials involving human participants with a twofold scope: a) to capture the current status of ethical aspects/issues at each pilot site and b) to serve as a checklist reminding the researcher to consider all relevant ethical aspects before conducting any evaluation activities within SHOW, in view of the pilot phase (pre-demo the first to come).

The form itself is divided into 6 different subsections (e.g. participants and informed consent, ethical control instruments, privacy, safety, risk assessment and reimbursement).

For the sake of the current Deliverable (D3.5) and in view of the upcoming final demo phase but also the pre-demo phase for the sites that have not yet launched it (the pre-demo phase is on-going already at the time of this Deliverable issue for some of the test sites), this Questionnaire has been redistributed to the Mega and Satellite test sites to lead to an updated summary of the status across the test sites, when and where necessary. In addition, information has been collected and added for the new test site of Carinthia (replacing the Vienna site in Austria), as well as by the Salzburg site that was not included in the previous version due to COVID-19 related delays in collecting all necessary information concerning the relevant site's operation.

Out of all the reviewing work of this period, it has emerged that all collected data will be kept entirely confidential and their anonymity will be protected in full across all sites, as dictate by the SHOW Ethics Manual.

Field trials data management will be carried at all pilot sites according to General Data Protection Regulation (GDPR) (Regulation EU 2016/679) and the project data management procedures identified already in the D14.2: Data Management Plan (DMP) and further elaborated in its update D14.3: DMP – final version. Furthermore, it is the LERs in continuous collaboration with their entity's Data Protection Officer (DPO), when existing and when applicable, who will guarantee the compliance of the project data related activities with the GDPR regulations.

In the following paragraphs, the updated results for all SHOW demonstration sites and their data collections are summarised for each subsection. It should be noted that the following updates have excluded the demonstration sites that are not applicable for several reasons currently in the project (as explained in the previous sections), while the follower sites relevant information will be explored in a later stage in the project and reported respectively in D12.8: "Follower sites multiplication plans and actions, to the extent applicable".

For the Mega- and Satellite sites, final monitoring findings will be reported in D11.3: "Pre-demo evaluation activities" and D12.9: "Real-life demonstrations pilot data collection and results consolidation" respectively.

4.2 Participants and informed consent

The Controller/Processor must have a valid lawful basis to Process Personal Data. Among the SHOW sites that completed this questionnaire, six (6) of them (Carinthia, Copenhagen, Karlsruhe, Rouen, Salzburg, Trikala) stated that there is an international or national legislation (or institutional regulation), which they must follow when performing tests within SHOW project, involving healthy human participants, while six (6) of them (Copenhagen, Karlsruhe, Linköping, Rouen, Salzburg, Trikala) stated that there is respective

legislation/regulation for the involvement of participants with cognitive impairments/learning difficulties and five (5) of them (Copenhagen, Rouen, Salzburg, Trikala, Turin) for involving illiterate or with co-morbid conditions participants.

The GDPR sets a high standard for consent, while also 8 of the SHOW sites (e.g., Brainport, Brno, Copenhagen, Karlsruhe, Rouen, Salzburg, Trikala, Turin) are also obliged according to their national/regional/institutional regulation to obtain the consent of pilot activities participants. This means that there will be differences among the sites when it comes to the relevant lawful basis for Personal Data depending on the type of organization. Still, all relevant information will be given to the participants of all test sites in SHOW.

Each demonstration site will edit the required templates of the informed consent/assent forms and information sheets, according to their main research objectives per demonstration phase and will define the procedures regarding the collection, storage, and protection of personal data, in compliance with the European and national legislation and the project established processes and mechanisms, but also in relation to the local logging processes, when to the extent applicable. The information sheet and informed consent templates can be found in Annexes I to VI of D18.1. The signed forms, whenever required, will be kept locally and will be available upon request.

All demonstration sites representatives have confirmed that the informed consent will be provided/translated in a manner to be understood by “the man/woman in the street”, while also all participants will be given sufficient time to reflect their decision of giving or withholding consent. Other than that, only two (2) of the test sites are anticipated to conduct tests with individuals without having the necessary cognitive capacity and/or ability to consent; in specific, children are planned to participate in evaluation in Linköping and users with special needs and mental disabilities in Tampere (in the pre-demo phase in first place). In such cases, the provisions of the consent will be handled through their parents (or other person/ adult legal representative of their interests) and they will of course also be informed and consent. The informed consent form will be translated into the national language of all test sites. Following the approval of the informed consent by respective bodies, its translated version will be used with a small group of project participants to validate that the included information and the chosen form of presentation is appropriate and understood by the participants.

Moreover, five (5) of the test sites (Brno, Linköping, Rouen, Tampere, Trikala) stated that they expect to also have participants, who for any reason, will be unable to read the form by themselves (e.g. children or participants with severe visual impairments) and/ or illiterate participants). Thus, in all sites, participants not able to read will give oral consent, which will be witnessed by at least one person, whose name will be also recorded when recording the individual's grant of consent. In relation to that, twelve (12) of the test sites (Carinthia, Graz, Karlsruhe, Gothenburg, Linköping, Madrid, Rennes, Rouen, Brno, Tampere, Trikala, Turin) also declared that the oral consent of an illiterate participant in the presence of a witness adequate/appropriate is also in accordance with their national legislation and/or institutional protocols. The routines are the same regardless time of involvement of participants during the SHOW project.

4.3 Ethical control instruments

At nine (9) of the test sites (Brainport, Carinthia, Copenhagen, Graz, Linköping, Gothenburg, Madrid, Salzburg, Tampere, Turin) there is no ethics controlling body or controlling committee necessary to be contacted and get approval from (on national/regional/local/institutional level) for the experimental procedures prior to the evaluation activities, while some of them (e.g. Brainport) have internal review board on human research. Out of the ones that stated that there is a local ethics controlling committee/ controlling body that their organisation is usually obliged to get approval from, only the site of Trikala stated that in this specific case, it is not necessary for them to obtain this approval for the specific project, as the informed consent form process fulfils the requirement.

Moreover, some test sites stated auditing their ethical controls at division or department level (e.g. Brainport, Copenhagen, Madrid, Rennes, Rouen,) and/or on a laboratory or workgroup level (e.g. Tampere). The Salzburg site stated that ethical controls are only carried out on request at the ethics committee in Salzburg. Requests from Salzburg Research in the past were done at project level.

However, the Local Ethics Responsibles (LERs) will be contacted by the SHOW Ethics Board to ensure that the processes are conducted in line with the project's ethics policy and that no further action is necessary to be taken in relation to ethics approvals from regional bodies. An overview of the answers for each project pilot site reported in the "Questionnaire on ethical and legal issues" for the "Ethical control instruments" session has been reported in Table 4.

Table 4: Overview of the "Ethical control instruments" session by SHOW test site[21].

If there is a local ethics controlling committee that your organization will be obliged to get approval from for the experimental procedures before beginning with the experiment, will you obtain this approval?	Yes	No
Carinthia		x
Graz		x
Salzburg		x
Gothenburg		x
Linköping		x
Madrid		x
Rouen	x	
Brainport		x

[21] Not applicable test sites are not included in the tables of this section.

If there is a local ethics controlling committee that your organization will be obliged to get approval from for the experimental procedures before beginning with the experiment, will you obtain this approval?	Yes	No
Brno	x	
Copenhagen		x
Tampere		x
Trikala	(x)	
Turin		x

For those sites that Ethics approval is required at any level (institutional, national, etc.), the corresponding forms will be collected (the process has started already) and reserved internally in the project to be available upon request.

4.4 Privacy

Out of the Mega and Satellite test sites, five (5) stated that they will record no personal data during the SHOW field testing (Brainport, Carinthia, Graz, Rennes, Tampere). In case and to the extent this gets anticipated by the data collection requirements of the project, the collected data will be anonymous and with no association enabler in order to retrieve them. There might cases that for the accommodation of traveller services (e.g. on-demand services), there will be data storage of personal info; in those cases, data will be however anonymously stored, coded as will be instructed in the context of the project data processing mechanisms.

This is the case for subjective data collection during field trials that may contain personal data (e.g. demographics, etc.) but will be associated with no contact details or any other info that may infer associations revealing traveller identities. Indeed, the central to the project surveys, organised through Netigate tool, ensure this.

Also, in some sites that aim to recruit travellers, such as Linköping, banking and other financial information will have to be collected for payment or invoicing purposes. In this case, such info will be kept strictly locally by the respective department of the managing entity and will for no reason shared with any other department of the entity itself and, furthermore, with the project other entities. All in all, in all cases, participants will be informed that their data will be kept entirely confidential and that their anonymity will be protected and it will be indeed done as such.

The Local Ethics Responsible (see Annex IV) are the a priori identified persons and will be the only contacts having access to full contact details of the participants as well as to their consent forms that will be signed in all cases. Moreover, all sites have stated that there is a Data Protection Authority on national/regional level, as presented in Table 5. This, however, does not assume that a special permit is required for the SHOW field trials.

Table 5: National/ Regional Data Protection Authorities in SHOW test sites.

SHOW test site	Data Protection Authority
French sites	CNIL - https://www.cnil.fr/
Swedish sites	Swedish Authority for Privacy Protection (Datainspektionen) - https://www.imy.se/other-lang/
Carinthia	DSGVO Datenschutzgrundverordnung https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html
Graz	dsb – Datenschutzbehörde: https://www.data-protection-authority.gv.a
Salzburg	Datenschutzbehörde https://www.data-protection-authority.gv.at/
Karlsruhe	Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden- Württemberg https://www.baden-wuerttemberg.de/de/header-und-footer/datenschutz/
Madrid	Agencia Española de Protección de Datos - https://www.aepd.es/es
Brainport	Autoriteit Persoonsgegevens - https://autoriteitpersoonsgegevens.nl/e
Brno	The Office for Personal Data Protection (CZE: Úřad pro ochranu osobních údajů) - https://www.uoou.cz/en/
Copenhagen	Datatilsynet - https://www.datatilsynet.dk/generelt-om-databeskyttelse/lovgivning
Tampere	The Office of the Data Protection Ombudsman - https://tietosuoja.fi/en/home
Trikala	Hellenic Data Protection Authority (HDPA) - https://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_sc a =PORTAL
Turin	Garante per la protezione dei dati personali, https://www.garanteprivacy.it/home_en

A Data Protection Officer (DPO) is also appointed at the respective organisation of almost all sites that have completed this questionnaire. The contact details of those DPOs have been also collected and are included in Table 6.

Table 6: Data Protection Officer at SHOW test sites.

SHOW demo	Data Protection Officer	Contact Details
Rouen	Transdev Group has appointed a DPO (**Martial Michaux**) and because Transdev Group has more than 300 subsidiaries, numerous people are responsible for the implementation of Transdev Group policies locally. For Transdev Group Innovation: Mihai CHIRCA and Valerie AICHOUN are in charge of the questions relating to GDPR.	martial.michaux@transdev.com mihai.chirca@transdev.com
Carinthia	**Jennifer Amritzer**, MSC, Technical Manager	jennifer.amritzer@suraaa.at
Graz	No DPO at Graz. A Data Protection team is established instead, consisting by Mario Rumpf and Ulrike Fleischmann.	mario.rumpf@v2c2.at
Salzburg	A DPO has not been designated – see clarification below.	
Karlsruhe	**Daniel Vonderau**	(vonderau@fzi.de)
Goethenburg	**David Ericson** (& Mattias Wadsten for KEOLIS overall)	dpo@ri.se (& mattias.wadsten@keolis.se)
Linköping	**Louise Dahlgren:** Personuppgiftsansvarig	vti@vti.se
Madrid	**Francisco Ramón González Calero Manzanares**	FranciscoRamon.GonzalezCalero@eradrid.es
Brainport	**Remy van den Boom** LL.M	https://www.tno.nl/en/about-tno/contact/corporate-legal/privacy-statement/
Brno	**Tomáš Habán** (Head of legal department)	tomas.haban@cdv.cz

SHOW demo	Data Protection Officer	Contact Details
Copenhagen	**Tina Cort Pedersen** (Datasafety)	tcp@moviatrafik.dk
Tampere	**Reijo Kukkonen** (Quality and Safety Director)	Reijo.Kukkonen@sitowise.com.
Trikala	**Loukas Vavitsas**	lvavitsas@e-trikala.gr
Turin	**Andrea Pautrè** (GTT) - In GDPR the DPO is foreseen for all public authorities and it does not apply to Fondazione LINKS.	

The only site, where a DPO has not been designated is Salzburg. SRFG does not have an appointed Data Protection Officer but is does have a central contact point: datenschutz@salzburgresearch.at. According to Article 37 (1) GDPR a company is obliged to examine the need of a data protection officer. Each company has to do this on its own responsibility and the decision is based on the fact whether the core activity of the company comprises (extensive) processing of sensitive data. SRFG has carefully investigated this and concluded that there is no need to appoint a DPO.

Finally, all sites had stated their intention to clarify to the SHOW participants that all data collected in the activities they are participating in will be kept entirely confidential and that their anonymity will be protected in full, while nine (9) of them (presented in below) have identified persons (inside their entity) and according to their positions/roles in their entity, who are authorised to have access to the data collected and / or who have access to any data storage devices, both, paper-based and electronically, in addition to LERs (if not already being the LERs themselves) and the local data processors as listed in section 5.8.

Table 7: Authorised persons with access to collected data in SHOW test sites.

SHOW test site	Authorised persons with access to collected data	Contact Details
Rouen	This is detailed in internal policy documents	
Linköping	Dr Anna Anund, Research director, HF	anna.anund@vti.se
Gothenburg	Jan Jansson & Johnny Melander	Jan.jansson@keolis.se; johnny.melander@keolis.se
Madrid	Sergio Fernández Balaguer. Jefe de Departamento de Proyectos de Colaboración Internacional	Sergio.Fernandez@emtmadrid.es
	Jesús Perucha Ramos. Seguridad de la Información	Jesus.Perucha@emtmadrid.es
Brainport	Only staff involved in the SHOW project on a need-to-know basis.	

SHOW test site	Authorised persons with access to collected data	Contact Details
Brno	Mr. Marek Vanžura, Head of Autonomous driving department	marek.vanzura@cdv.cz
	Mr. Václav Linkov, Researcher/Psychologist,	vaclav.linkov@cdv.cz
	Ms. Kateřina Bucsuházy, Head of In-depth road accident analysis department,	katerina.bucsuhazy@cdv.cz
	Mr. Ondřej Maceja, Researcher	ondrej.maceja@cdv.cz
Copenhagen	Tina Cort Pedersen, Datasafety	tcp@moviatrafik.dk
Trikala	This will be detailed in internal policy documents	
Turin	Brunella Caroleo, Senior Researcher	brunella.caroleo@linksfoundation.com
	Michal Rataj, Junior Researcher	michal.rataj@linksfoundation.com
	Maurizio Arnone, Head of Research Area	maurizio.arnone@linksfoundation.com

4.5 Safety

The majority of the SHOW test sites (10) have stated that they will not provide information to the SHOW participants about any participant's illness that is detected, mainly due to the fact that no medical data will be recorded or collected in any way. Some of them excluded though the cases of COVID-19 infections (that may turn to be a European regulation in any case).

Moreover, fourteen (14) of them stated that their pilot implementation will be evaluated for any side-effects and that they have in place written procedures (or dedicated training session) for safety for employees and volunteers within their own group or institution (i.e. the safety drivers participating), mainly governed by the internal safety and quality protocols, while some of them also made distinction between general safety procedures and special safety regulations regarding COVID-19.

4.6 Risk assessment

Regarding the risk-assessment, concerning breach of privacy and / or breach of safety in the different sites, almost all test sites stated that they will perform one. In Table 8 below, a brief outline and/or justification for each test site is presented. It is worth stressing, that in most cases, such a process is anyway a requirement for getting a permit.

Table 8: Overview of the risk assessment" performance per test site.

SHOW test site	Yes	No	Brief outline/ Justification
Carinthia	x		They are performing a risk-assessment once per year.
Graz	x		A risk assessment concerning safety will be performed. This assessment covers systematically all sections of the test area and assesses the safety hazards, probabilities and corrective actions by the safety driver. A risk assessment concerning privacy though, will not be conducted, since no personal data will be recorded.
Salzburg	x		Chances and risks concerning the risk-assessment of breach of privacy and/or breach of safety are depicted in the quality management system of Salzburg Research. Salzburg Research is certified according to the new standard ISO 9001: 2015.
Karlsruhe	x		They will perform a risk-assessment, if necessary, according to established risk-assessment policies by internal guidelines and guidelines created by data protection authorities.
Goethenburg	x		They will do GDPR and Privacy audits as well as Information security audits before starting test on the site (requirement for getting permit in Sweden anyway).
Linköping	x		A local risk assessment is done as a part of the permission and is then continuously followed up.
Madrid	x		To be considered, to meet the project practices and requirements.
Rennes	x		The cyber security of the site and of data will be assessed through a protocol to be drafted during the pre- demo period.
Rouen	x		A clear policy is realised in order to deal with eventual breach problems.
Brainport	x		To be considered, to meet the project practices and requirements.
Brno	x		It is a standard procedure done according to our institutional policies.
Copenhagen	x		Part of the national test-approval that have to be obtained in order to conduct the test.

SHOW test site	Yes	No	Brief outline/ Justification
Tampere	x		To be considered, to meet the project practices and requirements.
Turin	x		A periodic review of the entire plant and individual legal obligations is envisaged, with reference to the As-Is and the indication of the measures deemed necessary in order to mitigate the risks to the rights and freedoms of data subject.
Trikala	x		To be considered, to meet the project practices and requirements.

Moreover, more than half of the test sites (Carinthia, Graz, Linköping, Gothenburg Rouen, Salzburg, Brno, Copenhagen, Tampere) stated that their organisations are insured against risks as a result of breach of privacy and safety and that this is a typical part of their business operations (i.e. TRANSDEV, KEOLIS), while 13 sites stated also that they will not need to involve other organisations (entity, unit, division, department, etc.) for conducting research and management of the risks, other than the national Transport agencies that are naturally involved in the process in order to grant permit to the site.

4.7 Compensation and Reimbursement

Demonstration sites may set up incentives to be offered to participants in field trials but these will be subjected to approval of the SHOW Ethics Board. Instead of cash, reimbursement may be in the form of vouchers, the possibility to share results of the study, charitable donations, etc.

However, the vast majority of the SHOW test sites eleven (11) have stated that reimbursement practices are allowed in their country/region/institution, while 9 of them stated that, also despite of the regulation allowing it, no financial or in kind payments (including reasonable expenses and compensation for time of participation) will be offered to participants for participating to their field trials in the context of SHOW. Only 1 test site so far (Copenhagen) stated that compensation for participation will be in the form of small cash payments (> 40 euro) and Salzburg representatives also stated that this needs to be defined and might be a potential.

5 Data Privacy Impact Assessment

This Chapter focuses on the central to the project Data Privacy Impact Assessment and, in specific, in relation to the data exchanged, stored and processed in the context and for the sake of the evaluation activities of the project. Other personal data that may fall in other types of activities in the project, as listed under section 3, are not dealt within this section, as they are not deemed applicable for a Data Privacy Impact Assessment. Examples of such cases are as follows:

- The A3.3 survey on local regulation of shared CCAM. This survey has been anonymous, but we allowed respondents to indicate whether they were available for follow-up interviews, if they ticked the box they had to include their name, contact details and the name of their organisation.
- For WP17 Follower Site recruitment, applicants had to provide the name, contact details and organisation to allow us to contact them; if selected they will be asked if they want to be included in project internal contact lists.
- Local focus groups and dissemination events that have or will be convened in the course of the project and will follow similar principles as above. Registration to such type of events typically requests for name, company, email address, job title, department, etc.
- Subscription to the project newsletter, where people are asked their e-mail address.
- Subscription to the project Stakeholders Forum that have to provide name, organisation, website, email, type of company, country and reasons why they want to join.
- Collected personal data is only used in each case to get in touch with the respondents in order to serve the specific scope in each case and is not shared to any other than the controlling - in each case - SHOW entity and, of course, to external to SHOW entities. In each of the above cases, a GDPR specific clause - conforming with the data protection policy presented in this document - has been added. The SHOW data protection policy is reflected also at the disclaimer present in the project web site at: https://show-project.eu/disclaimer-policy/ (and in accordance with the GA, as already explained in Chapter 3).
- The sections 5.1 to 5.7, present the updated central to the project DPIA. By central, it is meant that they refer to the central cross-cutting mechanisms and activities of the project that deal with data collection, processing, use and exchange of any type, related to the field trials and evaluation activities planned. On top of that, all test sites of the project[22], have identified if there is a need for conducting a DPIA on local level for their test site, at their own responsibility and following the advice of their DPO, when existing.

The status and relevant discussion for each test site DPIA, is provided in the closing section of this Chapter, namely section 5.8. In this context, local data controllers and processors have been identified in addition to the ones applying for the project in a cross-cutting level and listed in section 5.1.

Reasons for local DPIAs may relate to personal data that may be collected for site specific reasons and are not foreseen, however, to be collected in the central infrastructure of the project. It is also heavily dependent on whether traveller services will be deployed that will inevitably require the collection, in first place, and then processing and utilisation of traveller personal data,

[22] The ones current operating in SHOW and are not blocked for any reason/under amendment.

that will be stored, apart from the central digital infrastructure of the project, in the distributed data management platforms/repositories, if and when any.

5.1 Data Controllers and Processors in SHOW evaluation activities

According to GDPR principles:

- **Data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with other persons, determines the purposes and means of the processing of personal data. In SHOW this role is undertaken by the following entities on a cross-cutting level:
    - **VTI**, being the lead Partner coordinating the project evaluation framework and experimental plans subsequent issues (in the context of WP9), which implies that defines among other the data that needs to be collected for the assessment of SHOW.
    - **VEDECOM, IESTA, CTL-UP, BAX COMPANY** and **DLR**, as controllers of the user acceptance surveys content to be diffused in the context of the field trials.
    - **VUB,** being the lead Partner coordinating the project impact assessment work (in the context of WP9 and WP13) in collaboration with the other WP13 activity leaders, namely **NTUA**, **TNO**, **BAX&CO** and **CTLup** that monitor different aspects of the impact assessment.
    - **IDIADA,** being the lead Partner coordinating the project technical validation work in WP11.
    - **VIF,** being the lead Partner coordinating the project simulation work (in the context of WP10) in collaboration with the other WP10 activity leaders, namely **FZI, AIT and NTUA** that monitor different aspects of the simulation work.
    - **CERTH** in collaboration with **RISE,** being the lead Partners that will actually make the final decision, collect, classify, process and visualise in a centralised to the project way all the performance data originated from the test sites of the project and different ends of their cooperative context (vehicles, digital and physical infrastructure, services, terminals) in the context of WP4, WP5 and WP6. **CERTH, CTL & DTU** are also deciding the data required for the AI services to be developed in WP5.
- **Data processor,** on the other hand, is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller and under its guidance. In SHOW, data processors are all entities participating in field trials or contributing to them in each local ecosystem. It may be also the case that external to SHOW parties are involved here, e.g. the holders of the physical infrastructure. On top of them, some of the above controllers are also processors in a cross-cutting way in the project, as they will be dealing also with the processing of the data. In specific, the following partners have been so far identified to be involved with the processing of either subjective of performance data for research reasons: **CERTH, IDIADA, DLR, CTL, VEDECOM, EUROMOBILITA**, **JRC** (technical verification and validation data processing), **FVE** (pre-demo phase data processing), **VUB**, **AVL** (Netigate central data processor) and **VTT** (final demo phase results lead processor). It is not impossible that more will be identified in the course of the project.

It is reminded that the above entities apply for the **cross-cutting to the project treatment of (different types of) data in any sense**. The local to the test sites treatment of data is handled by local data controllers and processors as explicitly identified in section 5.8. Apart from that, and as already mentioned at the Introduction of this Chapter, other type of surveys

– not directly related to evaluation – will relate to other specific entities as data controllers and processors.

5.2 Why do we need a DPIA in SHOW (Step 1)

SHOW is a large-scale Innovation Action that aims to bring together a vast array of technologies in the CCAV sector, deploy a series of passenger and logistics transport services and, at the end, assess the impact of its solutions across a series of aspects enabling also their projection to wider populations through further simulation studies.

As it is natural, in order to achieve those goals, and primarily answer its KPIs (see the list of KPIs in *D9.2: Pilot experimental plans, KPIs definition & impact assessment framework for pre-demo evaluation*) it will collect a series of data at a relatively big length for different purposes.

The key clusters of data that will be stored/processed in SHOW are as follows:

- **Subjective data,** encompassing:
  - *demographics* (age, sex, country/place of residence, education, working experience, entity and position/role in entity) that are being asked in the context of the project passenger and stakeholder acceptance studies and interviews in the context of the field trials, but, also, similarly in the context of surveys, focus groups, workshops, etc.;
  - contact details of participants (name, surname, e-mail, address, banking details of participants for invoices, for follow-up actions, or other reasons, etc.);
  - general views on CCAV - needs & preferences;
  - assessment of SHOW solutions;
  - feedback for co-design of SHOW solutions or other mechanisms enabling SHOW solutions;
- **Static data:** vehicle ID, manufacturer, model, seating capacity, standing capacity, push chair capacity, wheelchair capacity, max payload, service mode, automation level, energy type
- **Dynamic data**: connection status, location, energy level, soc, speed, odometer, occupancy, door status, violation of door ,dispatch status, orientation, heading, acceleration, navigation mode, steering angle, GNSS connection, cargo, payload, cargo pickup location, cargo drop off location, cargo transported, prams on board, wheelchair on board
- **Event based data**: event, type of event, located event, alarm, emergency notifications time, emergency notifications location, incident notification time, incident notification location, vehicle is driving in reverse, vehicle is braking, strong braking, severe braking, shuttle switched to manual mode, dui: klaxon triggered, dui: buzzer triggered
- **Service data**: stop places, lines, routes of each line, service area, passing time, timetable planned, timetable actual, operating day
- **Booking/ride data**: passenger location, passenger destination, timestamp, vehicle load, vehicle availability, desired pickup location, desired pickup time, desired drop-off location, desired drop-off time, planned pickup location, planned pick-up time, planned drop-off location, planned drop-off time, actual pickup location, actual pickup time, actual drop-off location, actual drop-off time, planned booking route, actual booking route, direct ride distance, direct ride duration, actual ride distance, actual ride duration, trip reason

- **External data**: temperature, pressure, humidity, temperature min, temperature max, , weather main, weather description, city traffic, maps, parking, parking bay, parking capacity, parking properties
- **Other digital infrastructure data** recorded from: video – internal & external cameras/surveillance systems on AVs and infrastructure end, magnetic loops, lidar sensors, cameras installed on traffic lights or bridges, video - external cameras, radar sensors, radio frequency sensors, Bluetooth sensors, sensors for capturing wireless internet traffic, network traffic metadata, 5G stationsThe full detailed list of performance data asked to be shared centrally to the project is part of the project fully defined Data Registry. Data will be stored and processed by CERTH at the SHOW Data Management Platform.

The subjective data asked in the context of the cross-cutting user acceptance surveys, out of the ones listed above, are the *demographics*, the *general views on CCAV - needs & preferences* and the data related to the assessment of SHOW solutions;

The reason for conducting a DPIA lies basically in the identification of any potential of tracking and processing, in any way, of personal identifiers.

To the current knowledge of the Consortium, this might be the risk in collecting booking/ride data during services deployment. Also, data coming from the internal and external cameras, Network traffic data, Bluetooth sensor, Wheelchair on board and Passengers with special needs. Network traffic data include Username, Password, IP address, MAC address, session and, maybe, cookies.

As concerns the data that comes from the vehicles' sensors, the format in which the information will be provided is aligned with all the security measurements. The determination of each vehicle is based on three identification numbers; the site, the fleet and the vehicle. Therefore, the cross-checking of what data belongs to a specific vehicle is infeasible even for the technical team of SHOW Data Management Platform.

The central processing of the subjective data prohibits totally the tracking of any association to specific persons, as this process is handled through Netigate tool. Any personal identifiers may be available only on local level and will never be shared with the project. Please see more about this specifically in section 5.8.

5.3 Describe the processing (Step 2)

During the project, a centralized data collection will be managed with regard to the activities to be held in the field trials of the two rounds, namely the pre-demo and the final demo phase.

As already mentioned, subjective data will be handled through Netigate tool for all test sites. Netigate is password protected. The key data processor having full data access is AVL in this case. Still, data will be shared with some of the central data processors, listed in previous section, and, also, with the local data processors, listed in section 5.8, as part of the results analysis, simulation and impact assessment activities. All data are extracted in a spreadsheet.

Still, it is emphasized that there is absolutely no potential for tracking any personal identifiers through the subjective data collection in this manner. As such, no matter to which entities the data is shared, there is 0 risk identified.

Other than that, the rest subjective data that will be collected during focus groups, workshops, etc. that do not constitute part of the field trials will be managed on local level on an anonymisation manner and only the processed aggregated results will be communicated further to the Consortium. Personal data in this end (e.g. e-mail, banking details) will be treated as

described above in the Deliverable and in section 5.8, with only the designated persons having access to them.

The performance/objective/observation data on the other hand, is collected through two main mechanisms. The first one supports the real-time provision of the data and is the Kafka broker. The connection is established taking into account the architecture of each site under the surveillance and assistance of WP5 technical team. The procedure is simple enough. The second one supports the historical data provision and the main component is the commercial open-source CKAN platform. The organizations are registered as unique entities and are able to upload and manage only their own datasets. In both connections, all the required cybersecurity measurements have been established. A main functionality of the SHOW Data Management is the access to the partners that are responsible for the implementation of services and impact assessment.

As mentioned above, data collection and processing will serve a series of scopes as follows:

1. Feeding and visualization of the project KPIs and other key metrics that will be determined during the project. Visualisation aims to be dynamic and address all pilot sites of the project and will be implemented through the project Dashboard.

2. Feeding the AI services that will be further developed in the project (WP5).

3. Feeding the assessment of the project in the context of WP11 and WP12 and according to the evaluation and experimental protocols that are/will be defined in WP9.

4. Feeding the impact assessment of the project across all layers specified in the context of WP13 and as determined in the impact assessment framework of WP9.

5. Feeding the simulation studies of WP10.

Final processing will be held by the respective Partners in the dedicated Activities according to the work allocation anticipated in the project.

Still, first level processing of most data will take place in the SHOW Data Management Platform of A5.1 (see D5.1 for its description). Data collected will be encrypted and be protected further by the cybersecurity mechanisms that have already and will be developed, as they are described in D4.1, D4.3 and D5.1. In the SHOW Data Management Platform, the data of all the partners is translated into the common terminology as it has been defined through the SHOW Data Registry. The data is cleaning and getting prepared for the calculation of the KPIs. Both initial data and calculated KPIs are saved in the database.

Full access in the data has only the administrators of real-time (Kafka broker) and the historical (CKAN platform). As it has been already mentioned, the parts that will deploy new services or need the data for the impact assessment should obtain access only in the data that is required for each case. The training of the models is feasible to be completed based on historical data. Therefore, the access will be established through separate groups in CKAN Platform that fulfils all the cybersecurity measurements. For the evaluation of the services, the real-time connection may be required. A dedicated API will be developed for the reason in order to avoid a direct connection in the Kafka broker.

Still, as defined in D5.1, those type of data adhere to the Privacy Policy that is described in D5.1.

5.4 Consultation process (Step 3)

The consultation process in SHOW has been done under the auspices of ERTICO, being the Data Manager of the project, VTI, being the leader of the respective Activity in the project and CERTH being heavily involved in data controlling and processing in the project. The GDPR

regulation and in specific to automation has been explored, while the different interpretations on local site level have been also analysed (and reported in section 5.8).

It is stressed also here that it is upon the liability of each test site and their DPOs to conduct a local DPIA.

On cross-cutting level, SHOW has conducted provisionally the current DPIA, with the collaboration of all above mentioned entities and all its test sites.

5.5 Assess necessity and proportionality (Step 4)

GDPR compliant informed consent forms (provided in D18.1) on one hand and the Privacy Policy described in this document and on D5.1 on the other hand are the key mechanisms that will be applied. The scope of the Privacy Policy in the D5.1 consists of two main parts; the data that origins from the passengers and the data provided by the sites for the needs of SHOW Project. The processing described above is vital to the project needs and cannot be skipped; any aspect of it.

Data minimisation has been achieved in first place by creating a *Data Registry* in the project that substantiates all project data needs in an aggregated manner. As such, data minimization involves limiting data collection to only what is required to fulfil the research purposes of the project, as already listed above.

This means also that any processing that will follow (the analysis of data to produce meaningful insight) will only use the least amount of data necessary. Within SHOW this feature is available through narrow data collection along with User verification and screening. Moreover, a progressive data management is adopted that is associated with a strategic deletion of data when they are no longer required. A data allocation procedure allows also for optimum utilisation within the SHOW ecosystem.

With regard to the subjective feedback, the principle of minimization is also applied by narrowing the surveys to the absolutely info required. Also, during any evaluation or other activity involving user feedback, an information sheet will accompany the informed consent forms where the purpose of the survey will be presented as well as the way the collected data will be treated by SHOW.

The processors will operate under the auspices of the Data Manager of the project (ERTICO; WP14), their controllers (defined in section 5.1) and their LER which operated under the auspices of the Ethics Board of the project. Also, whenever applicable, the processors will have to collaborate with their DPO. International transfers are applicable in the context of the project and according to Regulation EU 2018/1725, which states that international transfers may take place when there is an adequate level of protection to the fundamental right of individuals (data subjects) to data protection. Adequacy assessments will be carried out by those wishing to transfer data outside the European Economic Area (EEA) in collaboration with the DPO. Special safeguards are foreseen to ensure that the protection travels with the data. Specifically, the reform of EU data protection legislation offers a diversified toolkit of mechanisms to transfer data to third countries: adequacy decisions, standard contractual clauses, binding corporate rules, certification mechanism, codes of conduct, so-called "derogations" etc.

5.6 Identify and assess risks (Step 5)

Risks related specifically to DPIA objectives, dealing with data breach – and not tackled above in the context of ethics related risks – are presented in Table 9. It should be again reminded that the local to the sites risks are included in their local DPIAs, if applicable. Herein, only the risks related to data breach associated with the central mechanisms of the project, are mentioned. In specific, herein, by data we mean the performance data stored in the central SHOW Data Management Platform, as personal identifiers are possible only therein.

Table 9: DPIA related risks in SHOW.

#	Privacy issue	Risk to individuals	Compliance risk	Associated organization / corporate risk	Likelihood of harm [remote, possible or probable]	Severity of harm [minimal, significant or severe]	Overall risk [low, medium or high]
1.	Risk that the security of the data is compromised (i.e. data breach).	Risk that sensitive personal data is lost or stolen or destroyed causing distress or damage to the data.	Risk of breach of data protection legislation.	Risk of reputational damage to the project overall and the entity/entities involved and of enforcement action being brought. Risk to delivery of research objectives both current and in the future. Risk of complaints or litigation from affected individuals.	Remote	Significant	Low
2.	Risk that due to a data breach, the true identity of a user or a vehicle will be identified.	Risk that the real identity of a user or a vehicle will be identified. This means that, for	Risk of breach of data privacy legislation.	As above.	Remote	Significant	Low

#	Privacy issue	Risk to individuals	Compliance risk	Associated organization / corporate risk	Likelihood of harm [remote, possible or probable]	Severity of harm [minimal, significant or severe]	Overall risk [low, medium or high]
		example, the stored locations will be matched with a user and, thus, the locations of the places they most frequently visit (i.e. home, work, etc.) will be identified.					
3.	Risk that personal data is retained for longer than is necessary.	Risk that individual's data is held for longer than is required and that security and other organisational methods applied to the personal data lapse.	Risk of breach of data protection legislation.	As above.	Remote	Minimal	Low

5.7 Identify measures to reduce risks (Step 6)

Measures so far identified are presented in Table 10.

Table 10: Measures to reduce DPIA related risks in SHOW.

Risk	Options to reduce or eliminate risk	Effect on [eliminated; reduced; accepted]	Residual [low; med high]	Measure approved [Yes/No]
1,2	All identity data (site, fleet and vehicle ids will be encrypted before stored in the data repositories. Therefore, even in the event of a data breach, an attacker will not be able to de-hash the encrypted information (at a reasonable time) and identify the user's true identity or other info. The cybersecurity mechanisms of the project will further prevent data breach.	Accepted	Low	Yes
3	A process of completely deleting all stored personal data will be designed and developed, and it will be triggered by the system administrators at the end of the project. As defined in the SHOW Privacy Policy (of D5.1), SHOW will keep personal data and data from pilot sites only for the period necessary for the purposes identified, namely, as long as the user's login remains active and the pilot sites are agreed and the purposes for which it was collected remain; and may only be retained for longer periods, provided that they are processed solely for the purpose of scientific research or for statistical purposes.	Accepted	Low	Yes

5.8 Local DPIAs

In addition to the above DPIA that has been reviewed for the central to the project data collection and processing processes, during this period, the need for conducting or not a local DPIA has been recognised from the project test sites and is justified in the following table. This table should be read in conjunction with D14.3 that summarises on the GDPR templates completed by the test sites.

The local data controllers and processors listed below should be seen on top to the project central data controllers and processors that have been identified in the previous Chapter.

Whenever, a local DPIA has been or will be conducted in near future, it is/will be reserved locally and will be available upon request. This is also the case for the DPO related letters, whenever mentioned.

It is reminded that according to **GDPR Article 35 and WP29 DPIA Guidelines**:

1) A DPIA is not applicable when the vehicle data is used solely for local operations and research purposes.

2) An incidental finding may be defined as ‘a finding that has potential health or reproductive importance, unknown to the participant, which is discovered unexpectedly in the course of conducting research, but is unrelated to the purpose and beyond the aims of the study. In this project, we consider it highly unlikely that any incidental findings will emerge. Thus, we have no specific medical or psychological support roles to allow for analysis and counseling of participants if incidental findings were to appear. Therefore, the official policy for incidental findings is to refer any such findings to the relevant associations for them to deal with using their expertise in this area.

3) A DPIA is generally not required in the cases, when the action:

    1. Is not introducing a new and innovative data processing technology (for example combining face and fingerprint recognition for improved access)
    2. Does not use systematic and extensive profiling with significant effects on natural persons.
    3. Does not process special data or criminal offence data on a large scale that can be considered as increasing the possible risk to the rights and freedoms of individuals.
    4. Does not systematically monitor publicly accessible places on a large scale.
    5. Does not process personal data on a large scale in general, regarding the number of individuals, the volume of data, the duration and the geographical extend of the processing activity.

In this context, the SHOW field operations are highly unlikely to result in a high risk to data subject’s rights and freedoms so, a priori, there is no need to conduct a DPIA. Still, due to the local interpretation of the law, the differentiations across the test sites as well as the different core business activity of some SHOW beneficiaries, extending beyond SHOW, and, finally according to the mandate given by the responsible DPO, there are some SHOW test sites (or entities of them) that have conducted a DPIA or about to do so for the reasons explained in the following table.

As a summary of the findings presented in the table below, the following are being evident:

1. There are cases that the DPO of the lead entity(ies) of the test site have not recognised a need for conducting a DPIA. This is also dependent on the size of the test site, the core business of the entities involved or the type of equipment used on several ends (vehicles, infrastructure, etc.). Lastly, in some cases, this is also associated to the fact that a specific to SHOW DPIA may have not been conducted, but broader DPIAs, covering automated operations and, also, in this context, SHOW specific ones, have been done in a cross-cutting way from some SHOW beneficiaries (i.e. in KEOLIS, TRANSDEV, GTT, etc.).

2. In any case, it can be safely assumed, either as a result of the local DPIA or as a reason for not conducting one, that the risk of data privacy breach is very limited, for the following reasons:

    a. There is primarily no intention to collect personal data in SHOW as it is evident in the way the user acceptance surveys have been implemented through Netigate tool, from where it is impossible to identify any associations to specific persons (no possible connection to a name of a person or an IPR address to get in contact with the responder), and also in the list of performance data that is requested to be provided by the test sites in the Data Management Platform of SHOW.

b. Even if, inevitably, some personal data is collected and temporarily stored (i.e. in the case of interviews or other types of transactions with passengers, for example for reimbursement reasons or with specifically recruited VRUs for dedicated to them solutions), responses/identifiers (i.e. VRUs tags), apart from being provided with consent, will be anonymised and will be not associated to the persons. No further sharing for no reason will take place with any other person or entities of the project without the acceptance of the LER and a clear None Disclosure Agreement.

c. As it can be seen below, the video streaming data from vehicle and infrastructure cameras/surveillance systems are either not recorded, or deleted after some hours, or if they are recorded, it is done according to the national law and for traffic safety analyses and risk assessment scope exclusively. Also, acknowledgement of video surveillance data are carried in the vehicles to be visible by passengers, safety drivers and other people interacting with them and being on their way. In neither case, any type of this data is shared with SHOW.

d. The data that will be collected within SHOW central repository are anonymised (even the vehicles of the fleets cannot be identified as such), are protected through encryption and cybersecurity mechanisms as discussed above and in D5.1, and is shared upon request, and in an encrypted format, with specific project entities dealing with data analysis for a specific goal (i.e. impact assessment in WP13, AI services in WP5). Furthermore, state of the art cybersecurity services, mainly based on AI models, will be also deployed during the SHOW project.

Finally, it should be stressed that the in between sharing of data in the local ecosystems are also reflected at the test sites architectures and data flows (as described in D4.3).

To conclude and on the basis of the following summarised reports, but, also, on the basis of the detailed local DPIAs, when existing, it can be assumed that the risk is never (at any test site) above medium and in most cases low, the effect on the risk is reduced, the severity of harm is minimal and the likelihood of harm is remote.

It is common belief in SHOW that no system is perfect. A data breach can happen despite the mechanisms and precautions applied. But it can result in no arm.

Table 11: Status of Local Data Privacy Impact Assessments in SHOW.

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
Linköping - Swedish Mega Site	VTI (EASYMILE & NAVYA)	Anna Anund (VTI)	Anna Anund (VTI)	Yes – VTI has conducted a DPIA.	The personal data that is collected in Linköping for the SHOW project are the data collected in surveys and interviews through Netigate. In case of need for temporary personal data storage, this will be anonymized and locally stored, accessed by the designated persons only. No other data is planned for since no incentives in terms of money etc. are planned to be used, and hence no addresses etc. will be needed. Data related to demand transportation is without a connection to personal data. Data related to vehicles are shared directly with CERTH/ITI in the context of the central data management that is protected via specific mechanisms. Vehicle video data is used only for traffic safety analysis. In the case of NAVYA .they have applied for authorization from CNIL (Commission nationale de l'informatique et des libertés) to process the data from cameras. This is not yet granted. As such, so far, they can only analyse data coming from

[23] According to GDPR, Data Controllers and Data Processors can be either entities or physical persons of entities.

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					anonymous sources like LIDAR, GNSS, etc. Thus, a DPIA (cross-cutting to NAVYA) is not yet applicable. In EASYMILE case, the SHOW deployed demonstrators do not even use cameras; they use only lidars. Thus, no DPIA has been deemed necessary on EASYMILE side. The above applies for all the other test sites as well where NAVYA and EASYMILE deploy vehicles.
Gothenburg - Swedish Mega Site	RISE Research Institutes of Sweden AB & KEOLIS	David Ericson (RISE)	Cilli Sobiech (RISE)	RISE has conducted a DPIA already. Keolis has also provided a formal letter.	The DPIA of RISE has been conducted covering the scope of all field trials planned. Data collected in SHOW is for evaluating the user needs/acceptance and the stakeholder views for research purposes. Personal data collected during the interviews and the passengers' surveys (age, sex, etc.) will be anonymized, will be provided upon informed consent. No names, e-mails or job titles will be collected anyway. No other data will be collected from RISE. As KEOLIS confirms in the formal letter sent, the cameras attached to the automated shuttles will not record any personal information and are used for real time traffic matters only, a vital part of the traffic safety. Hence, according to KEOLIS, a DPIA is not required for this service.

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
Madrid Mega Site	EMT	Francisco Ramon Gonzalez Calero Manzanares (EMT)	Francisco Ramon Gonzalez Calero Manzanares (EMT)	Yes – EMT has conducted a DPIA	The reason for conducting a DPIA has been due to the fact that the vehicles at Madrid Mega Site will carry exterior video surveillance cameras and although they will not record but broadcast in real time, a DPIA has been assumed provisionally significant for EMT. In the testing period, the images captured from the outside will be processed together with the information from the radars and sensors to improve driving safety and to perform all the intelligence and processing to allow autonomous driving. The images recorded by the video cameras are stored both in the on-board system and in the central servers, in an encrypted manner, so that their confidentiality and integrity is ensured throughout the life cycle of the images. Likewise, secure means of communication are used in the communication between the central servers and the systems on board the buses. The access application to the on-board CCTV system implements authentication mechanisms by means of a digital certificate. Security operators use your personal ID to authenticate in the System. The EMT Data Protection Service, Legal Advice, Technology, Transportation and Management have been involved to ensure the security of data. For the rest subjective data, the same applies as

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					described for other sites. If specific personal data needs to be locally stored, will be anonymized and access to personal identifiers is granted to the designated persons only.
Karlsruhe – German Mega Site	FZI	Nico Lambing (FZI)	Nico Lambing (FZI)	Not yet – will be done in view of the final demo phase.	Although the vehicles to be deployed in Karlsruhe are using a Lidar sensor, FZI has deemed necessary to proceed with a DPIA. The personal data related to subjective surveys will be treated in anonymity as already described for other test sites.
Rouen –French Mega Site	TRANSDEV	TRANSDEV	TRANSDEV	Yes – Done for broader to SHOW operations.	In collaboration with external legal experts one DPIA has been realised at TRANSDEV to cover the automated driving (use of external cameras for automated driving). Another DPIAs is under processing with their DPO, and it is related to other technological aspects (as supervision control centre, or as internal cameras in vehicles). All TRANSDEV DPIAs are not specifically related to a test site; they are working on a transversal approach. For personal subjective treatment, the principles described for other test sites are applicable here too.

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
Carinthia – Austrian Mega Site	pdcp GmbH (& NAVYA)	Petra Schoiswohl (pdcp GmbH)	Petra Schoiswohl (pdcp GmbH)	pdcp GmbH (leader of the test site) has already conducted a DPIA.	The DPIA conducted from pdcp GmbH is covering the scope of all field trials planned in the project. As stressed in the local DPIA, there is no personal data that will be stored by the test site itself. If this is the case, for example in the context of interviews with stakeholders, then those will be anonymized according to the national (Austrian) Data Protection Act 2000 (year 2018). The reason for conducting a DPIA in first place, was due to the camera installed in the interior of the autonomous shuttles of the company Navya as well as 2 cameras in the exterior area. Still, the project leaders do not have access to the camera recordings. Only the manufacturer of the automated shuttles has access to this data. These data/recordings are automatically deleted after 48 hours. They are solely for the safety of the passengers in the event of an accident or near-accident. Still, in any case, passengers are informed about the video recordings via stickers in the shuttles.
Graz – Austrian Mega Site	VIF, AVL, Yunex-	VIF	VIF	According to the formal letter sent by VIF DPO, the	There is no personal data that will be stored by the test site itself. If this is the case, for example in the context of interviews with stakeholders or during the exchange with passengers, then those will be anonymized with no

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
	Siemens Mobility			Graz partnership (VIF, AVL, Yunex-Siemens Mobility) confirm, that upon exploration, there is no need to conduct a local DPIA for Graz.	identifiers possible and will be in general processed in agreement with GDPR and the Austrian data protection law. In addition, the video data of the vehicles will be not be recorded (by AVL) during the field trials. The AVL-DRIVE system that will be deployed in Graz will be used to assess a lot of additional KPIs (as also promised in the SHOW Grant Agreement). This system includes a MobilEye camera, but the data is never recorded, but directly processed to identify objects around the vehicle. Apart from that, there is no other camera inside the vehicles that will record data of passengers and safety driver. The Lidar AVs are equipped with does not allow person identification. The smart cameras of the infrastructure are also used as black boxes. No trip booking is planned whereas passengers will be informed about the ride.
Salzburg – Austrian Mega Site	SRFG	Markus Karnutsch (SRFG)	Markus Karnutsch (SRFG)	Not done – Considered not applicable	According to Article 37 (1) GDPR, SRFG has carefully investigated this and concluded that there is no need to appoint a DPO, although it has a central contact point: datenschutz@salzburgresearch.at. An SRFG internal register for the registration of all data processing activities on project level has been

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					established. Internal procedures of Salzburg Research, that are defined in the quality management system (certified according to ISO 9001:2015 standard), define how personal and sensible data are stored and who has access to that data. In addition, chances and risks concerning the risk-assessment of breach of privacy and/or breach of safety are also depicted in the quality management system of Salzburg Research.All recorded personal data, if any, will be pseudonymised. No personal data will be processed in relation to specific users. The pseudonymised data is used for further processing. Evaluations are carried out for scientific purposes only. The data is saved and stored in accordance with the technical and organisational guidelines of Salzburg Research. Since no sensitive data is collected, a data protection impact assessment has not been deemed necessary.
Brno Satellite Site	CDV – Transport Research Centre,	Mr. Bohuslav Dokoupil (CDV)	Mr. Bohuslav Dokoupil (CDV)	Not done – Considered not applicable	As explained in the formal signed letter sent by CDV (Brno site leader) DPO, the test site does not expect the processing of personal data beyond previous DPIA or processes. In case, the need arises for personal data collection, then this will be anonymized. Initially, the site planned to collect video data of passengers in the vehicle

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
	ARTIN, City of Brno				and to analyze their emotional behavior, but because of the case law in current situation, the site decided not to proceed in this direction. The collection of this type of data is expected to take place as of 2024 – 2025, out of SHOW.
Brainport Satellite Site	TNO	Sven Jansen (TNO)	Sven Jansen (TNO)	Not done – considered not applicable	According to internal policies, an internal scan was carried out checking the need for a DPIA considering the currently foreseen activities in the Brainport. Outcome of this scan is that currently no DPIA is required, due to the nature of the field trials planned by TNO.
Turin Satellite Site	GTT	Gabriele Bonfanti (GTT)	IOKI, Stefano Buscaglia (Links)	Yes, GTT has conducted a DPIA broader to SHOW, covering also SHOW operations. Will also conduct one in view of the	GTT hasn't conducted a DPIA for the specific SHOW operations in the pre-demo phase, but will conduct one for the final demo phase. Still, GTT has already conducted a DPIA for on-demand services in general, according to the Provision nr 467/2018 by the Italian Data Protection Authority; this DPIA contained a risk evaluation that involved more data than the ones needed for this service, so it is more complete and precautionary, covering also SHOW activities.

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
				final demo phase.	The DPIA has been conducted by GTT due to the fact that the processing involves collection, recording, storage, consultation, possibly disclosure by transmission within the consortium partners of data which are necessary to book an on-demand ride on the autonomous shuttles. Passengers data collected and processed relate to first name, surname and telephone number of passengers; collected through the app and stored in a database. Access is provided to the designated persons only.
Trikala Satellite Site	eTrikala mainly (ICCS, CERTH, UNIGENOVA)	eTrikala	ICCS	Not done – not considered applicable (formal letter provided by DPO of eTrikala)	A priori, the operations and vehicles in Trikala site will not collect and provide the SHOW project with any personal, extra and/or sensitive data. In the limited cases, this will happen (i.e. during interviews, booking of trips, recruitment of VRUs for the dedicated applications), all data will be anonymized and access will be granted to the designated persons in each case. No personal identifiers will be traceable to other persons than those. For all personal data reported (if any), the names of the participants will be replaced with ID codes to maintain anonymity. In case of the existence of an online booking application, only the email will be asked. In all cases,

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					interviewees and passengers will provide consent. Also, participants will be informed if cameras are installed inside the vehicles for safety reasons as the Greek legislation framework states. In case of an internal camera inside the bus, it will be used only for monitoring and not recording. The purpose is to replace the vision of the driver by the vehicle's operator in the Control Room for passengers' safety. Even though Trikala automated vehicles will observe and map the environment, they will not share that data to the SHOW project and what is observed/mapped will be removed and deleted in the short term. According to the GDPR Article 35 and WP29 DPIA Guidelines, the Trikala Data Processing Activity is not likely to result in a high risk to data subject's rights and freedoms so there is no need to conduct a DPIA.
Tampere Satellite Site	SENSIBLE4	Timo Mustonen (SENSIBLE4) for vehicle data	Timo Mustonen (SENSIBLE 4) for vehicle data	Not done – not considered applicable	There is no need for a site-separate DPIA for Sensible 4 vehicles utilised in the SHOW project related pilot at Tampere, Finland. Sensible 4 privacy statement relating pilot vehicles (available at https://sensible4.fi/privacy-road-traffic/) summarises all the necessary activities and covers the Sensible 4 data procedures of the provided vehicles at Tampere site.

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
		Pekka Eloranta (SITOWISE) for subjective data	Pekka Eloranta (SITOWISE) for subjective data		In more detail, apart from the cases that limited subjective data may be collected locally and will be treated in anonymity as it has been already explained in other test sites, Sensible 4 collects and processes the following limited personal data depending on the specific case and time that relate to video images monitored and recorded in the dynamic mode (on-the-move) in the open public traffic during Pilot driving testing and operation by video cameras mounted on the pilot vehicles. Recoding takes place only during vehicle operation (movement on the road with brief stops on traffic lights, at bus stops, other obstacle detection) for the duration of the specific Pilot and during limited hours/day, which varies for each specific Pilot (details here). SENSIBLE4 does not conduct static video surveillance of one specific area 24/7. They also does not monitor same people or vehicles for the extended period of time. Also, they do not use recorded images for identification of people, vehicle owners or drivers. Their technology (software) does not have any features or tools that enable them to do so (no facial recognition, no tracking, no automated decision-making that can affect Your rights). They only process limited personal data of Data Subjects (video/photo images only) and not for the purpose of identifying, not for using these

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					data to disadvantage of Data Subjects, not used for any automatic decision making (Art. 11 GDPR). Their software does not have excessive data analytics – no facial recognition, no license-plates tracking, no automatic decision-making regarding Data Subject. Personal data is collected from cameras as a part of the entire vehicle technical data from its sensors, lidars and other special equipment. The remote Pilot operator and supporting technical team are watching all images in the video-stream in real time transmitted through the mounted cameras and vehicle computer during the Pilot Vehicle driving on the public road in the open traffic. Video-stream from the mounted cameras is also transmitted to the Pilot Vehicle's computer (PC) and driver manually saves recording on encrypted storage media. Limited number of their authorised technical experts format the recorded video into special files ("ROS bags"), that can be read only by an experienced IT expert. The formatted video-files are saved to the secured physical or cloud servers located in Finland. Transfer of files takes place in accordance with internal process of strict monitoring, ensuring safety of the data. Saved video files are modified and applied in the software development activities by a limited number of authorised experts for creation of a tool

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					teaching our autonomous-driving software system to recognize and detect obstacles, including people, animals, bicycles, other vehicles, buildings, traffic lights etc, where individual personalities are irrelevant (machine-learning). Video footage is also necessary to investigate technical incidents such as Pilot Vehicle malfunction, failure to react to the remote operator's command or the safety driver's action – information that is crucial for the further development of the safe and efficient technology for all Traffic Participants. Sometimes video footage is sampled into fractions of short-interval recording and transmitted for testing functioning of connection and correctness of integration with the monitoring centre located away from the Pilot Vehicle, sometimes in another EEA country; in such case a limited number of authorised employees of our customer, local transport authorities, fleet operator has access to the samples of the video footage for the described purpose. Technical measures like blurring or darkening images make them unrecognisable for the vehicle system, cause difficulty in detecting the object correctly as different from the other vehicles, trees, buildings. Additional processing (by applying special measures) during the data recording delays the video steam. Receiving information with delay,

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					the remote operator cannot ensure timely reaction, which may result in the traffic accident. If software system cannot efficiently differentiate people from other objects and traffic participants, predict human behaviour in the traffic in order to ensure future safety of its operation, the risk to Traffic Participants' safety significantly increases and software will never learn properly. These measures may also render video material unusable for the traffic accident investigation, as the vehicle prototypes are not currently equipped with the black-box devices due to absent regulation. Processing of the above defined data aims to: Ensure safe operation of the experimental Pilot Vehicle in the public traffic, prevent collision due to Vehicle malfunction, any damage to health and personal safety of the Traffic Participants, public and private property on the road and nearby – Task carried out in public interest, Art. 6(1)(c) GDPR (general public and property safety); Comply with general traffic safety rules applicable to passenger vehicles by operating a new technology prototype vehicle in piloting/testing mode -Controller's

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					obligation under law, Art. 6(1)(d) GDPR (comply with the applicable law on traffic safety). Allow for the Scientific research and development ("R&D") of the autonomous driving technology and software ("self-driving") that helps brining electrical vehicle operation to the next level of automation (SAE-4), ensure competitiveness of the European economy, automotive industry and leads to a safer traffic for all participants – Task carried out in the public interest, namely general scientific research, development of the new technology for the benefit of public, Art. 6(1)(e); Allow for Scientific R&D of the autonomous technology ("self-driving/connected/smart electrical vehicles") is also core business of SENSIBLE4 start-up company (SME), small private enterprise – Controller's legitimate interest, Art.6(1)(f); For performing legal obligations of technical support, services, back-end operation, repair, fixing malfunction, ensuring safety or other under the binding agreements with their customers, including public (EU and Finnish) funding authorities, project coordinating research facilities, private companies working on developing of the

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					self-driving vehicles – Controller's legitimate Interest, Art. 6(1)(f); SENSIBLE4 determines the reasonable and legally justified retention period defined as follows: In earlier Pilots and depending on the Pilot Vehicle type video-stream data may require manual back-up by the safety driver every 4 minutes, or it will be automatically erased. In more recent Pilots and vehicle-types, especially operated outside Finland, back-up process is automated; Live-feed video data is not stored in the camera equipment and only saved to the Pilot-Vehicle encrypted-PC and safely erased from the Pilot Vehicle PV entirely after completion of each Pilot; Daily recorded video feed during Pilot operation copied to encrypted storage media and securely erased from Pilot-Vehicle-PC and from the encrypted storage media not later than one week (7 days) from the recording; Video data is stored on SENSIBLE4 local-secured-servers utilised for the software development for the

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					duration of the system software development up to five (5) years from the end date of each Pilot; When IT experts process video data on the secured Company computers for the purposes of the software development, it is securely erased from the PCs after 6 months; Video feed recording evidence of the traffic accident will be stored for the duration of statutory limits applicable in the jurisdiction where the accident takes place in order to safeguard or improve legal position of the affecteTraffic Participants (for instance in relation to the statutes of limitations, litigation, or regulatory investigations) and can be provided to the authorities under request. During the retention period, SENSIBLE4 can at their own discretion at any time safely erase some old data and data-sets and replace them with the new data, more relevant to the R&D. After applicable retention period personal data will be securely erased from all SENSIBLE4 systems and devices, systems and devices of our data processors or joint data controllers in accordance with the law. SENSIBLE4 employs reasonably and technically available and necessary

SHOW test site	(Provisionally) applicable Test site Entities for conducting local DPIA	[23]Local Data Controllers	Local Data Processors	DPIA applicability and status	Discussion
					organisational, technical, and physical security measures in order to protect data from loss, misuse, unauthorised access, disclosure or theft. Where we engage third-party suppliers to provide services that enable them to access personal data (such as cloud services providers), we ensure their credibility, require them by contract to have sufficient security controls in place and comply with GDPR. Some of the safeguards they use include physical security of their premises, firewalls, VPN, multilayer authorization, restricted access, cloud storage, device and connection encryption, limited employee access, instructions on monitoring the access and use of data. Finally, there are no transfers of personal data between parties.

6 Conclusions

The current Deliverable stands for the SHOW Final Ethics manual & Data Protection Policy and Data Privacy Impact Assessment. It constitutes an update of the previous version released in the previous period of the project (D3.4). It provides the code for conduct of research integrity and includes the Data Protection Policy for SHOW but also the Data Privacy Impact Framework and the DPIA for the project, as well as the status of the local to the test sites DPIAs. The living Ethics Board of the project, the demo sites DPOs, as well as all the legislation and non-binding instruments to be considered by SHOW's Ethics Board are described.

The findings out of the ethics monitoring process conducted in this period have been updated in the document, in view of the on-going pre-demo and upcoming final demo phase. All the information provided in the current document, in the form or principles, processes and mechanisms, is mandatory to follow when involving humans in the SHOW activities, beyond the evaluation activities. The monitoring of ethics and GDPR issues in the project is a continuous process. While the current Deliverable, along with the final DMP of D14.3 finalise the basis for the principles and mechanisms to be applied, the next steps, some of which extent until the end of the evaluation activities of the final demo phase, are as follows:

1. Revision of the GDPR templates of D14.3 in the context of WP14, in view of the final demo phase.
2. Update of the LERs (Annex IV) ad hoc.
3. Update of the summary on the test sites Ethics Controlling Reports (following the template of Annex II) and as presented in the Chapter 3 of the current document, after the end of the pre-demo phase (to be reported in *D11.3: Pre-demo evaluation activities*) and after the end of the final demo phase (to be reported in *D12.9: Real life demonstrations pilot data collection and results consolidation*), including reporting of the test sites that for Amendment reasons are not reported in this document.
4. Signing the ethical checklist of Annex I (short overview of the Annex II questionnaire) by each LER for the pre-demo phase (currently on-going in the project) and the upcoming final demo phase. Completed ethical checklists will be collected and reserved internally at project level and will be available upon request.
5. Ethical approvals being collected (if needed) at demonstration site level for both pre-demo and final demo phases and reserved internally at project level and will be available upon request.
6. The corresponding information about the follower sites of the project, to the extent that is applicable, will be reported at *D12.8: "Follower sites multiplication plans and actions, to the extent applicable".*
7. When the need to convene a local DPIA has been identified (section 5.8), it will be done as such (if not already done) and will be reserved locally and available upon request. The same is valid in case that such a need has not been identified; an explicit declaration by the respective DPO will be granted, kept locally to be made available upon request.

References

"European Convention on Human Rights." World Encyclopaedia. 2005. Retrieved July 3rd, 2015 from Encyclopedia.com: http://www.encyclopedia.com/doc/1O142-EuropeanConventnnHmnRghts.html

American Psychological Association. (2002). American Psychological Association ethical principles of psychologists and code of conduct (standard 3.10). Retrieved July 1st 2019, from: http://www.apa.org/ethics/code2002.html

Charter of Fundamental Rights of the European Union. Official Journal C 34, 18/12/2000 P. 0001 – 0022.

Retrieved 1st July 2019 from:

Council of Europe. Additional Protocol to the Convention on Human Rights and Biomedicine, Concerning Biomedical Research. Council of Europe Treaty Series - No. 195 25 January 2005. Available from: www.conventions.coe.int/ Treaty/EN/Treaties/Html/195.htm

ICO.org.UK

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation.

SHOW (2021). D3.4: SHOW updated Ethics manual & Data Protection Policy and Data Privacy Impact Assessment. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

SHOW (2021). D5.1: SHOW Big Data Collection Platform and Data Management Portal. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

SHOW (2020). D18.1: POPD - H -Requirement No. 1. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

SHOW (2020). D18.2: POPD – Requirement No. 3. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

SHOW (2021). D9.2: Pilot experimental plans & impact assessment framework for pre-demo evaluation, Grant Agreement No. 875530.

SHOW (2021). D4.3: Open modular system architecture – second version, Grant Agreement No. 875530.

Annex I: SHOW Ethics checklist

Name of the investigator responsible for this project: (Name, email address)

1. Who is conducting the Pilot?

2. Title of the study

3. What is the purpose of this research study?

4. Who can take part in this study?

5. Why should a person consider joining this study?

6. If a person joined the study, can he/she change his/her my mind and drop out before it ends?

7. What exactly will be done to with a person, and what kinds of treatments or procedures will he/she receive?

8. What kinds of harm can a person experience in this study, and what will the investigators do to reduce the risk of harm?

9. What will the investigators do to make sure that the information collected on persons will not get in wrong hands?

10. What kinds of benefits can person expect from taking part in this study?

11. What kinds of benefit to others can come out of this study?

12. Will the persons get paid for taking part in this study?

13. Will the person or the persons health insurance company be charged for any of the costs of this study?

14. What can a person do if he/she wants to find out more about the study, or to complain about the way he/she is treated?

15. Will personal information be shared with any other partner of third party?

16. What will happen to any information given by a person and how will it be stored?

17. How long will personal information be stored?

18. Will the data possibly be commercially exploited?

19. Is SHOW Data Protection Policy regarded?

20. Is there any reason to conduct a DPIA?

	Please circle as necessary	
Is there a need for ethical approval?	Yes	No
If yes, has it been approved?	Yes	No
If yes, has it been uploaded to the Collaboration tool WP3/A3.1	Yes	No
Is the proposed research adequately designed, so that it will be of informational value	Yes	No
Does the research pose risks of physical or psychological harm to participants by usir deception, obtaining sensitive information or exposing them for risks in terms of safety and/or security hazards?	Yes	No
If risks exist, does the research adequately control these risks by including procedures such as debriefing, removing or reducing risks of physical harm, or obtaining data anonymously? If that is not possible, will the research procedures guarantee that information will remain confidential?	Yes	No
Will participants receive adequate feedback at the completion of the study, including a debriefing if that is necessary?	Yes	No
Have I as part of the project informed the Ethics Board about the ethical issues I have identified and of which I am aware?	Yes	No

Annex II: SHOW Questionnaire on ethical and legal issues

This questionnaire on ethical and legal issues has been filled in by the LERs (Local Ethics Representatives), responsible for conducting trials involving human participants. It is a checklist reminding the researcher to consider all relevant ethical aspects before planning and then conducting any data collection activities within SHOW. The questionnaire is divided into five subsections: Informed consent, Ethical control instruments, Privacy, Safety, Risk assessment and Reimbursement.

Questionnaire on Ethical and Legal issues

A) Participants and informed consent

1. **Are you (so far) obliged according to national/regional/institutional regulation to obtain the consent of pilot activities participants?**

   ❑Yes ❑ No

   If ***yes***, briefly explain which specific aspects of trials you currently obtain informed consent for: _____

2. **Do you intend to conduct pilots in SHOW with individuals who might not understand the informed consent forms that will be used in SHOW?**

   ❑Yes ❑ No

   If ***yes***, briefly explain the procedures you currently follow in order to obtain informed consent in such cases: _____

3. **Is there any doubt about the anticipated SHOW pilot trials individuals' cognitive capacity to consent (if known already)?**

   ❑Yes ❑ No

   If ***Yes***, please clarify who will provide consent in such instance: _____

4. **a) Will the informed consent provided in common language to be understood by "the man/woman in the street"?**

   ❑Yes ❑ No

   If ***no***, why not?

   b) Will the participant be given sufficient time to reflect their decision of giving or withholding consent?

   ❑Yes ❑ No

If ***no***, why not? Please indicate the time to be given to the participant.

5. **Do you believe that any of the participants will be unable to consent in any way for any reason?**

   ❑Yes ❑ No

   If ***yes***, **no experiment should be performed since these participants are excluded from SHOW trials. Please list here each excluded case.**

6. **Do you believe that there will be participants, for any reason, unable to read the form by themselves (there is a range of people who are unable to read the consent form; these include those who have severe visual impairments, e.g. cataract, glaucoma)?**

   ❑Yes ❑ No

   If ***yes***, be advised that any participant that will not be able to read must give oral consent which has to be witnessed at least by one person. If that will be the case, please ensure that you will record the name of the witness when recording the individual's grant of consent.

7. **Do you believe that there will be illiterate participants??**

   ❑Yes ❑ No

   If ***yes***, be advised that an illiterate participant has to give oral consent which has to be witnessed at least by one person. If that is the case, please name the witness (in case of controlled trials):

8. **Is the oral consent of an illiterate participant in the presence of a witness adequate/appropriate in accordance with your national legislation (and/or institutional protocols, if any)?**

   ❑Yes ❑ No

9. **Is there an international or national legislation (or institutional regulation), which you must follow when performing tests within SHOW project?**

   a) involving healthy human participants?

   ❑Yes ❑ No

   If ***Yes***, please give details (reference number and short description of how you will assure compliance):

   b) involving participants with cognitive impairments / learning difficulties?

   ❑Yes ❑ No

   If ***Yes***, please give details (reference number and short description of how you will assure compliance):

c) involving *illiterate* or *with co-morbid conditions* participants?

❑Yes ❑ No

If ***Yes***, please give details (reference number and short description of how you will assure compliance):

B) <u>Ethical control instruments</u>

10. Is there a local ethics controlling committee/ controlling body (on national/regional/local/institutional level) that your organisation will be obliged to get approval from for the experimental procedures before beginning with the experiment, will you obtain this approval?

❑Yes ❑ No

If ***Yes,*** will you **obtain this approval?**

❑Yes ❑ No

If ***Yes,*** please give details of the relevant body and shortly describe the specific procedure:

If ***No***, please explain what is your current practice respectively:

11. At which level of your organization / enterprise, *ethical controls* are audited?

❑ laboratory or workgroup

❑ division or department

❑ institution

❑ regional

❑ national

12. If there is an established ethical control procedure which you must follow before performing tests, please explain how you will assure compliance when performing tests with:

a) healthy participants:

b) participants with cognitive impairments/ learning difficulties:

c) illiterate or with co-morbid conditions participants:

C) <u>Privacy</u>

13. What personal data of pilot participants will be recorded as part of the trials? Please list them here and explain how they will be recorded:

14. Is there any Data Protection Authority on national/regional level?

❑Yes ❑ No

If *Yes*, please provide its name and url to it (if any):

15. If there is an established Data Protection Authority issuing procedures / standards you must follow before performing tests with human participants and their personal data:

a) Please state if they are applicable for SHOW trials:

❑Yes ❑ No

b) If *Yes* above, please explain here how you will assure compliance (according to current practice):

c) If *Yes* above, please give a url to them (if any) and provide a short summary of them:

d) If *No above*, explain why they are not applicable in SHOW case and how you plan to deal with data protection issues (according to current practice):

16. If there is an appointed Data Protection Officer at your organization, please share here the contact details (name, position, e-mail) of that person:

17. If there is not an appointed Data Protection Officer at your organisation, please explain why it is the case:

18. Will you follow or are you aware of any official national or international guidelines on protecting privacy?

❑Yes ❑ No

If ***Yes***, please give a brief outline and provide references:

19. Do you intend to clarify to the SHOW participants that all data collected in the activities they are participating in will be kept entirely confidential and that their anonymity will be protected in full?

❑Yes ❑ No

20. Will you identify persons (in your entity) and their professions/positions who are authorised to have access to the data collected and / or who have access to any data storage devices, both, paper-based and electronically?

❑Yes ❑ No

If *Yes*, please give a list of those persons contact details (names, position, e-mails):

If *No*, please explain why you are not doing so:

D) <u>Safety</u>

21. Will you provide information to the SHOW participants about any participant's illness that is detected (if relevant)?

❑Yes ❑ No

22. Will the pilot implementation at your site be evaluated for any side-effects?

❑Yes ❑ No

If ***Yes***, please give a brief outline of it:

23. Will you have written procedures for safety for employees and volunteers within your own group or institution?

❑Yes ❑ No

If ***Yes***, please give a brief outline of it:

If ***No***, please explain the reasons briefly or what corrective actions you take:

E) <u>Risk assessment</u>

24. Will you perform a risk-assessment concerning breach of privacy and / or breach of safety at your site?

❑Yes ❑ No

If ***Yes***, please give a brief outline of it:

If ***No***, please explain the reasons briefly refer to any corrective actions you will take:

25. Is your organisation insured against risks as a result of breach of privacy and safety?

□Yes □ No

If ***Yes***, please give a brief outline of it and state the insurer, if possible:

If ***No***, please explain the reasons briefly and state who would cover any insurance-related costs:

26. For conducting research and manage the risk, do you need to involve other organisations (entity, unit, division, department, etc.) that might influence your research activities and/or your ethical and legal conduct?

❑Yes ❑ No

If ***Yes***, please give a brief outline of it:

F) Reimbursement

27. Is reimbursement practices allowed in your country/region/institution?

❑Yes ❑ No

28. If *Yes*, will financial / in kind payments (including reasonable expenses and compensation for time of participation) be offered to participants for participating to your demonstration trials in the context of SHOW (applicable only for pre-demonstration phase or in-depth controlled trials part of final demonstration phase)?

Another factor that may cloud the judgement of a potential participant when deciding whether or not to participate in research is whether money or payments in kind (e.g. gift vouchers) will be offered. It is reasonable for expenses and compensation of time to be offered. However these should not be so large that a participant is more concerned about what s/he will be receiving rather than the risks involved with the research. If children will be involved, then the researchers might consider the fact that what an adult considers to be a reasonable expense/compensation might be very different from a child's perspective (i.e. a child may consider 10 Euros to be a huge reward and, therefore, the 10 Euros might unduly influence a child's decision as regards whether or not to participate).

❑Yes ❑ No

If ***Yes***, please give a brief outline of it:

Annex III: Data Privacy Impact Assessment (DPIA template)

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of the LER person	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as relevant deliverables and other supportive documents that reside in SharePoint. Summarize why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing

Describe the scope of the processing

Describe the context of the processing

Describe the purposes of the processing

Step 3: Consultation process

Consider how to consult with relevant stakeholders - describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm (Remote, possible or probable)	Severity of harm (Minimal, significant or severe)	Overall risk (Low, Medium or High)

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** [eliminated; reduced; accepted]	**Residual risk** [low; medium; high]	**Measure approved** [Yes/No]

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		

Item	Name/position/date	Notes
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Annex IV: SHOW LERs

Advisor Ethical Expert (AEE)		
Entity	**Person**	**Email:**
EC – Expert panel	Suzanna Kraak	Suzanna.KRAAK@ec.europa.eu

Core Ethical Board (CEB)		
Role	**Person**	**Email:**
Coordinator	Henriette Cornet	henriette.cornet@uitp.org
Technical and Innovation manager	Evangelos Bekiaris Maria Gkemou	abek@certh.gr mgemou@certh.gr
WP9 leader	Anna Anund	anna.anund@vti.se

Local Ethical Representatives (LER)[24]				
#	**Country**	**City**	**Person**	**Email:**
1	France	Rouen	Sam Lysons	sam.lysons@transdev.com
2	France	[25]*Rennes*	Isabelle Dussutour Florent Poiret	isabelle.dussutour@id4car.org florent.poiret@chu-rennes.fr
3	Spain	Madrid	Francisco Ramón González-Calero Manzanares	FranciscoRamon.GonzalezCalero@e madrid.es
5	Austria	Graz	Joachim Hillebrand	joachim.hillebrand@v2c2.at

[24] Follower sites LERs will be defined in the next period for Thessaloniki and Brussels, the plans of which will be elaborated.

[25] To be replaced – subject to Amendment.

Local Ethical Representatives (LER)[24]				
#	**Country**	**City**	**Person**	**Email:**
6	Austria	Salzburg	Markus Karnutsch	markus.karnutsch@salzburgresearch
7	Austria	Carinthia[26]	Petra Schoiswohl	petra.schoiswohl@suraaa.at
8	Germany	Karlsruhe	Juergen Weimer	Juergen.Weimer@dlr.de
9	Germany	Monheim[27]	Katharina Karnal	katharina.karnahl@dlr.de
10	Germany	*Aachen*[28]	Helen Winter	Helen.Winter@mail.aachen.de
11	Sweden	Linköping	Anna Anund	anna.anund@vti.se
12	Sweden	Goethenburg[1]	Stig Persson	stig.persson@ericsson.com
13	Finland	Tampere	Pekka Eloranta	pekka.eloranta@sitowise.com
14	Denmark	Copenhagen	Anette Enemark	aen@moviatrafik.dk
15	Italy	Turin	Brunella Caroleo	brunella.caroleo@linksfoundation.co
16	Greece	Trikala	Anna Antonakopoulou	anna.antonakopoulou@iccs.gr
17	The Netherlands	Brainport, Eindhoven	Sven Jansen	sven.jansen@tno.nl
18	Czech Republic	Brno	tomas.haban@cdv.cz	tomas.haban@cdv.cz

[26] As a replacement for Vienna – part of Amendment.

[27] As a replacement for Mannheim – part of Amendment.

[28] To be replaced – subject to Amendment.

[29] Replacing former Kist – part of Amendment.