Autonomous Vehicles to Evolve to a New Urban Experience

DELIVERABLE

D1.4. Initial Privacy protection & Data Management Plan

Co-funded by the Horizon 2020 programme of the European Union

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 769033

Disclaimer

This document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Document Information

Grant Agreement Number	**769033**
Full Title	Autonomous Vehicles to Evolve to a New Urban Experience
Acronym	AVENUE
Deliverable	D1.4. Initial Privacy protection & Data Management Plan
Due Date	31.10.2018
Work Package	WP1
Lead Partner	CERTH
Leading Author	Mary Panou, Evangelos Bekiaris, Ioannis Gragopoulos
Dissemination Level	Public

Document History

Version	**Date**	**Author**	**Description of change**
0.1	21-09-2018	Mary Panou, Evangelos Bekiaris, Ioannis Gragopoulos	V0.1 - 1st draft version
1.0	27-10-2018	Mary Panou, Evangelos Bekiaris, Ioannis Gragopoulos	V1 – Complete version, including partners input on data to be gathered in the project
1.1	31-10-2018	Dimitri Konstantas	Final review

Table of Contents

Executive Summary

The current document constitutes AVENUE first version of Data Management Plan, D1.4: "Initial Privacy protection & Data Management Plan" and is the 1st version of the project's guide as to how the Consortium will manage the data throughout all its phases (collection, storing, sharing, processing etc.), what decisions the Consortium will make regarding making data Findable, Accessible, Interoperable and Re-usable (FAIR) and the mechanisms to enable the data management decisions.

AVENUE aims at providing citizens with door-to-door public transport services to facilitate their mobility through autonomous mini buses. The project aims to include all potential types of users coming from diverse background and travel habits and preferences in order to offer tailor-made solutions that meet their needs.

To provide the above-mentioned solution, the project will collect user-related data. The Consortium must fully comply with any laws and regulations in any relevant jurisdiction relating to privacy or the use or processing of data relating to natural persons. These include:

(a) EU Directives 95/46/EC and 2002/58/EC (as amended by 2009/139/EC) and any legislation implementing or made pursuant to such directives and the Privacy and Electronic Communications (EC Directive) Regulations 2003;

(b) from 25 May 2018, the EU General Data Protection Regulation 2016/679 ("GDPR"); and

(c) any laws or regulations ratifying, implementing, adopting, supplementing or replacing GDPR; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

In specific, following the EC guidelines for the Data Management Plans [1], **Chapter 1** introduces the purpose and intended audience of the current document as well as the interrelations to other project work items.

Chapter 2 presents the nature of the data to be handled in AVENUE, its categorisation, sources, the privacy policy as well as the template to be used for describing the datasets and the objectives of the project that will be met through these data collection and processing.

Chapter 3 describes the data collection and storage processes, data protection, retention policy, access, sharing, ownership as well as any measures to be taken for preventing malevolent abuse of the research findings.

Chapter 4 describes the processes and the mechanisms that will be applied for making the data FAIR.

Chapter 5 refers to the necessary GDPR compliant roles that will be allocated for the smooth operation of the project. It also presents the project's ethical policy, ethics helpdesk and all relevant ethical aspects, which will/is further defined in Deliverables D11.1, D11.2, D11.3 and D11.4.

Finally**, Chapter 6** concludes the document.

The current document is a living document and thus it will be updated during the project lifetime as needed, including more detailed information regarding collected data. The next official updated version will be publicly released as part of D1.5 "Final Privacy protection & Data Management Plan", in Month 48, providing final information about the descriptions of different data sets, the AVENUE repository, final DPIA report (the template form can be found in Annex 1.2, as well as any data embargos and data destruction periods).

1 Introduction

Public transport consists of a key element in the economic development of a region and the quality of life of its citizens. Throughout the years, municipalities and public transport operators aim to improve services through an optimal balance between increased and improved service (more vehicles, more km, comfortable, convenient, reliable, etc.), usage incentives (lower fares, Parking-and-Rail etc.) and costs. At the same time, the most common criticisms of public transport concern the low speed and flexibility compared to private cars, the high transport fees and the reliability and availability of the service.

"**A**utonomous **V**ehicles to **E**volve to a **N**ew **U**rban **E**xperience" (AVENUE) project will especially focus on introducing disruptive public transportation paradigms led by SMEs on the basis of door2door services and the nascent concept of the 'Mobility Cloud' aiming in setting up a new model of public transportation.

1.1 Project objectives

AVENUE aims to deploy and validate autonomous vehicles that are integrated in the existing public transport services for several European cities and to validate the safety of autonomous vehicles being used in complex urban environments. Additionally, the project aims to develop and test new, innovative and disruptive urban public transport services based on the use of autonomous vehicles, so as to raise user awareness and increase user acceptance. At the same time, AVENUE will ensure that the use of autonomous vehicles within the context of urban public transport services is a new experience for the passengers. Recommendations will be made for public transport operators and authorities concerning the development and integration of autonomous vehicles in the urban and sub-urban transport environments to encourage the promotion of the advantages of public transport autonomous vehicles to the public. Finally, AVENUE will evaluate the socio-economic impact and the benefits of the deployment of autonomous vehicles for urban public transport.

1.2 Conceptual architecture

The figure below depicts AVENUE's conceptual architecture, including all different elements and roles needed to provide the personalized point-to-point services:

1. Transport operators and bus manufacturers that will collaborate to improve fleet management, service optimisation and access bus performance analytics;
2. The AVENUE core service platform;
3. Transport infrastructure and the automobile and pedestrian traffic that provide the AVENUE core service platform with itineraries/status and city/traffic information respectively;
4. Autonomous minibus that includes the autonomous vehicle control;
5. Human assistant inside the vehicle that caters to special services addressing users with special needs;
6. The vehicle passengers that request the in-vehicle services;
7. The user interfacing (smartphones, call centre, cell phones) that handles in and out vehicles responses;
8. Out of vehicle users that interact with the AVENUE platform through transport requests and request of information/validation.

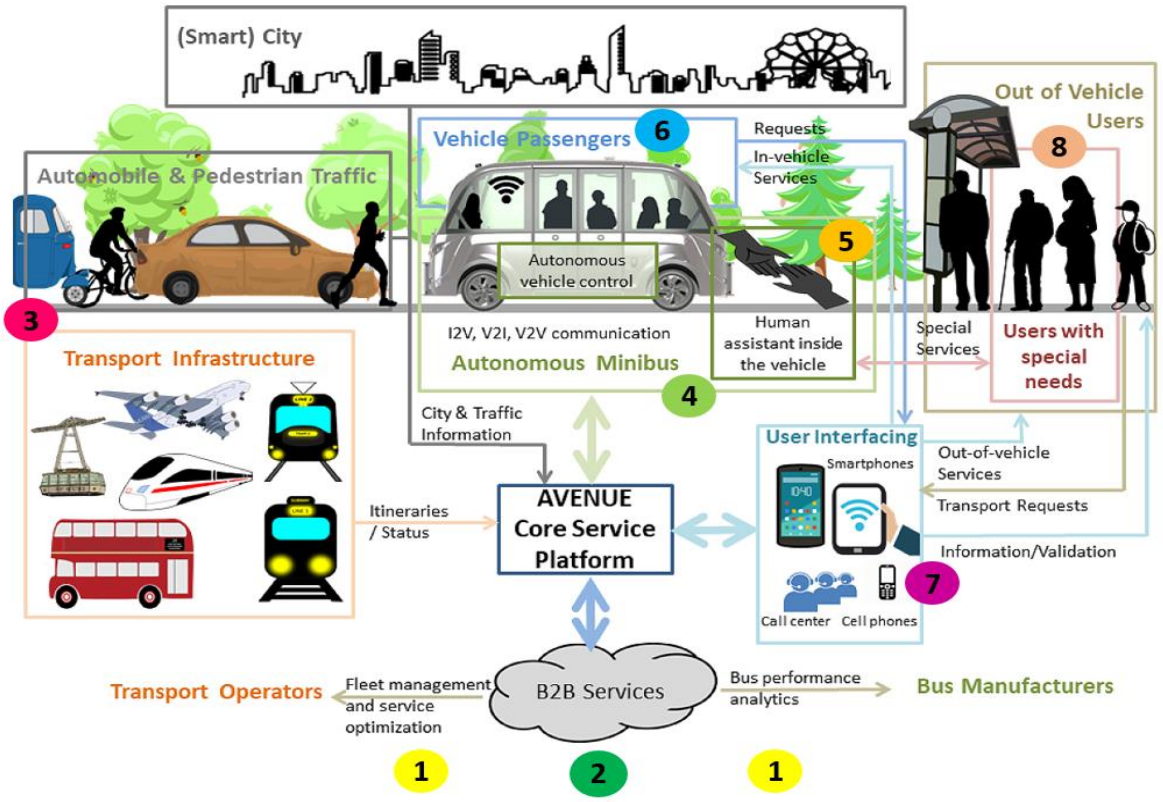


Figure 1. AVENUE conceptual architecture

1.3 Purpose of the document

This document is the first version of the project's Data Management Plan (DMP). The purpose of this document is to provide an overview of the data set types and categories collected during the lifetime of the project and to define the project's data management policy that will be further adopted by the Consortium.

The data management plan defines how data in general and research data will be handled during the research project and will make suggestions for the after-project time. It describes what data will be collected, processed or generated by the AVENUE core service platform and by all the AVENUE ecosystem, what methodologies and standards shall be followed during the collection process, whether and how these data shall be shared and/or made open not only for the evaluation needs but also to comply with the General Data Protection Regulation (GDPR) requirements. In addition, this document will define how they shall be curated and preserved. The AVENUE Data Management Plan will be updated by the evolution of the project.

The overarching project-related GDPR mechanisms are the following:

- **completing** the GDPR compliance template by all project partners that will collect, store and analyse data (template can be found in Annex 1.1);
- **preparing** the Data Protection Impact Assessment in two stages (template can be found in Annex 1.2);
- **determining** and assigning the roles of DPO (Data Protection Officer) at each pilot site;
- **defining** the data protection policy of the project.

This initial version of D1.4, which is submitted in Month 6, identifies a first set of data sources, data categories, datasets, data types and metadata that will be involved in the project and describes the data management process that will be followed in the next steps of the project. This version also

includes how the data owners will contribute to further versions of the deliverable to complete their dataset descriptions.
The Data Management Plan is a living document that will be updated with new information as they arise throughout the duration of the project. The Deliverable will be updated in M48 through deliverable D1.5 and will include the final services offered to users by the AVENUE platform, final data from all partners, finalised decisions on embargo policy as well as finalised decisions and processes for any pending issues that are not specified early on the project.

1.4 Intended audience

The intended audience for AVENUE consists of project partners who are involved in data handling in any manner during the project's lifecycle. These are the project Consortium and the partners that are involved in the pilot tests who collect, store and process information throughout the project, the developers that develop the platform and are expected to ensure data protection, the partners that will publish their work as well as all members that participate in the dissemination process of the project.

1.5 Interrelations

Data Management aspects are closely related to:

a) **Ethics Issues** in AVENUE, especially in the context of collecting, managing and processing (sensitive) personal data from real-life users;
b) **Security aspects**, e.g., data privacy and protection, data ownership, etc.;
c) **Design and development activities** in terms of defining the data that need to be collected or reused to offer tailored services to each specific user group (i.e., older people, people with disabilities, commuters, business travellers, tourists, etc.); and
d) **Legal issues** related to personal data (including sensitive personal data), security and privacy.

Therefore, this document will be updated as the work evolves and in close synergy with the following tasks:

- WP1: T.1.4. IPR & Data Management Plan
- WP2: T.2.2. Passenger needs (including PRM) and requirements specification
- WP2: T2.3 Stakeholders identification, expectations and barriers imposed
- WP5: T5.2 Data and fleet coordination and management
- WP6: T6.3 Security and privacy control
- WP7: Autonomous vehicles for public transport demonstrators
- WP8: Socio-economic and environmental evaluation
- WP11 - Ethics requirements

The work packages interrelations are presented in the figure below (Figure 2).

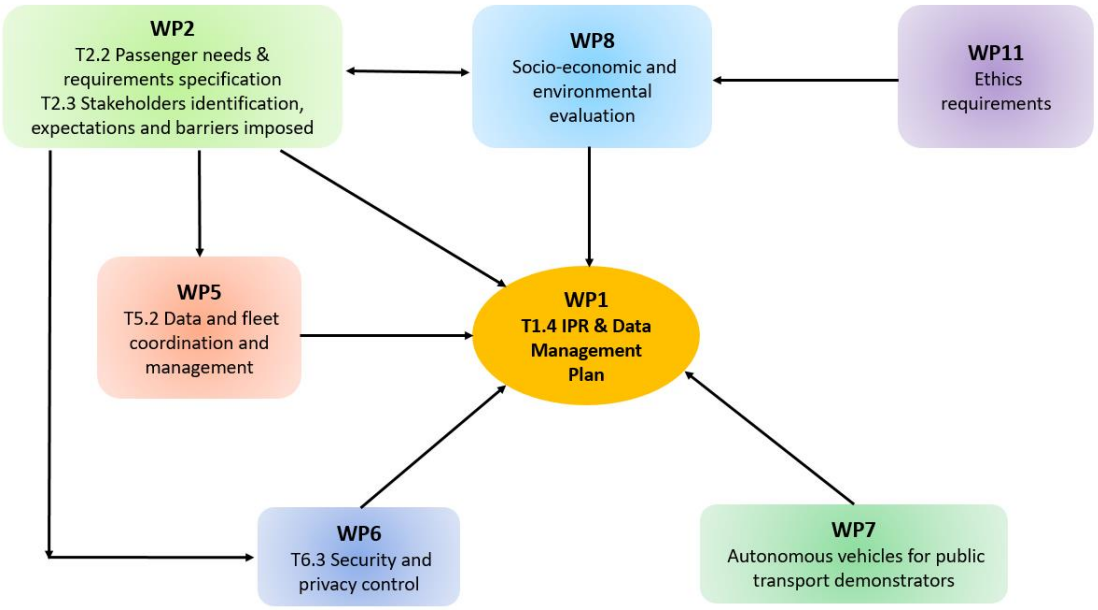


Figure 2 Interrelations of AVENUE's work packages (WPs)

2 AVENUE data

2.1 Data summary

This section provides an explanation of the different types of data sets to be produced or collected in AVENUE project, which have been identified at this stage of the project. As the nature and extent of these data sets can evolve during the project, more detailed descriptions will be provided in the updated versions of the DMP. The descriptions of the different data sets, including their reference, file format, standards, methodologies and metadata and repository to be used are given below.

The aim of this chapter is to:

- provide a first categorization of the data;
- identify a list of the data types that will generated;
- provide a list of metadata that will be used to describe generated data and enable data re-use;
- provide recommendation on data collection and sharing process during the project and beyond

As the nature and extent of these data sets can evolve during the project, more detailed descriptions will be provided in the updated versions of the DMP. The descriptions of the different data sets, including their reference, file format, standards, methodologies and metadata and repository to be used are given below.

2.2 Data presentation

2.2.1 Data identification

The AVENUE project will produce different categories of data sets. Based on the information collected from the above-mentioned template, data is categorised appropriately, as follows:

- **Data types**: this category refers to the type of data in terms of its source and relevance (i.e. vehicle related data, user data etc.);
- **Data sets**: refers to the nature of a complete set of data, that may contain information about different topics (i.e. an excel file containing information about user preferences);
- **Dataset category**: refers to the categories of data based on the level of process (i.e. raw, pre-processed, aggregated, consolidated, metadata, etc.).

In order to identify and define the data types and data management procedures, a template was circulated to the partners to be completed with information and descriptions about the data and metadata that will be collected with their service/tools. The description includes some technical information (such as format, size, privacy level, etc.) but will be further clarified and updated, if necessary, in following versions.

In detail, the template collected information about the following:

- The name of the data
- Whether the data was collected or created
- Data description
- Data category
- Data type

- Data format
- Data size
- Data Ownership
- Privacy level
- Data repository during the project (for private/public access)
- Data sharing
- Back-up frequency
- Status of data at the end of the project (destroyed or not)
- The duration of the data preservation (in years)
- Data repository after the project is complete

The information gathered was analysed so as to identify the types of data and determine how to manage it within the Data Management Plan and as instructed by the GDPR principles.

2.2.2 Data sources

This section describes the data sources and data flows as determined by **Figure 3**, which depicts a generic AVENUE diagram and demonstrates the main data flows in three data flow stages. In AVENUE the following **user groups** are determined as **data sources**: Autonomous Minibus, Data providers, Customers, the AVENUE core services and the Operators. The following figure (Figure 3) depicts the main data sources that will contribute to the AVENUE core services and the main data flows, in three stages that are transferred from one to another.
More specifically, during the first flow stage, initial data comes from the following three user groups:

- **Autonomous Minibus**: This group provides information about the vehicles that participate in the project as well as information related to emergency control needs.
- **Data Providers**: data providers provide information about the public transportation, city conditions, traffic state and any other form of data concerning the urban environment where the pilots are taking place.
- **Users/Customers**: participating users/customers provide information from inside and outside the vehicles about their preferences, needs and wants.

Then, for the second flow stage, the above collected information flows towards the **AVENUE core services** group, so as to cover the following activities:

- Handle passenger requests;
- Provide solutions according to transport policies and provide feedback to help them improve as necessary;
- Build and provide Vehicle-to-Platform interfaces and data transfer protocols;
- Achieve dynamic route planning and fleet optimisation;
- Improve decision making and dispatching of resources and vehicles as necessary;
- Ensure GDPR compliant data management.

Finally, information ends up at the **operators'** end to inform surveyors, administrators and policy makers so that they can proceed with the appropriate decision making and policy making that will bring about the expected results.

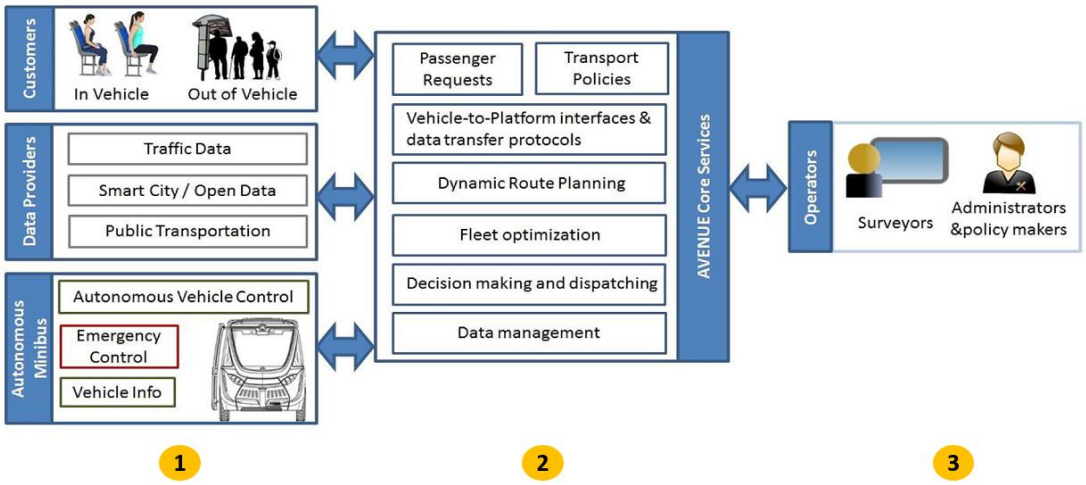


Figure 3. Generic AVENUE diagram and main data flows

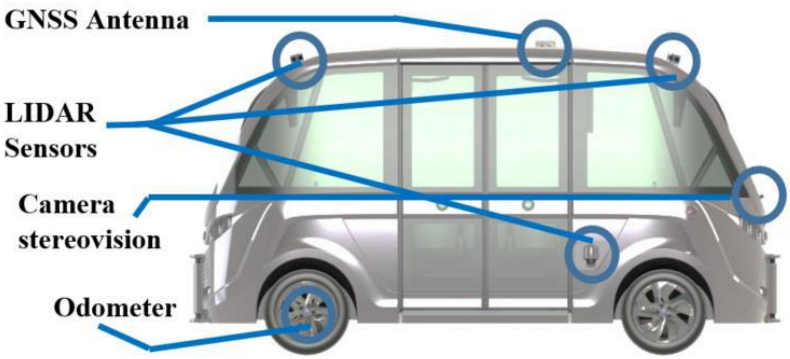
AVENUE project will collect a large amount of raw data to measure and identify the needs of passengers to provide integrated point-to-point services, as well as handle information from vehicles, transport providers and bus manufacturers.

From raw data, a large amount of derived data will be produced to address multiple research needs. Derived data will follow a set of transformation: cleaning, verification, conversion, aggregation, summarization or reduction. In any case, data must be well documented in order to facilitate and foster sharing, to enable validity assessments and to enable its efficient use and re-use. Thus, each data must be described using additional information called **metadata**. The latter must provide information about the data source, the data transformation and the conditions in which the data has been produced.

The following list further summarises and describes **the data types** and **data sources** that will be collected:

Autonomous Minibus: The Autonomous Minibus information is the data collected from the vehicles that take part in the pilots.

Vehicle info	The data that describes the condition and the mobility of the vehicle. Such data can be, for example, longitudinal speed, longitudinal and lateral acceleration etc. The vehicle information is shared between the Autonomous Vehicle Control (AVC) and the closed circuit that is used by the operators for communication and control.



Picture 1 Sensors and equipment to collect data on the AVENUE mini buses

Data providers: The information from data providers refers to traffic data, smart city/open data and public transportation information. More specifically:	
T*raffic data*	Provides information about how travel speeds on specific road segments change over time.
Smart city/open data	Information that is freely available to users
Public transportation	This data consists of information about public transportation services and schedules.
Customers: information from final users, which are out-of-vehicle people, in-vehicle people and operators.	
Out-of-vehicle	Information from/about people waiting for AVENUE services.
In-vehicle	Information from/about people enjoying the AVENUE services (passengers).
Operators	Information from/about professionals who work either as distant surveyors or system administrators.
AVENUE core services: describes information from all previous user groups that is necessary for the smooth and uninterruptible operation of AVENUE services.	
Data management	Describes the way information is exchanged and managed.
Decision making and dispatching	Refers to information necessary for the decision-making process and for the dispatch of an autonomous vehicle towards a customer.
Fleet optimisation	Information that allows for optimum use of fleet.
Dynamic route planning	Data concerning optimum route planning and taking.
Vehicle-to-Platform interfaces and data transfer protocols	Information exchanged between the vehicle and the platform.
Passenger requests	Information regarding the needs and preferences of passengers.
Transport policies	Information concerning the existing policies in the transport sector.

2.2.3 Data collection

Within the project's framework, a socio-economic and environmental impact assessment will be conducted. To this end, several methods will be applied to collect the necessary information. The data that will be collected refer to user experience, accessibility for persons with restricted mobility (PRM), socio-economic and environmental acceptance. The following table (Table 1) summarises the research methods and tools that will be used for the collection of this data.

Table 1 Objectives, methods and tools used in user related data collection

Objective	Method	Tools
User experience	Qualitative	• Longitudinal studies • Accompanied observation • Focus groups
	Quantitative	• Shadowing/observation plus questionnaire
Socio-economic and	Quantitative	• Shadowing/observation plus

environmental acceptance		questionnaire • Large scale survey: zero measurement, intermediate measurement, final control measurement • Big Data analysis (videos recorded in the busses could be analysed)
Accessibility for PRM	Qualitative	• Focus groups • Accompanied observation

Data collection regarding user needs, traffic, preferences, etc. throughout the pilots will be made using paper-and-pencil and online questionnaires. The gross random sample will range from five to eight thousand residents, elected randomly and living in a thirty to fifty-kilometre radius via post code areas. Invitations will be sent by email (if personalised e-mail addresses are available) with the link to the online questionnaire or by post with a paper-and-pencil version of the questionnaire and a return envelope. The net sample will depend on the return flow, although a minimum of 10% is expected. The paper pencil version of the questionnaire will be scanned via *evasys* (https://en.evasys.de/), the online questionnaire will automatically be registered via *Unipark* (https://www.unipark.com/en/) and the statistical analyses will be made via SPSS. Respondents will consent to be contacted via email prior any project-related communication takes place in order to comply with GDPR requirements. The process will be described in the PIA report submitted in the final version of this Deliverable in Month 48. However, the methodology applied will be reported in an intermediate stage by involved partners, when pilot plans are set and before any testing is conducted. As this Deliverable is treated as a living document, when the processes are put in motion and are reported, then they will be added in the Deliverable.
Vehicle operation related data will be collected through sensors, pavement tapes, proximity sensors, seat sensors, surveillance cameras, etc. will be managed in accordance with local policies of the operators.

2.2.4 Data types, datasets and dataset categories

This section presents a short description of the data that will be collected, generated and managed in AVENUE. More specifically, data is clustered into three different sections: **data types**, **datasets** and **datasets categories**. Data types are related to the source of the data, i.e. vehicle data, traffic data, etc., datasets refer to the file extension of the data and, finally, dataset categories refer to the level of process that the data has undergone.

The **types** of data generated, collected and managed within AVENUE fall into the following categories:

- Subjective data (user profile and user request related data)
- Vehicle related data
- Urban environment related data (traffic and city related data)
- Infrastructure related data

As far as **datasets** are concerned, the following will be handled by AVENUE:

- Reports (in the form of word or pdf documents)
- Excel files with raw data, as received by sensors, surveys etc.
- Video signals
- Database

The following table is a template that will be used to describe the datasets.

Table 2 – Dataset Description template

Dataset Reference	AVENUE_WPX_TX.X_XX Each data set will have a reference that will be generated by the combination of the name of the project, the Work Package (WP) and Task (T) in which it is generated and (for example: AVENUE _WP3_T3.4_01)
Dataset Name	Name of the data set
Dataset Description	Each data set will have a full data description explaining the data provenance, origin and usefulness. Reference may be made to existing data that could be reused.
Standards and metadata	The metadata attributes list The used methodologies
File format	All the format that defines data
Data Sharing	Explanation of the sharing policies related to the data set between the next options: **Open**: Open for public disposal **Embargo**: It will become public when the embargo period applied by the publisher is over. In case it is categorized as embargo the end date of the embargo period must be written in DD/MM/YYYY format. **Restricted**: Only for project internal use. Each data set must have its distribution license. Provide information about personal data and mention if the data is anonymized or not. Tell if the dataset entails personal data and how this issue is taken into account.
Archiving and Preservation	The preservation guarantee and the data storage during and after the project (for example: databases, institutional repositories, public repositories …)

The AVENUE project will produce different dataset categories. More specifically:

- **Context data**: data that describes the context of a pilot.
- **Acquired and derived data**: data that contains all the collected information related to a pilot.
- **Subjective data**: questionnaires, surveys, personal and group interviews.
- **Raw/unprocessed data**: data collected directly from the source (either objective or subjective).
- **Metadata**: descriptions of data that will facilitate the data analysis and data pre-processing.
- **Aggregated data**: data summary obtained by reduction of acquired data and generally used for data analysis.
- **Consolidated data**: data collected across sites and per data type.

2.2.5 Subjective data types

This type of data is collected during all types of qualitative surveys, questionnaires, personal and group interviews (WP2) that take place in the project. This data is **collected**, **managed** and **processed** by AVENUE partners. The data may be collected from users/customers, data providers and operators as well as other types of stakeholders. In all cases, the data is/will be anonymised to ensure privacy

and protection of the participants' identity. In the case of the users/customers, subjective data will mostly deal with travel preferences and needs.

2.2.6 Data privacy policy

Participants' personal data will be used in strictly confidential terms and will be published only as statistics (anonymously). In addition to the ethical aspects analysed, the following safety provision will be considered during the project:
Only one person per site (relevant Ethical issues responsible) will have access to the relation between test participants' code and identity, in order to administer the tests. This means that data will be pseudonymised, making the compliance with GDPR essential. The GDPR compliance form will be filled in by all project partners throughout the duration of the project. The GDPR compliance form is found in Annex 1.1. Further to that, all partners will fill the Data Protection Impact Assessment form (Annex 1.2), again throughout the duration of the project. The filled in forms will be presented in D1.5 (due for Month 48). One month after the pilots end, this reference will be deleted, thus safeguarding full anonymisation of results. The data will be gathered at each pilot site with consideration for the following aspects and compliance to GDPR:

- **Confidentiality and data protection**: Participants, and the data retrieved from them (performance or subjective responses) must be kept anonymous unless they give their full consent to do otherwise.
    - Identifiable personal information should be encrypted (i.e. pseudonymisation and coding). Otherwise ethical approval is necessary specifically for this;
    - 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).
    - Each individual entrusted with personal information is personally responsible for their decisions about disclosing it;
    - Pilot site managers must take personal responsibility for ensuring that training procedures, supervision, and data security arrangements are sufficient to prevent unauthorised breaches of confidentiality.

- **Encrypted and pseudonymised data**: To mitigate the risks involved with processing data subject information, any data collected will be encrypted or pseudonymised to the extent reasonably possible, so that individuals cannot be identified, as recommended by Article 32 of the GDPR. Pseudonymised data is data that 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 [2].

Any data that will be stored will not consist of personal information that can lead to the person giving the information. Nevertheless, stored date relate only to users' preferences in daily activities or health problems, not to a person's beliefs or political or sexual preferences.

The following data will **not** be stored:

- Medical info.
- Name, address, telephone, fax, e-mail, photo, etc. of the user (any direct or indirect link to user ID).
- User location (retrieved every time dynamically by the system, but not stored).
- Any other preferences/actions by the users, except the ones motioned explicitly above.

- Destination of the users (will be used to provide the service but will not be stored).

In addition, aggregated data and conclusions related to impact estimations will be shared with researchers outside the Consortium upon agreement to do so, as the project participate in the Open Research Pilot. This will be decided and finalised in the updated version of the Data Management Plan in D1.5.
For statistical analysis, the decisions made by the participants may be associated with their type, their travelling preferences, age, gender, nationality, familiarity and use of services and transport modes, etc. This will be decided and finalised in the updated version of the Data Management Plan in D1.5.

AVENUE core services platform aims to provide users with high quality door to door services. However, it will perform this taking into consideration the following:

- All required user profile data will be stored at his/her mobile device and be securely protected (by password or highly advanced security mechanisms; this depends upon how much the user is willing to invest on it).
- Relevant preferences relate to his/her mobility, favourite locations, frequent routes will be stored in their mobile device and be securely protected (by password or highly advanced security mechanisms; this depends upon how much the user is willing to invest on it).
- The user's location, route and destination will be only temporarily stored (i.e. during a trip), in order to assist the user and will be automatically deleted afterwards. Any location information will be stored on the user's mobile device, discharging the consortium from any responsibility of handling sensitive data.
- The user will have the capacity to view, change or delete, as he/she wishes, all stored data by the system (including his/her profile data), with the help of a very simple and multimodal interaction (touch, buttons and voice input supported).
- All AVENUE applications are using unobtrusive sensors, i.e. embedded on a seat or wearable, avoiding the use of cameras and other visual detection sensors that may be misused by an intruder.

The above data privacy policy applies also on any communication dissemination activities held within the project to promote its results and communicate new knowledge.

2.3 GDPR compliant system architecture

The following figure depicts the detailed architecture of the AVENUE system. At the bottom of the detailed AVENUE architecture lies the Multisensor Data Collection System (MDCS). This is the sensing layer that consists of several sensors, whose purpose is to detect changes and events in their environment (either the autonomous mini bus, the interior or the exterior). This layer consists of three groups of sensors. As depicted in the graph (Figure 4), the sensors can be road pavement tapes, proximity sensors, privilege passenger presence, seat sensors, surveillance cameras, route cameras, geographic positioning systems (GPS), global system for mobile (GSM), Light Detection And Ranging (LIDAR) or accelerometers.

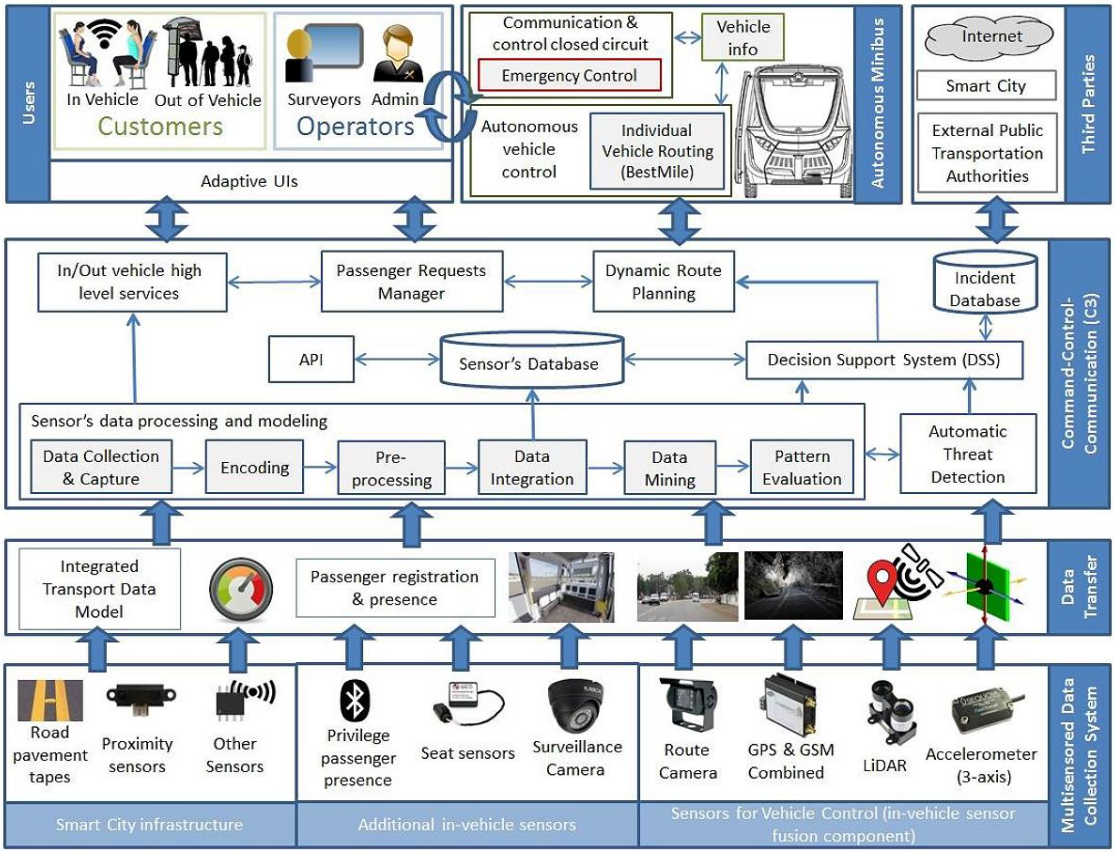


Figure 4 Detailed System Architecture

The information collected by the sensors is sent to other complex electronics through the **Data Transfer** layer, entailing all processes for the transfer of information from the collection devices and equipment towards the command-control-communication level. The **Command-Control-Communication (C3)** is the main services layer for the AVENUE project. Within this layer, software components will receive information from the sensors' layer, process it and allocate it to the respective sub-components to support activities such as decision making, route planning, management of passenger requests, incident management. At the same time, there will be an Automatic Threat Detection component to further raise passengers' acceptance, evaluating the behaviour of passengers. A sensor's data processing and modeling component will do all the processing and update the Sensor's Database. A Decision Support System (DSS) will assist with the decision-making activities and will help administrators and surveyors to make decisions about possible issues.

Within the C3 level, the data collected and captured undergoes encoding before being pre-processed. The data that is encoded includes data from infrastructure sensors, data regarding passengers' registration and presence as well as user location. Data encoding implies that it cannot be retrieved from the database by unauthorized users, complying with GDPR regulations about data security.

2.4 Data documentation

Data documentation will mostly be metadata and will be used in order to recognize each data type and source. The initial documentation details that will be included for each service are shown below.

2.5 File naming

File naming depends largely on service and the datasets to be derived by this service and/or connected with this service. They have to be **consistent** and **descriptive**.
The creation of the unified database will be based on a common file naming and organizing among partners in order to help partners organize effectively and efficiently their work and, of course, ease collaboration with other partners. Additionally, partners using this file naming system will find it easier to work (and share) the correct version of data and accompanying metadata files. The following file naming offers a consistent naming of the files in order to make it easier to identify, locate and retrieve the data files.

This file and folding naming system will be used for all data and metadata files.

1. **Project acronym:** AVENUE
2. **Service related:** Service acronym (initials based on the name given in DoA)
3. **Location (where it resides):** e.g. DFA_DB (Daily Functions Assistance Database)
4. **Researcher name/initials:** Ian Smith (i.e. IS; alternatively, could use database user credentials)
5. **Pilot identifier:** e.g. GP for Geneva Pilot site
6. **Date or range of pilot:** 011216
7. **Type of data:** CE for calendar entries
8. **Conditions:** condition_user group (e.g. baseline_PT)
9. **Version number of file:** Only singular number are acceptable (1, 2, 3)
10. Three letter file extension for application specific files (e.g. csv)

Any spatial characters are avoided because they might not work well with certain programmes and avoid spaces (i.e. use underscores instead). Each data folder will include a regularly updated README.txt in the directory to explain the codes, abbreviations used and, in general, the coding practices and naming conventions used. Based on the example used above, an efficient naming convention within the AVENUE project looks like that:

AVENUE_DFA_ DB_IS_GP_011216_CE_baseline_PT_v1.csv

3 Data Collection and Storage Methodology

As previously stated, data will be stored in secure server systems. Only the PC and selected personnel from demonstrators will possess the key to re-identification, making the data pseudonymised. No data related to personal information of the involved participants will be collected and stored. Instead, all participants will be granted with an identification number based on each participant's role in each of the city (role ID), allowing mapping of participants' actions during the execution and pilot realisation phase. The relationship between the role ID and the participant will be recorded at the repository and will be stored separately and securely. This file will be accessible only to the corresponding site manager. The key to link the participant's name to the code which identifies the data file will not be provided to anyone and the privacy of the data will be protected. Furthermore, data will be kept for the least a period of time necessary to accomplish the goals of the project and the population of the AVENUE Repository. This period of time will be defined when the pilot data collection process will be established and after Consortium consensus.
In any case, all data that will be considered confidential from the pilots will be discarded by the project completion, whereas only the public models and respective datasets that will be described in detail in the Data Management Plan will be kept open. Partners will define the data embargo period (if any) and those who are data owners will decide which datasets (or parts of) will be openly shared. Such decisions will be made after AVENUE datasets have been collected.

3.1 Data protection

In order to protect the collected data and control unauthorised access to the AVENUE data repositories, only authenticated personnel will have access to pilot-specific data collected. During the proposed system lifecycle, a holistic security approach will be followed, in order to protect the pillars of information security (confidentiality, integrity availability) from a misuse perspective. The security approach will be identified by a methodical assessment of security risks followed by their impact analysis. This analysis will be performed on the personal information and data processed by the proposed system, their flows and any risk associated to their processing. The details on measures to prevent misuse of data and research findings as well as the performance of security audit and data privacy assessment will be reported in the related Ethics deliverables.
Towards the protection of personal data of volunteer pilot participants, the following issues will be taken into account:

- All data associated with a recognizable person will be held private.
- Individual data on participants will be used in strictly confidential terms and will only be published as statistics (anonymously).
- Any data or information about a person will be held private, regardless of how this data was acquired. Therefore, data obtained incidentally within AVENUE project will be handled with confidentiality. This accidental obtainment does not substitute the compulsory procedure, in which researchers need each participant's explicit consent to obtain, store and use information about them.
- Data collection will be anonymous but data are defined as pseudonymized because their personal details will be securely stored. Only one person will have access to these details and no access to pilot data. Contact details are kept in case we wish to contact participants for participation in another pilot phase. However, as pilot plans are not still in place, we state that data are pseudonymised. If pilot data collection will not entail keeping contact details, then data will be fully anonymized.

- The acquired data will under no circumstances be used for commercial purposes.

During the AVENUE project, responsibilities will be clearly assigned for the overall management and control of research findings and the controlling of access rights. The person who will be responsible on issues for data security will directly inform to the quality board, the ethics helpdesk and the project coordinator.

3.2 Data storage, backup and repository

Data collected by the AVENUE services and the pilots must be securely stored and regularly backed-up. In some cases, multiple copies should be made, especially for large datasets that need to be stored in large capacity external drives. To this end, the data management plan has to ensure the following checklist is ticked:

How will the raw data be stored and backed-up during the research project? How will the processed data be stored and backed-up during the research project? What storage medium will be used for the storage and backup strategy? Is the backup frequency sufficient to ensure data restoration in the event of data loss? Is the data backed up at different locations?

A **Data Repository** will be created for the purposes of storage during the project and potentially for a period of time after the projects is complete. The project's repository will be hosted at the University of Geneva (UniGe). It is physically located in the premises of the university, where there will be regular back-ups and continues intrusion controls with the use of advanced security detection systems. Further to that, the repository will be strongly protected in conformation with current security practices.

Access to the data repository will be given to project participants through an identification number based on each participant's role in each of the city (role ID), that will allow the mapping of participants' actions during the execution and pilot realisation phase. This file will be accessible only to the corresponding site manager. The key to link the participant's name to the code which identifies the data file will not be provided to anyone and the privacy of the data will be protected. The relationship between the role ID and the participant will be recorded at the repository and will be stored separately and securely. Data will be kept for the least period of time necessary to accomplish the goals of the project and the population of the AVENUE Repository. In any case, all data that will be considered confidential from the pilots will be discarded by the project completion, whereas only the public models and respective datasets that will be described in details in the Data Management Plan will be kept open.

However, not all partners have yet decided which strategy to follow and how to proceed with their data storage policy and backup frequency. This will be finalised in the next version of the Data Management Plan D1.5.

It is common practice to store the data for a time period of 2 to 3 years after the project is complete. The data produced in the project as Public Deliverables have, in principle, no expiration data and can be kept for at least ten years in the project's repository. Data that is collected from interviews, vehicle operations, pilots etc. will be handled differently; the anonymised part of data will be retained (and possibly made available to researchers) while vehicle operation data will be handled according to the policies of the operators as the data may be requested for legal purposes by the authorities. This data will not be public and will be erased from the data repository only to remain stored at the operators' systems.

Partners may choose to keep the data for some time, indefinitely or even delete as soon as the project is complete. NAVYA and CEESAR have decided that information that is collected by sensors regarding incidents/accidents, nominal behaviour, reports and incident/accident database will be

stored in a private cloud for a duration of four (4) years and will be destroyed at the end of the project. Other partners will decide about the duration of storage within the following months. This is an issue to be determined as the project continues and will be finalised in the updated version of the Data Management Plan, D1.5 due for M48.

3.3 Data retention and destruction policy

Within the AVENUE Data Management Plan, the open research data retention and destruction strategy will be also reported along with the limits on their secondary use and their disclosure to third parties. A number of critical factors that are relevant for data retention will be taken into account, namely:

i) Purpose of retaining data,
ii) Type of open data collected,
iii) Policy access to the open data,
iv) Data storage, security and protection measures and
v) Confidentiality and anonymity of data.

According to the project's data retention policy, the data stored for the purposes of the project will be deleted after 4 years after the completion of the project. This will take place from authorized partners to ensure data deletion is conducted in a correct and legal manner and it is also subject to changes and modifications during the project, if considered necessary.
Regarding **data destruction**, as computerized data (hard disk drives) will be used for data storage, existing methods for permanent and irreversible destruction of the data will be utilized (i.e. full disk overwriting and re-formatting tools). In all cases the data protection and privacy of personal information will be governed by the following principles, which consist of part of an overall information security policy:

- Protective measures against infiltration will be provided;
- Physical protection of core parts of the systems and access control measures will be provided;
- Logging of AVENUE system and appropriate auditing of the peripheral components will be available.

3.4 Data access, sharing and reuse

At each pilot site, a nominated person will be responsible for overseeing that data are safe and secure. Overall, data will be stored in secure server systems and will be anonymised. Only the PC and selected personnel from demonstrators will possess the key to re-identification. No data, related to personal information of the involved participants will be collected and stored.
One person will be allowed to have **access** to full datasets (i.e. higher authorisation level) and the rest of the data team will have medium or lower level of authorisation. Data will be stored in secure areas (physical, network, private cloud-based). Higher level of authorisation is granted only for sensitive and personal data. According to the system architecture, sensitive information received by sensors and users is encoded, making access to the data from unauthorised users impossible. Data to be shared for analysis or transferred to the AVENUE database will not include any personal or identification data.
Data collection, storing, accessing, and sharing abides to the international legislation (Data Protection Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data") and guidelines.

Different levels of authorisation will exist also for remotely accessing data. High level access to data will not be possible outside the work premises, as they are defined at each pilot site.
Use of cloud store data will be available for medium and lower level of access. Not all individuals will have the same access privileges in order to avoid data corruption, loss and damage. Dataset owners will have full access (read, write, update, delete), however, individuals who want to use/reuse the dataset will be able to read and download but not make any changes or modifications to the specific dataset. Of course, all datasets will be password-protected. In some cases, encryption will be necessary.
The main restrictions with regards to confidentiality are the following:

- Name
- GPS coordinates (only metadata or surrogates)
- Raw video and audio recordings

The above data is identified based on the initial data pools set by partners responsible for services/tools. Other data restrictions might arise during the course of the project. If so, they will be finalised in the next version of the deliverable, D1.5.

Concerning **data sharing**, under Horizon 2020, publications resulting by work performed within a project have to be in open-access journals [3]. Participating in an open scholar community can help make the work of partners, and the project, more visible to researchers who work in similar disciplines and research areas. Specifically, for AVENUE, publishing in open-access journals is sought. Relevant dissemination activities target, organize and manage publishing efforts (WP10).
Data re-use by external researchers and other stakeholder groups will be feasible for selected datasets. The embargo period will be at least the duration of the project, as partners would like to easily manage the data whilst collection, analysis and reporting is ongoing. Sharing and-reuse will be applied in the central database according to data depositor's wishes and suggestions.

3.5 Data ownership

Any data gathered during the lifetime of the project are the ownership of the beneficiary or the beneficiaries (joint ownership) that produce them according to **subsection 3, Art. 26 of the signed Grant Agreement (769033**). The beneficiaries have the intellectual property rights of the data they collect and re-use of data is defined by the limitation they might set in how they will make data available. This means partners decide if they make data open-access (no additional restrictions on access to data or publications) or there is an embargo period, whereby permission for accessing the data is given after a certain period of time. As datasets have not been formed yet and services are to be enhanced and connected to the AVENUE app centre, therefore this information will be available in an updated version of this deliverable.

3.6 Measures for preventing malevolent/ criminal/terrorist abuse of research findings

During the AVENUE project, responsibilities will be clearly assigned for the overall management and control of research findings and the controlling of access rights. The person who will be responsible on issues for data security will directly inform to the quality board and the project coordinator. The research findings will be protected from malevolent/criminal/terrorist abuse by following strictly procedures, as they will be defined by the Ethical Advisory Board.

4 FAIR Data

To further promote knowledge transfer and to contribute towards new research content and results, AVENUE participates in the Open Research Data Pilot (ORDP). However, any data that is identified and labelled as "restricted" or under an "embargo" period will be excluded from the ORDP. To accommodate this, the data that will be included in the ORDP should be handled according to the FAIR principles, meaning that the data that will be generated during and after the project will be made **findable**, **accessible**, **interoperable** and **reusable**.
The FAIR principles are applied in AVENUE due to the fact that they serve as a template for lifecycle data management and they ensure that the most critical components are covered. Further to that, H2020 endorses the FAIR principles and encourages their implementation amongst its projects regardless of scientific and research disciplines.

To make data **findable**, including provisions for metadata the following need to be taken into consideration:

- The datasets will have very rich metadata to facilitate the findability.
- All the datasets will have a Digital Object Identifier provided by the AVENUE public repository.
- The reference used for the dataset will follow this format: AVENUE_WPX_AX.X_XX, including clear indication of the related WP, activity and version of the dataset.
- The standards for metadata will be defined in the "Standards and metadata" section of the dataset description table (see Table 3 for the current version of the template).

To make data **accessible:**

- Datasets openly available are marked as "Open" in the "Data Sharing" section of the dataset description table (see Table 3, Annex 2).
- The repository that each dataset is stored, including Open access datasets, are mentioned in the "Archiving and Preservation" section of the dataset description table (Table 3, Annex 2). The repository that will be used is still under consideration.
- "Data sharing" section of the dataset description table (Table 3, Annex 2) will also include information with respect to the methods or software used to access the data of each dataset.
- Data and their associated metadata will be deposed either in a public repository or in an institutional repository.
- "Data sharing" section of the dataset description table (Table 3, Annex 2) will outline the rules to access the data if restrictions exist.

To make data **interoperable:**

- Metadata vocabularies, standards and methodologies will depend on the repository to be hosted (incl. public, institutional, etc.) and will be provided in the "Standards and metadata" section of the dataset description table (Table 3, Annex 2).

To make data **re-usable** (through clarifying licenses):

- All the data producers will license their data to allow the widest reuse possible. More details about license types and rules will be provided in the next version of the deliverable.
- "Data Sharing" section of the dataset description table (Table 3, Annex 2) is the field where the data sharing policy of each dataset is defined. By default, the data will be made available for reuse.
- The data producers will make their data available for third-parties within public repositories only for scientific publications validation purposes.

5 AVENUE Ethical Policy

AVENUE project involves data collection from users in the context of demonstration activities. All national legal and ethical requirements of the Member States where the research is performed will be fulfilled. Any data collection involving humans will be strictly held confidential at any time of the research. This means in detail that:

- all test participants will be informed and given the opportunity to provide their consent to any monitoring and data acquisition process; the subjects will be volunteers and all test volunteers will receive detailed oral information.
- no personal or sensitive data will be centrally stored. In addition, data will be scrambled where possible and abstracted in a way that will not affect the final project outcome.

Furthermore, participants will receive in their own language:

- a commonly understandable written description of the project and its goals;
- the planned project progress and the related testing and evaluation procedures;
- advice on unrestricted disclaimer rights on their agreement.

5.1 AVENUE Ethics Helpdesk

To properly address all ethics issues that have come up and/or will come up during the project, an Ethics Helpdesk will be set up. The **Ethics Helpdesk** will oversee the research in order to guarantee that no undue risk for the user, neither technically nor related to the breach of privacy, is possible. This allows the Consortium to implement the research project in full respect of the legal and ethical national requirements and code of practice. Whenever authorizations have to be obtained from national bodies, those authorizations will be treated as documents relevant to the project. Copies of all relevant authorizations will be submitted to the Commission prior to commencement of the relevant part of the research project.

The procedures and the criteria that will be used to identify/recruit research participants will be kept on file and submitted upon request. As far as the informed consent procedures implemented are concerned, they will also be kept on file and submitted upon request (see paragraph 5.4 below).

All used assessment tools and protocols within AVENUE demonstrators will be verified beforehand by its Ethics helpdesk regarding their impact to business actors and end users prior to their application at the sites. The helpdesk takes responsibility for implementing and managing the ethical and legal issues of all procedures in the project, ensuring that each of the partners provides the necessary participation in AVENUE and its code of conduct towards the participants. Each city will have its own Ethics Committee and one person will be nominated per site as responsible for following the project's recommendations and the National and European legislations.

5.2 EU General Data Protection Regulation (GDPR) compliance

The EU General Data Protection Regulation (GDPR), entered into force on 24/05/2016 and its provisions will be applicable in all EU member states on May 25th, 2018. The AVENUE project will be developed in full awareness of the GDPR requirements.

According to the Information Commissioner's Office (ICO), there are seven key principles set by GDPR [4]:

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

The above principles consist of the core of the methodology, according to which all necessary steps are taken to become GDPR compliant. AVENUE, as a European funded project with a Consortium of industry and research members, needs to demonstrate compliance by maintain a record of all data processing activities. The personal data that will be collected during the research should be kept secure through appropriate technical and organisational measures. The types of privacy data that GDPR protects are:

- Basic identity information such as name, address and ID numbers;
- Web data such as location, IP address, cookie data and RFID tags;
- Health and genetic data;
- Biometric data;
- Racial or ethnic data;
- Political opinions;
- Sexual orientation.

The above are considered **personal data**.

According to the European Commission (EC) [5], when collecting participants' data, people must be clearly informed about the following minimum:

- What is project AVENUE;
- Who the Consortium consists of;
- Why the project will be using their data;
- The categories of the concerned;
- The legal justification for processing their data;
- How long will the data be stored for;
- Who else might have access to the data;
- Whether the data will be transferred outside the EU;
- Participants have a right to have a copy of the data, the right to file a complaint with the Data Protection Authority (DPA) and the right to withdraw their consent.

For all the above, information will be provided in a written format, in a transparent, concise, accessible and clear manner, free of charge.

5.3 GDPR roles

In order to face the data management challenges in an efficient manner, all AVENUE partners have to respect the policies set out in this DMP. Within the framework of GDPR, the roles that are identified for AVENUE are those of the:

- Data Protection Officer (DPO),
- Data controller,
- Data processor and
- Data producer

Each partner will allocate the persons responsible for each role. The role allocation will be finalised in the next version of this deliverable, D1.5 due for M48. Further to that, the Data controller and Data Processor will fill in the GDPR Data Processing record template for the DPO to validate it. The Data Controller's record template and the Data Processor's record template are found in Annex 3.

5.4 Ethical and legal issues related to data sharing

AVENUE proposed solutions does not **expose**, **use** or **analyse** personal sensitive data for any **purpose**. In this respect, no ethical issues related to **personal sensitive data** are raised by the technologies to be employed in large scale demonstrators foreseen in Switzerland, France, Denmark and Luxembourg. However, AVENUE Consortium is fully aware of the privacy-related implications of the proposed solutions and respects the ethical rules and standards of H2020, and those reflected in the Charter of Fundamental Rights of the European Union. Generally speaking, ethical, social and data protection considerations are crucial and will be given all due attention.
All relevant principles and the main procedures regarding privacy, data protection, security, legal issues and ethical challenges are defined in the Project's Ethics Manual and will be updated in their upcoming versions. Further to that, the general principles for handling knowledge and IPR within AVENUE will be settled in a Consortium agreement (CA), signed by the AVENUE Consortium at the project start. These principles are in line with H2020 IPR recommendations.
The described procedures have been drafted and will be updated in consultation with the project's Ethics Management Panel (composed of one external member, the Coordinator, the Technical & Innovation Manager and the Quality Manager) that will act as supervisors of the ethical activities of the project and the local ethics committees at each pilot site, in order to take into account both European and national ethical and legal requirements.

5.5 Informed Consent

AVENUE scenarios will target participants with competence to understand the informed consent information. Pilot sites, i.e., AVENUE partners participating in the pilots, will receive only anonymised and coded or pseudonymised information. Any recorded data will be available to pilot sites only in anonymised format.
The consent procedures will be carefully determined and managed in WP11 and used in WP7 that will manage the demonstration activities which will be performed in the selected cities. The informed consent form, which each participant will be asked to complete prior to their participation in the pilots, aims at ensuring that the user accepts participation and is informed about all relevant aspects of the research project; it will be collected in written form after the users have been provided with clear and understandable information about their role (including rights and duties), the objectives of the research, the methodology used, the duration of the research, the possibility to withdraw at any time, confidentiality and safety issues, risks and benefits. The templates of the informed consent/assent forms and information sheets will be included in the deliverables D2.10-D2.12.
The basic elements of the AVENUE informed consent include:

1. The objectives of the study, its duration and procedure
2. The purpose of the pilots
3. Description of the type of information to be collected
4. Privacy and data protection procedures
5. Appointed data collectors and processors
6. Data ownership, storage location and storage duration
7. The possibility to decline the offer and to withdraw at any point of the process (and without consequences)
8. Contact person

Further details on the informed consent can be found in the Description of Action, Part B.

6 Conclusions

This deliverable provides an overview of the data that AVENUE project will collect, manage, handle and produce along with related data processes and requirements that need to be taken into consideration. The document outlines an overview of the data types, sources, categories and collection methods and describes the processes that will be followed within the core of the AVENUE project regarding their processes.

The Data Management Plan is a living document and will be enriched along the project's lifetime as new information and decisions arise. The next version will include all final decisions regarding data storage, data ownership, data access, data sharing and repository issues.

To prepare for the next version that is due in Month 48 of the project, the partner handling the data management plan will circulate the necessary guidelines to the Consortium as the project progresses, so as to receive updated, valid and precise information before finalising the next deliverable.

7 References

1. European Commission, Directorate-General for Research & Innovation, "Guidelines on FAIR Data Management in Horizon 2020", available at http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hioa-data-mgt_en.pdf [last accessed: Nov. 29th, 2017]
2. Article 4(5) of the General Data Protection Regulation (EU) 2016/679
3. Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020 (*http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf*)
4. Information Commissioner's Office (ICO): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/
5. European Commission (EC) guidelines: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

Annex 1: GDPR compliance Questionnaire & Tentative DPIA form

Annex 1.1. GDPR compliance Questionnaire

The following questionnaire and the introductory text will be sent to partners to complete until M25.
This compliance questionnaire is designed to help you ask the right questions as you think about how your organisation uses personal data and whether you comply with GDPR.
The checklist of things to consider within each section should be seen as suggestions of measures and processes that might be relevant for your organisation to consider, rather than as an exhaustive list; the more broadly you can think about each question, the more helpful this questionnaire will be.

No.	Question	Checklist of things to consider	How is compliance demonstrated?
1. Data Protection Officer (DPO)			
1.1		The organisation has carried out an assessment to determine whether the triggers for appointing a DPO have been met i.e. either: ❑ (i) the organisation is a public authority; ❑ (ii) the organisation's core activities consist of processing special categories of personal data or information about criminal convictions and offences on a large scale; ❑ (iii) the organisation monitors personal information systematically or regularly as part of its core activities on a large scale. [See separate guidance note on whether a DPO needs to be appointed]	
1.2	Has a DPO been appointed?	❑ If no DPO has been appointed, reasons why have been recorded. ❑ If no DPO is appointed, GDPR working group has been implemented. ❑ Job descriptions of those members of staff who have additional responsibilities for GDPR compliance have been updated. ❑ Process established so that the organisation can continue to monitor and review its approach to personal data processing going forward, particularly where there is a change in systems and processes	
2. Processing Data			
2.1	What uses does the	❑ Data mapping process carried out to	

No.	Question	Checklist of things to consider	How is compliance demonstrated?
	organisation make of personal data?	understand and record the personal data flows and uses to, within and from the organisation. ❑ Data mapping template/ record of processing activities documented ❑ Record of processing activities documents what parts of the organisation process or hold special categories of personal data (i.e. data relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union activities, physical or mental health, genetic or biometric details, sexual life or details of criminal offences.) ❑ Additional security measures for special categories of personal data have been implemented ❑ Procedures implemented to ensure personal data is accurate and up to date ❑ Organisation has determined how it is going to treat historic personal data it holds	
2.2	Does the organisation systematically monitor publicly accessible data on a large scale?	❑ If yes, video usage notice and associated privacy notice for the public have been prepared	
2.3	Is personal data processed or accessed outside the EU/EEA?	❑ Is personal data processed or accessed outside the EU/EEA? ❑ Necessary protections have binding corporate rules, privacy shield, adequacy decision or appropriate safeguards including data processor contracts	
3. Policies			
3.1	What policies does the organisation have in place in relation to data protection compliance and have these been updated to take account of GDPR?	The organisation has the following policies in place: ❑ Data Protection Policy (to inform employees what they can and cannot do with personal data and cover GDPR compliance (including right to be forgotten, access requests, objections to processing, consent withdrawals, verbal exercise of rights) ❑ IT Policy ❑ Data Breach Policy ❑ Security Policy ❑ Data Retention Policy	
3.2	What privacy notices are used	❑ External Facing policy.	

No.	Question	Checklist of things to consider	How is compliance demonstrated?
	by the organisation, do they satisfy the new requirement of transparency in processing and where are they featured?	(NB. This is not a compliance requirement. However, often the privacy policy will be linked to specific external Privacy Notices which are required to be provided so that further copies can easily be obtained by data subjects if required.) ❑ Privacy Notice – For employees, workers, consultants and directors ❑ Privacy Notice – For Volunteers ❑ Privacy Notice – For Members ❑ Privacy Notice – For contractors who are sole traders/partnerships and detailed corporate CRM systems ❑ Timing and provision mechanism implemented to ensure privacy notices are sent out either at first point of contact if the personal data is collected directly or at first point of contact/within one month where data is collected indirectly	
4. Security and IT			
4.1	Does the organisation have adequate physical and IT security procedures to protect personal data and has it implemented technical and organisational measures to show that it has considered and integrated data compliance measures into its data processing activities?	❑ Physical security review carried out – both for IT systems and physical systems/records ❑ Additional security measures implemented to restrict access to personal data to only those who need access. ❑ Use of pseudonymisation to protect personal data considered where appropriate, i.e. processing personal data in a way which does not allow identification of the individuals without the addition of other data ❑ Additional security for special categories of data/criminal history data implemented ❑ IT systems and their compatibility with GDPR have been reviewed. ❑ Process established so that all decisions regarding security are to be reviewed regularly by GDPR working group and recorded accordingly	
4.2	Are all mobiles phones, laptops and tablets tracked in the asset register, pin or password protected, encrypted and remotely wipeable.	❑ Encryption/remote wipe measures for mobile devices implemented ❑ Asset register updated ❑ Relevant provisions about the use of remote devices and any remote access included within IT policy and staff handbook	

No.	Question	Checklist of things to consider	How is compliance demonstrated?
		❑ Use of removable storage restricted	
4.3	What protections are there against accidental loss, damage or destruction?	❑ Robust and frequent back up and disaster recovery procedures are in place ❑ Backups are retained for a sufficient period of time to protect against progressive corruption of data	
4.4	Does the organisation use a public cloud provider to store or share data?	❑ Security arrangements for cloud or third-party servers have been put in place ❑ Data processing agreement is in place with cloud provider ❑ Where there is a transfer/storage of personal data outside EU/ EEA, necessary protections have been implemented i.e. binding corporate rules, privacy shield, adequacy decision or appropriate safeguards including data processor contracts	
5. Data retention, classification and destruction			
5.1	Does the organisation have documented data retention periods? and are they followed?	❑ Data Retention Policy and matrix implemented ❑ Data retention periods have been captured in all privacy notices	
5.2	Can the organisation between data held as a data controller and data held as a data processor?	❑ Distinction has been captured in the data mapping template/record of processing activities	
5.3	When physical data/records are no longer required, are they securely destroyed?	❑ Security of data destruction – both hard copy and electronic ❑ Security of IT asset destruction ❑ Distinction made between confidential waste and non-confidential waste	
6. Training			
6.1	Do all staff and volunteers receive data protection training as part of their induction and at least once every 12 months?	❑ Implementation of a GDPR training programme (train the trainer) ❑ Future induction GDPR training implemented ❑ Ongoing GDPR refresher training implemented ❑ Senior management and members of the main board have received training on GDPR	
6.2	Do staff processing larger volumes of personal data or special categories health and disability data for participants or details of any criminal	❑ Enhanced GDPR Training has been undertaken by heavy/frequent personal data users	

No.	Question	Checklist of things to consider	How is compliance demonstrated?
	offences) have more detailed training, e.g. HR, Coaching, Performance, Membership, IT?		
6.3	Is non-compliance with the various policies linked to the potential disciplinary action in relation to staff? If so, how is this achieved, e.g. policies form part of staff handbook?	❑ GDPR compliance linked to potential disciplinary measures/staff handbook ❑ Employment contract updated	
7. Data Protection Impact Assessment (DPIA) (short version)			
7.1	Have any higher risk data processing activities been identified?	Assessment process carried out for any processing that is likely to result "in a high risk to the rights and freedoms of natural persons." i.e. the organisation: ❑ Uses systematic and extensive profiling or automated decision-making to make significant decisions about people. ❑ Processes special category data or criminal offence data on a large scale. ❑ Systematically monitors a publicly accessible place on a large scale. [The following nine criteria should be considered, in order to establish whether the organisation's processing operations require a DPIA due to their inherent high risk. A data controller can consider that a processing activity meeting two of the below criteria would require a DPIA to be carried out: ▪ Evaluation or scoring. ▪ Automated decision-making with significant effects. ▪ Systematic processing ▪ Sensitive data or data of a highly personal nature. ▪ Processing on a large scale. ▪ Matching or combining datasets e.g. originating from two or more data processing operations performed for different purposes and/or by different data controllers. ▪ Processing of data concerning vulnerable data subjects. ▪ Use of innovative technological or organisational solutions.	

No.	Question	Checklist of things to consider	How is compliance demonstrated?
		▪ Processing involving preventing data subjects from exercising a right or using a service or contract.] ❑ Where it has been decided not to carry out a DPIA, reasons have been documented. ❑ New DPIA to be carried out if there is a change to the nature, scope, context or purposes of our processing.	
8. Consent			
8.1	Is consent required for any processing?	❑ Explicit consents obtained for all testing related tasks ❑ Privacy notices updated to ensure consents are obtained where needed in respect of special categories of data ❑ Processes in place to deal with and action all requests for consent to direct marketing communications to be withdrawn	
8.2	If no consent is not required or obtained, which grounds for processing will be relied on? Consider: - for the performance of a contract to comply with legal obligations - to protect vital interest of the individual pursuing legitimate business interests If any of these apply, please provide an explanation of the position.	❑ Data categorisation recorded in data mapping/ record of processing activities ❑ Future planned data processing activities added to record of processing activities	
9. Sharing/Receiving data from third parties			
9.1	Does the organisation appoint any third parties as data processors?	❑ List of third party data processors added to record of processing activities ❑ GDPR supplier audit carried out ❑ GDPR compliant data processing agreement in place with suppliers/contractors where commercially feasible	
9.2	Does the organisation act as a data processor for any third parties?	❑ Arrangements put in place where acting as a data processor for third parties	
9.3	Does the organisation	❑ Organisation has determined how	

No.	Question	Checklist of things to consider	How is compliance demonstrated?
	share or receive personal data with any other third parties where neither party is processing data on the other's behalf?	personal data is processed with another data controller i.e. as joint data controller ❑ Terms with data controllers considered. ❑ Where personal data has been obtained indirectly from other sources, privacy notices include provisions confirming source of data. ❑ Any framework contracts have been updated to incorporate new GDPR provisions	
10. Rights of Individuals			
10.1	Is there a Subject Access Request Policy? If not, does the organisation have a clear and known process to deal with Subject Access Requests (SARS)?	❑ Subject access right procedure developed/tested ❑ Separate procedures manual for data subject rights considered. ❑ Data protection policy updated to reference subject access requests.	
10.2	What is the process for the organisation to respond to requests: (i) to rectify inaccurate personal data about an individual; (ii) under the right to be forgotten; (iii) to restrict processing; or (iv) for data to be ported?	❑ Subject right procedures developed/tested ❑ Separate procedures manual for data subject rights considered ❑ Data protection policy updated to reference subject access requests	
11. Data Protection Authority (DPA)			
11.1	Have you identified which DPA will oversee your data processing activities?		
12. Children			
12.1	Does the organisation hold or process personal data relating to children between 13 years - 16 years old?	❑ Child-friendly privacy notices prepared and provided. ❑ Process implemented to obtain consents from parents or guardians of children if needed.	
13. Compliance programme			
13.1	Does the organisation have regular GDPR compliance audits?	❑ GDPR compliance internal auditing function and frequency considered	
13.2	If so who is responsible for carrying out the audits?	i.e. DPO or GDPR working group has been formed.	
13.3	What are the organisation's processes for ensuring that policies are reviewed and	❑ GDPR compliance internal auditing function and frequency considered	

No.	Question	Checklist of things to consider	How is compliance demonstrated?
	updated on a regular basis?		
13.4	Are all records of the organisation collated or easily accessible to demonstrate the steps taken to ensure compliance with GDPR?	❑ GDPR accountability record/evidence holding system established	

Annex 1.2. Tentative DPIA form

What is a PIA?

A PIA will be required under Article 35 of the General Data Protection Regulation (EU) 2016/679. A PIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions.

Why should I do a PIA?	**When should I start a PIA?**
• To identify privacy risks to individuals. • To identify privacy and data protection compliance liabilities for your organisation. • To protect your reputation. • To instil public trust and confidence in your project/product. • To avoid expensive, inadequate "bolt-on" solutions. • To inform your communications strategy.	PIAs are most effective when they are started at an early stage of a project, when: • the project is being designed; • you know what you want to do and how you're going to do it; • you know who else is involved. But ideally it should be started before: • decisions are set in stone; • you have procured systems; and • you have signed contracts/ MOUs/ agreements.

Do I have to do a PIA?

Determining if you need to do a PIA - screening questions

*Answering yes to **any** of these questions indicates that a PIA is necessary.*

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

Carrying out a PIA

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. You can adapt the process and this template to produce something which allows your organisation to conduct effective PIAs integrated with your project management processes.

1. Identify the need for a PIA

2.1. Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

2.2. You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

2.3. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Please fill this out in light of the questions you answered 'yes' to above and provide further information. *E.g. The project involves [X] sharing personal data with [X]. [X] will also share personal data about [X individuals] with [X] organisation. The overarching purpose is [XYZ]. The benefits of collecting and processing the personal information is [X].* *The relationship between [X] and [X organisation] is [X] and [explain the role each party is playing and their responsibilities e.g. X organisation is delivering an IT system or [X] is providing research services].....etc.*

2. Describe the information flows

2.1. The collection, use and deletion of personal data should be described here (e.g. where you are getting the data from, where it will be stored and where it could be transferred to). You should also say how many individuals are likely to be affected by the project. It may also be useful to refer to a flow diagram or another way of explaining data flows.

2.2.

E.g. Data will be collected from research participants by [X] via [online] forms ↓ *Data will be stored encrypted on departmental drives* ↓ *Pseudonymised dataset will be provided to [Department X] etc.*

3. Consultation requirements

3.1. Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

3.2. Consultation can be used at any stage of the PIA process.

E.g. Discussed storage with Information Security Team.

4. Identify the privacy and related risks

4.1. Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation / corporate risk**
E.g. *1. Risk that the security of the data is compromised.*	*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 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.*
2. 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.*

5. Identify privacy solutions

5.1. Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced or accepted?
Risk '1' above. *Risk '2' above.*	*Encryption measures are used.* *Appropriate retention periods have been agreed.*	

6. Sign off and record the PIA outcomes

6.1. Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	**Approved solution**	**Approved by**
E.g. Risk 1	*Data will be deleted when it is no longer necessary to retain such data.*	*E.g. Data Protection Officer.*

7. Integrate the PIA outcomes back into the project plan

7.1. Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	**Date for completion of actions**	**Responsibility for action**
Data to be deleted.	*Insert date/description of when.*	*E.g. Data Protection Officer.*

Contact point for future privacy concerns
E.g. Data Protection Officer's details.

Next steps

It is recommended that the PIA is signed off at a senior level internally.
There is no strict requirement to file or be able to produce a PIA report but, if privacy concerns arise, it is good practice to be able to do so. We would recommend that the PIA is filed and stored internally.

Any questions?

If you are still unsure about whether you need to carry out a PIA or have any questions about the guidance above your first point of contract should always be your Data Protection Officer:

Name	
Position	Data Protection Officer
Telephone	
E-mail	

Annex 2: Completed Data Management Plan templates

Below, the AVENUE DMP template for data collected across pilot sites is presented. This Table will be continuously updated, and its final version will include additional information about *which* data (or parts of data) will be openly shared, *how* and *in which formats*. In addition, if data owners set an embargo period, this will be set and presented in the final version of this Table, in an additional column.

Table 3. Preliminary DMP templates for AVENUE.

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
Collected	Operator input to SoA	written answers to questions posted		document	doc / pdf		the 4 operators	consortium		restricted				
Collected	Operator input to SoA	Interview conducted		notes	doc		Amobility	consortium		restricted				
Collected	Operator input to Legal and social barriers and obstacles	written answers to questions posted		document	doc /pdf		the 4 operators	consortium		restricted				
Collected	5 user interviews	Interviews conducted		document	excell		Amobility	Siemens					After 3 months the interviews are made anonymously - the interviews are only shared anonymously with Siemens.	
Created	DRAFTs D2.1 First Gap analysis and recommendations on autonomous vehicles for public service	report		document	doc		Amobility	consortium		restricted				
Created	D2.1 First Gap analysis and recommendations	report		document	doc		Amobility	public		public				

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
	on autonomous vehicles for public service													
Collected	collected CAN/sensor data for incidents/accidents	set of collected data for some trips with incidents/accidents including video, continuous time-dependent data: speed, distance to left-right lines, battery level, yaw angle, etc, and event-dependent data such as braking, FCW, system alarms, LDW, obstacle detection including type, distance, relative velocity, etc. Collected data from operators in AVENUE will be useful as well as available data from other studies to anticipate a wider variety of situations.	Raw or preprocessed data	video signals	as handled by NAVYA	as handled by NAVYA	NAVYA	private (NAVYA)	private cloud, private drop box or as decided by NAVYA	Restricted	NA	Yes	4 years	NA

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
Created	Incident/Accident Reports	Reporting of encountered incidents/accidents, analyses, probable causes, mitigation measures, etc.	Internal Reporting / Dissemination material	documents	as handled by NAVYA, e.g. text document or others	as handled by NAVYA	NAVYA	private (NAVYA)	private cloud, private drop box or as decided by NAVYA	Restricted	Rather Update frequency when new incidents occur	Yes	4 years	NA
Created	Incident/Accident Database	raw data related to incidents/accidents, severity, participants involved, etc.	structured data in a database	database access	as handled by NAVYA	as handled by NAVYA	NAVYA	private (NAVYA)	private cloud, private drop box or as decided by NAVYA	Restricted	NA	Yes	4 years	NA
Created	Incident/Accident Reports	Reporting of encountered incidents/accidents, analyses, probable causes, mitigation measures, etc.	Internal Reporting / Dissemination material	documents	as handled by NAVYA, e.g. text document or others	as handled by NAVYA	Operators: AMOBILITY KEOLIS TPG SLA	Private - Operators: AMOBILITY KEOLIS TPG SLA	private cloud, private drop box or as decided by OPERATORS	Restricted	Rather Update frequency when new incidents occur	Yes	4 years	NA
Collected		Passengers numbers transported	Raw Data	Census	File extension		Keolis Lyon			Restricted	Daily	unnecessary	Until the end of the experimentation	
Collected		Vehicle-kilometres driven	Raw Data	Navyalead	File extension		Navya	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected		vehicle-kilometres automatic driven	Raw Data	Navyalead	File extension		Navya	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected		locational losses signal	Raw Data	Navyalead	File		Navya	partner	partner	Restricted	Daily	No	Undefined	Undefined

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
		numbers			extension				storage					
Collected		trajectory's mistakes	Raw Data	Navyalead	File extension		Navya	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	collected CAN/sensor data for nominal behaviour	set of collected data for some regular trips including video, continuous time-dependent data: speed, distance to left-right lines, battery level, yaw angle, etc. and event-dependent data, e.g. braking, FCW, system alarms, LDW, obstacle detection including type, distance, relative velocity, etc. Collected data from operators in AVENUE will be useful as well as available data from other studies to anticipate a wider variety of situations.	Raw or preprocessed data	video signals	as handled by NAVYA	as handled by NAVYA	NAVYA	private (NAVYA)	private cloud, private drop box or as decided by NAVYA	Restricted	NA	Yes	4 years	NA
Created	Incident/Accident	Reporting of		documents	as handled	as	NAVYA	private	private	Restricted	Rather	Yes	4 years	NA

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
	Reports	encountered incidents/accidents, analyses, probable causes, mitigation measures, etc.			by NAVYA, e.g. text document or others	handled by NAVYA		(NAVYA)	cloud, private drop box or as decided by NAVYA		Update frequency when new incidents occur			
Collected	interview data on the use of conventional public transport as well as wishes & expectations for future autonomous buses	Anonymous interviews with volunteers and passengers of public transport. Interviews conducted by AVENUE partners.		documents	as handled by Siemens	as handled by Siemens	each interviewee	data: private; aggregated results: public	offline PC	Restricted	N/A			N/A
Collected	Live information about the autonomous shuttle: - Location - Orientation - Speed - Door status - Battery level - Online (connected) - Managed / unmanaged by Bestmile platform - Field logs through	Source: Navya shuttles	Data displayed in Bestmile's Operator Dashboard	Information about vehicle behaviour	-	-	Transport operators (SLA, TPG, Keolis, AM)	Private to operator	no access for other partners	restricted	Live info is updated every second	live information only - for historic information see next row	-	-

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
	Field Agent App - Video streams (front, back, interior)													
Collected	Historic data: - Vehicle distance - Fleet distance - Average speed - Mode switches (autonomous / manual) - Percentage of manual mode	Source: Navya shuttles	Data displayed in Bestmile's Operator Dashboard	Information about vehicle behaviour			Transport operators (SLA, TPG, Keolis, AM)	Private to operator	no access for other partners	restricted	Daily	not necessarily, depending on request from operators	as long as desired	-
Collected	Survey: zero measurement	Survey: zero measurement - social acceptability	Raw Data	Document/statistical	File extension	?	HS-PF	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	Survey: intermediate measurement	Survey: Intermediate measurement - social acceptability	Raw Data	Document/statistical	File extension	?	HS-PF	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	Survey: control measurement	Survey: end/control sample - social acceptabiltiy	Raw Data	Document/statistical	File extension	?	HS-PF	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	Shadowing - user experience	Shadowing - observation _ user experience	Raw Data	Document/statistical	File extension	?	HS-PF	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected		Vehicle-kilometres driven	Raw Data		File extension		Navya	partner	partner storage	Restricted	Daily	No	Undefined	Undefined

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
Collected		vehicle-kilometres automatic driven	Raw Data		File extension		Navya	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected		locational losses signal numbers	Raw Data		File extension		Navya	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected		trajectory's mistakes	Raw Data		File extension		Navya	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	Survey: zero measurement	Survey: zero measurement - social acceptability	Raw Data	Document/statistical	File extension	?	HS-PF	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	Survey: intermediate measurement	Survey: Intermediate measurement - social acceptability	Raw Data	Document/statistical	File extension	?	HS-PF	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	Survey: control measurement	Survey: end/control sample - social acceptabiltiy	Raw Data	Document/statistical	File extension	?	HS-PF	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	Shadowing - user experience	Shadowing - observation _ user experience	Raw Data	Document/statistical	File extension	?	HS-PF	partner	partner storage	Restricted	Daily	No	Undefined	Undefined
Collected	Geo-Positioning	From Vehicle to Plateform.	Raw Data	API Request	API	Low	NAVYA	Plateform manager Partner	TBD with Plateform manager	Restricted	TBD	No	4 Years	TBD
Collected	Vehicle Status	From Vehicle to Plateform.	Raw Data	API Request	API	Low	NAVYA	Plateform manager Partner	TBD with Plateform manager	Restricted	TBD	No	4 Years	TBD
Collected	Vehicle Mission	Bi-directionel Vehicles <> Plateform.	Raw Data	API Request	API	Low	NAVYA / Platform	Plateform manager	TBD with Plateform	Restricted	TBD	No	4 Years	TBD

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
							Manager	Partner	manager					
Collected	In / Out Vehicle Video	From Vehicles to Plateform.	Raw Data	Video CODEC	API	High	TBD (NAVYA or Operator partner ?)	TBD (NAVYA or Operator partner ?)	Private Navya or Operator Partner	Restricted	TBD	Yes (Streaming)	Streaming	None
Collected	Blackbox	Log information and video data in case of accident (stored inside the vehicle)	Algo + Raw Data	Video CODEC + Sensors Data	Propriatary format	Very High	NAVYA	NAVYA	NAVYA	Restricted	30 minutes FIFO. 12 hours operational guarantee. 3 month In case of Incident	Yes	3 Month (legal requirement)	None
Created	Incident report	Report in case of incident	Document	Document	PDF	low	NAVYA / Operator Partner	Partner	Partner/ Open Cloud	Restricted	TBD	TBD	4 Years	Operator Partner Storage
Created	Owner guide	Technical and User guide of the vehicle, Technical and User Guide of Radio Base	Document	Document	PDF	low	NAVYA / Operator Partner	Partner	Partner/ Open Cloud	Restricted	TBD	TBD	4 Years	Operator Partner Storage
Created	Technical usage recommendation	Storage technical recommendation guide, Charging recommendation guide	Document	Document	PDF	low	NAVYA / Operator Partner	Partner	Partner/ Open Cloud	Restricted	TBD	TBD	4 Years	Operator Partner Storage

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
Created	Training support Guide	Training support Guide for the operator person inside the vehicle	Document	Document	PDF	low	NAVYA / Operator Partner	Partner	Partner/ Open Cloud	Restricted	TBD	TBD	4 Years	Operator Partner Storage
Created	Homologation Material	Any homologation material required by the regulators at country level	Document	Document	PDF	low	NAVYA / Operator Partner	Partner	Partner/ Open Cloud	Restricted	TBD	TBD	4 Years	Operator Partner Storage
Created	Maintenance report	A report after any intervention on the vehicle for preventive or curative maintenance	Document	Document	PDF	low	NAVYA / Operator Partner	Partner	Partner/ Open Cloud	Restricted	TBD	TBD	4 Years	Operator Partner Storage
Collected/ Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/public access)	Data sharing	Back-up frequency	Destroyed at the end of the project?	Duration of preservation (in years)	Repository after the project
Collected	Operator input to SoA	written answers to questions posted		document	doc / pdf		the 4 operators	consortium		restricted				
Collected	Operator input to SoA	Interview conducted		notes	doc		Amobility	consortium		restricted				
Collected	Operator input to Legal and social barriers and obstacles	written answers to questions posted		document	doc /pdf		the 4 operators	consortium		restricted				

Collected/Created	Name	Description	Category	Type	Format	Size	Owner	Privacy level	Repository during the project (for private/ public access)	Data sharing	Back-up frequency	Destroyed at the end of the project	Duration of preservation (in years)	Repository after the project
Collected	5 user interviews	Interviews conducted		document	excell		Amobility	Siemens					After 3 months the interviews are made anonymously - the interviews are only shared anonymously with Siemens.	
Created	DRAFTs D2.1 First Gap analysis and recommendations on autonomous vehicles for public service	report		document	doc		Amobility	consortium		restricted				
Created	D2.1 First Gap analysis and recommendations on autonomous vehicles for public service	report		document	doc		Amobility	public		public				

Annex 3 GDPR Data processing record template for DPO

NOTE: The information requested here is in line with the requirement to maintain data processing records under the GDPR and is specific to personal data. All data controllers must also keep records of data set descriptions according to the initial Data Management Plan D1.4. This information must be verified by the organizational Data Protection Officer.

I. Data controller's record of processing activities

1	**Contact details of Data Controller**
Email	
Company address	
Telephone	
2	**Purpose of processing**
3	**Description of categories of data subjects and of the categories of personal data**
4	**Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations**
5	**Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation**
5	**Where possible, the envisaged time limits for erasure of the different categories of data**
6	**Where possible, a general description of the technical and organisational security measures for**
a	the pseudonymisation and encryption of personal data;
b	the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c	the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d	a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

II. Data processor's record of processing activities

1	**Contact details of Data Controller**	
Email		
Company address		
Telephone		
2	**Categories of processing carried out on behalf of the processor**	
3	**Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation**	
4	**Where possible, a general description of the technical and organisational security measures for**	
a	the pseudonymisation and encryption of personal data;	
b	the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	
c	the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	
d	a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;	

Appendix A: