D5.4: ICT Data Management Plan

Date of document – 6/2020 (M6)

D5.4:

Authors: Miguel Rodríguez (ATOS); Martin Wagner (ATOS); Rebecca Aspin (GFX); Michel Bayings (GFX); Piero Macaluso (LINKS); Luca Mannella (LINKS)

Reviewers: Maurizio Fantino, Xavier Serrier (RSA)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

Technical References

Project Acronym	INCIT-EV
Project Title	Large demonstration of user centric urban and long-range charging solutions to boost an engaging deployment of electric vehicles in Europe
Project Coordinator	Renault SAS xavier.serrier@renault.com
Project Duration	1/2020 – 12/2023

Deliverable No.	D5.4
Dissemination level [1]	PU
Work Package	WP 5 – IT environment for improving the user charging experience
Task	T 5.1 – Data Governance and cybersecurity protection system
Lead beneficiary	28 (ATOS)
Contributing beneficiary(ies)	10 (CIRCE), 15 (LINKS), 19 (FPT INDUSTRIAL), 20 (MRAE), 21 (GREENFLUX), 25 (EVBOX)
Due date of deliverable	30 June 2020
Actual submission date	30 June 2020

[1] PU = Public

PP = Restricted to other programme participants (including the Commission Services)

RE = Restricted to a group specified by the consortium (including the Commission Services)

CO = Confidential, only for members of the consortium (including the Commission Services)

Document history

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

V	Date	Beneficiary partner(s)
1.0	07/04/2020	ATOS – ToC and first contributions
1.1	18/06/2020	ATOS – Integration version
1.2	26/06/2020	ATOS – Integration with comments from RSA
1.3	29/06/2020	Integration from LINKS and GFX
1.4	30/06/2020	Quality validation from RSA

Disclaimer of warranties

This document has been prepared by INCIT-EV project partners as an account of work carried out within the framework of the EC-GA contract no 875683.

Neither Project Coordinator, nor any signatory party of INCIT-EV Project Consortium Agreement, nor any person acting on behalf of any of them:

a. makes any warranty or representation whatsoever, express or implied,
   i. with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or
   ii. that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or
   iii. that this document is suitable to any user’s circumstance; or
b. assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if Project Coordinator or any representative of a signatory party of the INCIT-EV Project Consortium Agreement, has been advised of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

Table of content

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

0 EXECUTIVE SUMMARY

This document is the first version of a report including the ICT Data management plan for the data generated during the project. It is elaborated in the context of Task 5.5 “Data Governance and cybersecurity protection system” which controls the data value chain to assure its proper management according to the project needs and regulatory framework.

The Data Management Plan (DMP) has been developed in order to establish the measures for exploiting and promoting the findings during the project’s life, it will enhance and ensure relevant project´s information transferability and will take into account the restrictions established by the consortium agreement, as well as the privacy and data protection issues. In this sense, the Plan will set the basis both for the Dissemination Plan and Exploitation Plan.

The DMP describes the data management life cycle for the data to be managed in the project as well as the opinions and attitudes of people, via questionnaires, to be administered via INCIT-EV services or via wide online surveys. The objective is making research data findable, accessible, interoperable, and re-usable (FAIR).

The delivery of this Data Management Plan is done in accordance to the description in the Grant Agreement Annex 1 Part A with no time deviation and no content deviation from the original planning.

0.1 Acronym table

Table 1 - Acronym table

Acronym	Definition
DMP	Data Management Plan
FAIR	Findable, accessible, interoperable, and re-usable
ICT	Information and Communication Technology
API	Application Program Interface
GPDR	General Data Protection Regulation
DPIA	Data Protection Impact Assessment
ICS	INCIT-EV Cybersecurity Services
DSO	Distribution System Operator
CPO	Charging Point Operator

GSR	Galvanic Skin Response
EEG	Electroencephalogram

0.2 Index of Tables

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

1 INTRODUCTION

This document is the first version of the Data Management Plan of INCIT-EV project, namely it describes the methodology for data collection, storage, and processing within the framework of the project; it also introduces the chapters to be updated with the results of the procedures used to enforce accomplishment of the plan.

INCIT-EV aims to demonstrate an innovative set of charging infrastructures, technologies, and associated business models, ready to improve the EV users' experience beyond early adopters, thus, fostering the EV market share in the EU. The project will seek the emergence of EV users' unconscious preferences relying on the latest neuroscience techniques to adapt the technological developments to the users' subjective expectations with five demo environments at urban, peri-urban, and extra-urban conditions.

This Data Management Plan (DMP) has been developed in order to establish the measures for exploit and promote the findings during the project's life, it will enhance and ensure relevant project´s information transferability and will take into account the restrictions established by the consortium agreement, as well as the privacy and data protection issues. In this sense, the Plan will set the basis both for the Dissemination Plan and Exploitation Plan.

To evaluate the activities required to ensure INCIT-EV results, INCIT-EV will collect data from usage of electric vehicles (EVs) in general and will log and analyse various types of data relevant to trips done by people with such vehicles, to charging such vehicles and the usage of services and apps. Also, the opinions and attitudes of people will collect using questionnaires administered via INCIT-EV services or via wide online surveys.

The data, that would include personal data because of the possibility to attribute it to an indirectly identifiable natural person, will be processed within INCIT-EV for scientific reasons to analyse people's mobility and charging behaviour and, when possible, people's experiences with and attitudes regarding the usage of such vehicles. In the same way, for scientific reasons, INCIT-EV will collect a very large amount of technical data regarding charges and infrastructure developments.

All the data processing activities within INCIT-EV project must comply with the requirements of the General Data Protection Regulation (GDPR) [1] . Furthermore, INCIT-EV is participating in the Pilot on Open Research Data in Horizon 2020 so it must ensure that its data is FAIR, namely it is Findable, Accessible, Interoperable and Re-usable, and must follow their relevant guidelines [2] .

The report is structured as follows:

- Chapter 2 METHODOLOGY describes the overall methodology followed to collect, process and store data.
- Chapter 3 DATA SUMMARY detailing the propose of the data generation and collection including data types and formats.
- Chapter 4 FAIR DATA describes the procedures and guidelines to be followed to accomplish with data requirements from the Open Research Data pilot.
- Chapter 5 ALLOCATION OF RESOURCES
- Chapter 6 DATA SECURITY details all the procedures as well as the ITC tools and services used to ensure a secure management of the data during the project.
- Chapter 7 ETHICAL ASPECTS

- Chapter 8 MONITORING
- Chapter 9 FURTHER SUPPORT IN DEVELOPMENT INCIT-EV DMP
- Chapter 10 CONTRIBUTION TO EXPLOITATION AND DISSEMINATION
- Chapter 11 CONCLUSIONS

INCIT-EV's Data Management Plan is a living document that will report two new versions to detail the results of application of the rules and guides defined by this first version.

2 METHODOLOGY

The Data Management Plan (DMP) describes the data management life cycle for the data to be collected, processed, and/or generated by a HORIZON 2020 project. As part of making research data findable, accessible, interoperable, and re-usable (FAIR), a DMP will include information about the handling of research data during and after the end of the project:

- The kind of data the project will collect, process and/or generate, and to whom might it be useful.
- The methodology and standards that will be applied.
- The metadata required to enable data to be found and understood according to the standards of scientific discipline.
- The data that will be shared/made open access.
- The preservation of the data, including the period after the end of the INCIT-EV project, and the archive and preservation of open datasets.

2.1 Data to be collected within INCIT-EV analysis

Data could be collected by surveys, specific tools, and other equipment. Therefore, since some of the collected data in the latter case may involve sensitive data, all provisions for data management will be made in compliance with national and EU legislation, as described in the following paragraphs.

2.2 Data Collection and Storage Methodology

Overall, data will be stored in secure server systems and will be anonymised. Only the project coordinator and selected personnel from leading partners will possess the key to re-identification. No data, related to personal information of the involved participants will be collected and stored. Instead, all pilot participants will be granted with an identification number based on each participant's role, allowing mapping of participants' actions during the methodology execution. 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 leader of each related tasks. 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 period of time necessary to accomplish the goals of the project and the population of the INCIT-EV Repository. In any case, all data that will be considered confidential 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.

2.3 Users' data protection

There is a dedicated task to customers' research data handling, management, and protection. To protect the collected data and control unauthorised access to the INCIT-EV data repositories, only authenticated personnel will have access to 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, and 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. Towards the protection of personal data of specific participants, the following issues will be considered:

- All data associated with a recognizable person will be held private.
- Individual data on subjects 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 INCIT-EV 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.
- All individual information will be anonymised (or coded) in full and at the earliest possible point in time during data processing.
- The acquired data will under no circumstances be used for commercial purposes.

During the INCIT-EV 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 project's quality responsible and the project coordinator.

2.4 Data retention and destruction

Within the INCIT-EV 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. 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 INCIT-EV system and appropriate auditing of the peripheral components will be available.

2.5 Methodology & Guidelines for the delivery of Informed Consent

It will require the enrolment of people voluntarily declaring their consent to participate in the data and experiences collection activities of the project. Moreover, the consortium will take the appropriate action for ensuring that:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

1 Data cannot be collected without the explicit informed consent of people under observation; no person unable to express a free and informed consent for age-related reasons, on-going medical and / or psychological conditions, mental incapacity, will be enrolled in the study.

2 Data collected cannot be sold or used for any different purposes from the INCIT-EV project.

3 Any data, which is not strictly necessary to accomplish the current study, won't be collected; data minimisation policy will be adopted at any level of the project and will be supervised by the ethical/privacy component of the project.

4 Any shadow (ancillary) personal data obtained in the course of the observation will be immediately cancelled. However, we plan to minimize as far as possible this kind ancillary data. Special attention will be also paid to comply with Council of Europe's Recommendation R(87)15 on the processing of personal data for police purposes, Art.2: "The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry". Some sessions between technical and ethical components of the project will be devoted to this.

2.6 FAIR alignment

INCIT-EV adopted the FAIR DMP template, that has been designed to be appropriate for Horizon 2020 projects that produce, collect, store or process research data. The template describes the activities as part of the methodology and include:

- Data Summary
- FAIR Data
  - Making data findable, including provisions for metadata.
  - Making data openly accessible.
  - Making data interoperable.
  - Increase data re-use (through clarifying licenses as defined during project period).
- Allocation of resources
  - Explain the allocation of resources.
- Data Security
  - Address data recovery as well as secure storage and transfer of sensitive data.
- Ethical Aspects
  - In the context of the ethics management plan of the project as defined in Section 6 of this document.
- Other Issues
  - Refer to other national/funder/sectorial/departmental procedures for data management if any.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

2.7 Data access level classification process

The process to be followed by INCIT-EV DMP has been defined using a stepwise refinement for each result generated, processed, collected and stored during the INCIT-EV lifecycle and after led by the following questions which answers will enable classification of the different datasets:

1. Does a result provide significant value to others or is it necessary to understand a scientific conclusion?

- If the answer is yes, then the result is classified as public (granted for open access).
- If the answer is no, the result is classified as non-public.

For example, INCIT-EV specific code (e.g. a database initialization) is not for scientific interest to anyone, nor does it add any significant contribution.

2. Does a result include personal information that is not the author's name?

- If the answer is yes, the result is classified as non-public and personal information (e.g. name) must be removed before been published.

3. Does a result allow the identification of individuals even without the name?

- If the answer is yes, the result is classified as non-public.

This detailed in INCIT-EV ethics management plan as the INCIT-EV commitment to use anonymization techniques to conceal a single user's identity.

4. Can a result be abused for a purpose that is undesired by society in general or contradict with societal norms and the project’s ethics?

- If the answer is yes, the result is classified as non-public.

This detailed in INCIT-EV ethics management plan as the INCIT-EV commitment to use anonymization techniques to conceal a single user's identity.

5. Does a result include business or trade secrets of one or more partners of the project?

- If the answer is yes, the result is classified as non-public.

Business or trade secrets needs to be removed in accordance to all partners' requirements before it can be published.

6. Does a result name technology that are part of an ongoing, project-related patent application?

- If the answer is yes, then the result is classified as non-public.

In this case results can be published after patent has been filed.

7. Does a result break security interests for any project partner?

- If the answer is yes, the result is classified as non-public.

A simple methodology that ensures fast and easy way to determinate if data collections will be characterized as public or not.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

The following table summarizes the steps to determine the classification levels:

Table 2 - Classification Level Decision Table

Step	Question	Public	Non-Public
	Does a result provide significant value to others or is it necessary to understand a scientific conclusion?	Answer = Yes	Answer = No
2	Does a result include personal information that is not the author's name?	Answer = No	Answer = Yes
3	Does a result allow the identification of individuals even without the name?	Answer = No	Answer = Yes
4	Can a result be abused for a purpose that is undesired by society in general or contradict with societal norms and the project's ethics?	Answer = No	Answer = Yes
5	Does a result include business or trade secrets of one or more partners of the project?	Answer = No	Answer = Yes
6	Does a result name technology that are part of an ongoing, project-related patent application?	Answer = No	Answer = Yes
7	Does a result break security interests for any project partner?	Answer = No	Answer = Yes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

3 DATA SUMMARY

3.1 Purpose of the data collection and generation

This section outlines the purpose of the data collection and the generated results within INCIT-EV. A list of all collected data and existing or foreseeable results for dissemination is presented. The public data is separated into public deliverables, publications, and open research data. For each result and in accordance to the FAIR data management guideline (European Commission, 2013), also explained in detail in the following chapter, INCIT-EV provides a description, name the standards used for storage and metadata (making data findable & interoperable), and define on which open access platform it is handled.

INCIT-EV partners are committed to comply the ethical principles as set out in Article 34 of the Grant Agreement, which asserts that all project activities must be carried out in compliance with EU legislation towards data handling and preservation.

Software components related to data management will be included in next versions.

3.2 Data types and formats of data generated and collected

This section describes the different types of data sets that will be managed during the project:

- Deliverables
- Software data sets
- Questionnaires data sets
- Technical specifications related to devices (chargers, infrastructure). These will be part of deliverables related to WP3 and WP4.

Considerations for the specification of the data types:

- Data types details are not going to be provided because the project is still in an early stage. This information will be provided in next versions of the document.
- In the same way, information detailed about re-using data is not going to be included in this version.
- The size of data is not specified at this early stage. This information will be included in next versions.

3.2.1 Public Deliverable Management

The public deliverables generated in INCIT-EV are considered as part of the Data Management Plan. These are described in the following table. These documents will be published openly on the INCIT-EV webpage managed by CIRCE. Furthermore, CIRCE will make regular backup of this webpage with its public deliverables. Also, these documents will be added to Zenodo [3].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

Table 3 - Public Deliverables

Del. number	Deliverable title	WP	Type	Due Date
D2.1	User characterization: patterns and habits	WP2	Report	9
D2.2	List of users and stakeholders engaged for the use cases	WP2	Report	9
D2.3	Users expectations and concerns about e-mobility	WP2	Report	27
D2.4	Use cases evaluation from the users' perspective	WP2	Report	48
D2.5	Future strategies and recommendations to support e-mobility	WP2	Report	48
D2.6	Update of User characterization: patterns and habits	WP2	Report	28
D3.5	Report on user centric EV charging infrastructure	WP3	Report	12
D3.10	Update of Report on user centric EV charging infrastructure	WP3	Report	24
D4.6	Grid, urban and road infrastructure upgrading for meeting users' expectations report	WP4	Report	12
D4.12	Update of Grid, urban and road infrastructure upgrading for meeting users' expectations report	WP4	Report	24
D5.4	ICT Data Management Plan	WP5	Report	6
D5.6	INCIT-EV user interfaces	WP5	Demo	24
D5.10	First Update of ICT Data Management Plan	WP5	Report	18
D5.11	Second stage of Implementation of INCIT-EV ICT platform	WP5	Demo	36

D5.12	Second stage of INCIT-EV user interfaces	WP5	Demo	36
D5.15	Final Update of ICT Data Management Plan	WP5	Report	36
D7.2	Amsterdam-Utrecht urban area UC-1 complete solution description	WP7	Report	30
D7.4	Paris urban area UC-2 complete solution description	WP7	Report	30
D7.6	Saragossa urban area energy model and UC-6 and UC-7 complete solution description	WP7	Report	30
D8.2	Turin peri-urban area UC-4 complete solution description	WP8	Report	30
D8.4	Paris extra-urban area UC-3 complete solution description	WP8	Report	30
D8.6	Tallinn extra-urban area UC-5 complete solution description	WP8	Report	30
D8.11	Update of Tallinn extra-urban area UC-5 complete solution description	WP8	Report	48
D9.1	Use cases value proposition considering the whole ecosystem	WP9	Report	24
D9.2	Demand Scenarios (Roadmap) for the different use cases through PESTEL and estimation of penetration curves	WP9	Report	24
D9.4	LCCA for the 7 use cases	WP9	Report	42
D9.5	Proposal for pricing and revenue models in the 7 uses cases	WP9	Report	42
D9.7	Replication potential of technologies in the EU. Action plans for the INCIT-EV cities and TEN-T corridors	WP9	Report	48
D9.9	Regulation and standards recommendations on electric infrastructure charging	WP9	Report	48

D10.1	Dissemination and Communication Plan including project identity set	WP10	Report	6
D10.2	Project website	WP10	patents	4
D10.3	Project visual materials	WP10	Other	6
D10.4	Project synergies report	WP10	Report	12
D10.5	Mid-term Dissemination and Communication report	WP10	Report	24
D10.6	Citizens and tourism engagement	WP10	Report	48
D10.7	Final report on communication and dissemination activities	WP10	Report	48
D10.8	First update of Dissemination and Communication Plan	WP10	Report	18
D10.9	First Update of Project visual materials	WP10	Other	18
D10.10	Final update of Dissemination and Communication Plan	WP10	Report	36
D10.11	Second Update of Project visual materials	WP10	Other	36
D10.12	Final Update of Project visual materials	WP10	Other	48

3.2.2 Deliverables submitted

The following table includes all deliverables, organized by WP, submitted at month 6 of the INCIT-EV project.

Table 4 - Deliverables submitted

Deliverable number and name	Month	Type	Diss. Level	Publication deliverable code
D1.1 Project Handbook	3	Report	CO	D1_1_INCIT-EV_Project handbookv1_2.pdf
D1.2 Project Management collaborative space Guide	3	Report	CO	D1_2_INCIT-EV_Project Management Collaborative Space Guide.pdf
D1.3 Project Management Plan	2	Report	CO	D1_3_INCIT-EV_Project Management Plan_1.2.pdf
D1.6 Data Management Plan	6	ORDP	CO	D1_6 INCIT-EV_DMP ORDP.pdf
D5.4 ICT_Data_Management_Plan	6	Report	PU	D5_4_INCIT-EV_ICT_Data_Management_Plan.pdf
D10.1 Dissemination and Communication Plan including project identity set	6	Report	PU	D10_1_INCIT-EV_Dissemination_and_ Communication_plan.pdf
D10.2 Project website https://www.incit-ev.eu/	4	Patents	PU	INCIT-EV – D10.2 Project Website.pdf
D10.3 Project visual materials	6	Other	PU	D10_3_INCIT-EV_Project Visual Materials.pdf
D11.1 H - Requirement No. 1	3	Ethics	CO	D11_1_INCIT-EV_H requirement.pdf
D11.2 POPD – Requirement No. 2	3	Ethics	CO	D11_2_INCIT-EV_PODP requirement n2.pdf
D11.3 NEC - Requirement No. 3	3	Ethics	CO	D11_3_INCIT-EV_NEC requirement_3.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

3.2.3 Software Data Sets

The following table describes the Data Software components:

Table 5 - Software Components

Software Component	Partner	SI (Software Identifier)
INCIT-EV Platform	ATOS	S1
INCIT-EV User Interfaces and Payment	GFX	S2
INCIT-EV DSS (Decision Support System) and service application tools	LINKS	S3
INCIT-EV DSS and Service Layer Integration and Orchestration engine	ATOS	S4

The INCIT-EV DSS and Service Layer Integration and Orchestration engine will manage the deployment of the components.

Table 6 - Datasets related to Software Components

Data Set	Software Components involved	Potential Sensitive Information
Applications information (name, version)	S4, S1	
Libraries information (name, version)	S4, S1	
Subcomponents information (data bases, middleware, security components.)	S4, S1	
DSS protocols information	S4, S1, S3	
Payment protocols information	S4, S1, S3	
Charging infrastructure information	S1, S2, S3, S4	
User needs	S2, S3	X
User costs	S2, S3	X
EV charging profiles	S2, S3	X

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

Grid information	S3, S2	
Civil modifications for charging infrastructures	S3	
Infrastructure requirements for light-electric vehicle parking	S3	
Infrastructure requirements for charging infrastructures	S3	
Trips done by people	S1, S2, S3	X
Usage of services	S1, S2, S3	X
Usage of apps	S1, S2, S3	X
Usage of vehicles	S1, S2, S3	X

3.2.3.1 DSS Data Sets

Table 6 shows more detailed information about the data sets managed by the Decision Support System (DSS) implemented in WP6, led by LINKS. The table contains both the input data and the expected output data: it shows the datasets that the tool will need to make useful analyses together with the corresponding output for each module.

There are many cells still undefined at this stage because the development of the WP6 and the DSS is still in the requirements specification phase. The next versions of this document will provide further details.

Table 7 - DSS Data sets

Data Set	Input (I) / Output(O)	Data	Public Access	Third party	All INCIT-EV partners	Specific partner
Charging Stations	I	Position (Latitude, Longitude)		X		
	I	Quantity (Number of available connectors grouped by type of charging)		X		
	I	Type: Power (i.e. slow vs fast vs super-fast), Voltage, Technology (i.e. conductive vs inductive) , Connectors, efficiency, constraints (maximum power, queue, etc.)		X		
	I	Pricing		X		
	I	Operativity (True, False)		X		
	I	List of Connected Buildings (shops, offices, companies, lodging, restaurants, public transport stops)		X		
	O	Possible suggestions about suitable new charging stations solutions (e.g. position, quantity, type) TBD				
EV Penetration	I	Family Incomes	TBD	TBD	TBD	TBD
	I	Real estate values	TBD	TBD	TBD	TBD
	I	# private parking places	TBD	TBD	TBD	TBD

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

	O	#EVs per segment				
Price	I	Electricity price per hour of the day	TBD	TBD	TBD	TBD
	O	Best daily hours and charging stations				
EV Mobility	I	Floating Car Data (FCD)	TBD	TBD	TBD	TBD
	I	OD Survey	TBD	TBD	TBD	TBD
	I	#EVs per segment	Output of EV Penetration			
	O	Parking Duration				
	O	#Trips/Day				
	O	Km/trip				
	O	Fuel consumption/trip				
	O	EVs OD				
Parking	I	Buildings location (e.g. Public Offices, Hospitals, Private Offices, Shops, Supermarket/Shopping Center)	TBD	TBD	TBD	TBD
	O	Parking Duration				
OD Matrix	I	Population	TBD	TBD	TBD	TBD
	I	Workers	TBD	TBD	TBD	TBD
	I	#EVs per segment	Output of EV Penetration			
	O	EVs OD				
	O	km traveled				
	O	Charging needs				
Sizing and Sitting	I	Population	TBD	TBD	TBD	TBD
	I	Workers	TBD	TBD	TBD	TBD
	I	**Power Grid Data Set**				
	O	# Charging Stations				
	O	Location of CS				
	O	Power of CS				
	O	Technologies of CSs				
Power Grid	I	secondary substations (capacities and constraints)	TBD	TBD	TBD	TBD
	I	aggregated load profiles per station	TBD	TBD	TBD	TBD
	I	indication about available renewables	TBD	TBD	TBD	TBD

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

EV Drive	I	Anxiousness	TBD	TBD	TBD	TBD
	I	Departure State of Charge (SoC)	TBD	TBD	TBD	TBD
	I	EV Autonomy	TBD	TBD	TBD	TBD
	I	EV class	TBD	TBD	TBD	TBD
	I	SoC max	TBD	TBD	TBD	TBD
	I	Typical/representative calendar	TBD	TBD	TBD	TBD
	I	Parking Duration	TBD	TBD	TBD	TBD
	O	Drive Profile				

3.2.3.2 User Interfaces and Payment application

Table 7 shows an overview of the data sets managed by the User Interfaces and Payment application led by GFX. At this stage of the project, there are many cells still undefined. The next versions of this document will provide further details from this first version.

Table 8 - User Interfaces and Payment Application Data Sets

Data Set	Input (I) / Output(O)	Data	Public Access	Third party	All INCIT-EV partners	Specific partner
User Information		Personal data (name, surname…)	NO	NO	NO	NO
		Ad-hoc charging	NO	NO	NO	NO
		Anonymized Charge Data Records	NO	NO	NO	
OCPI (T5.3 & T5.6)						
OICP (T5.3 & T5.6)						
OSCP (Task 5.6)						
OCPP (Task 5.6)						

3.2.4 Data questionnaires

INCIT-EV's WP2 is responsible for conduct various questionnaires to a previous constructed list of users and stakeholders that has been engaged for each of the use cases involved in the project. The aim of the surveys is collecting the users' expectations and concerns about e-mobility for analysis proposes, the evaluation of the use cases from the users' perspective and collect recommendations that enable definition of future strategies that will support the enhancement of e-mobility.

Questionnaires will be classified based on the patterns and habits that characterize the users; therefore, no identity data will be collected during the survey, only for example, the respondent's city of residence, age group, gender, and current occupation if they are required. The collected data will be anonymous, stored in INCIT-EV repository and with limited rights of access.

Task 2.3 (M7-M27) will address the online questionnaires across at least 10 European Countries. We must pay special attention to the data management of sensitive information that will be followed according to section 6 (Data Security).

3.2.5 Bio signal acceptance information from user experiences

Task 2.4 (M25-M48) addresses a pilot study to identify the behaviour and perception of users regarding the electric mobility. This study includes behavioural cues provides by eye-tracking systems and body reactions provided by biosensors (GSR, heart rate, EEG).

We must pay special attention to the data management of the sensitive information that must be managed considering section 6.

4 FAIR DATA

4.1 Making data findable, including provisions for metadata

The INCIT-EV project has a strong commitment on making sure that the generated data will be identifiable and easily discoverable. For this purpose, metadata based on the OpenAIRE guidelines [4] for Data Archives[1] will be created. OpenAIRE has adopted the DataCite Metadata Schema v3.1 [5] and apart from a Digital Object Identifier (DOI), accepts also other persistent identifier schemes, such as Archival Resource Key (ARK), Handle, Persistent Uniform Resource Locator (PURL), Uniform Resource Name (URN) and Uniform Resource Locator (URL).

Regarding INCIT-EV documents/deliverables, clear and harmonized naming conventions will be used. Appropriate keywords will be selected, to facilitate the documents discoverability.

4.1.1 Findable documents

This section specifies the rules for facilitating storage and browsing of the documents. The rules are the following:

- No white spaces should be used in the document names. Use "-" instead of white spaces.
- Document must start with prefix "INCIT-EV".
- The conventions for the naming of the document are the following:

  "D[ID]_ INCIT-EV_ [Title]_v[Version].ext"

  Where:

  - ID is the identifier of the deliverable (e.g. 5.4)
  - Title is the title of the deliverable (with "-" instead of white spaces)
  - Version is the version number of the deliverable
  - Date is the creation/editing date in the format DD.MM.YY
  - Partner is the short name of the partner responsible for the deliverable.
  - Ext is the file extension of the file format (e.g.: pdf, docx…)

Regarding the publications of INCIT-EV project, Digital Object Identifiers (DOIs) [6] will be used to help retrieval.

4.2 Making data openly accessible

INCIT-EV project will participate in the 'Pilot on Open Research Data in Horizon 2020' with the rationale to provide open access of scientific publications; research integrity will be increased through transparency,

[1] https://guidelines.openaire.eu/en/latest/data/index.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

impact will be greater through re-use, duplication of efforts will be reduced, and civil society will benefit from better value from its financial contribution.

There are four main aspects of open data summarised in the acronym FAIR[2]:

- **Findable**: data has a unique, persistent ID, located in a searchable resource, and documented with meaningful metadata.
- **Accessible**: data is readily and freely retrievable using common methods and protocols, metadata is accessible even if the data is not.
- **Interoperable**: data is presented in broadly recognised standard formats, vocabularies, and languages.
- **Re-useable**: data has clear licences, and accurate meaningful metadata conformity relevant community standards and identifying its content and provenance.

INCIT-EV's data management plan establishes how this approach will be realised in practice with the initial plan presenting an overview and detail will be provided in the interim and final reports as the work packages proceed.

Project datasets for dissemination will be open access by default, as a minimum to validate scientific publications. However, not all project`s work packages will produce datasets that are intended for public dissemination; much of the data created and stored during the project is for internal management and communication within the consortium only. Of the datasets intended to be open access some, such as those that identify residential users, may also require aggregation or anonymization for security or commercial reasons prior to release.

Furthermore, the INCIT-EV repository will be registered in the Registry of Research Data Repositories[3] and the data will be offered under Creative Commons License Attribution-Non-Commercial CC BY-NC [7]. Specific scripts will be offered for accessing these data (using simple scripting language such as python or Perl) and offering basic statistics on the data. The source code of these access applications to Zenodo will be offered and will be made available on a public repository (e.g. GitHub) along with detailed documentation of usage.

All project deliverables will be available to authorized users in the project's working space managed by Microsoft Teams [8].

The public project deliverables and the executive summaries of deliverables which are not public will be available in the INCIT-EV website and will be made available to the ResearchGate. Consequently, all deliverables defined in the Description of Action as Public will be provided within an open space on the project website [9] after their review and approval by the EC, enabling everyone to access them.

For the rest of deliverables considered confidential (content is restricted), its executive summary will be available in the project website after the EC approval. These deliverables will be findable by the consortium via Microsoft Teams, which is managed by Renault SAS.

[2] https://www.force11.org/group/fairgroup/fairprinciples

[3] https://www.re3data.org/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

INCIT-EV will follow the Open Access [10] practice of providing online access to its scientific research articles, selecting either:

- Self-archiving/'green' open access – the author, or a representative, archives (deposits) the published article or the final peer-reviewed manuscript in an online repository before, at the same time as, or after the publication.
- Open access publishing/'gold' open access - an article is immediately published in open access mode.

4.3 Making data interoperable

All the data managed within the project will be available using dedicated scripts using APIs to access the INCIT-EV platform. The platform API will be open and thoroughly documented in order to enable and encourage its usage from every third-party application without forcing any dependencies on the provided scripts. It will also use established standards as much as possible.

Data models supported by the software will be open and available to interested developers. The project tools will be based on open source software to facilitate their adoption and possible modifications.

The data in the repository will be exposed in a text format following well-known and established standards (e.g., CSV, JSON or XML).

4.4 Increase data re-use (through clarifying license)

As mentioned, the public data from the INCIT-EV repository will be licensed for scientific purposes under Creative Commons License Attribution-Non-Commercial (CC BY-NC) after the completion of the project. Other than the ones imposed by this license, no other restrictions for re-usage by third parties are envisaged. The data will be available for five years after the project end.

INCIT-EV is part of the EC's Open Research Data Pilot Programme. Therefore, it must be easy to access and use the data generated by the project. This is described in the deliverable D1.6.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

5 ALLOCATION OF RESOURCES

The responsibilities are defined in the DOA in the within the Data Protection Board in the "3.2 Management structure and procedures" section. The Data Protection Board managers are responsible for the correct application of data protection rules throughout the project, promoting cooperation with the EU's data protection authorities. This board will report periodically to the coordinator regarding the data protection issues related to each demo.

The Board is Chaired by Renault SAS and will count with the contributions of ATOS, LINKS, GFX, BITBRAIN, POLITO, VEDECOM, CIRCE and EESTI.

The Data Protection Board will hold meetings on demand and continuous communication during demo phase of the project.

The Responsibilities are the following:

- Ensure proper and consistent application of data protection regulation throughout the project.
- Provide general guidance (guidelines, recommendations, best practice) to clarify law and its relevance to INCIT-EV.
- Foresee and identify possible data protection issues to propose contingency plans.
- Advise project's management bodies on any issue related to protection of personal data and upcoming legislation in the EU.

At this stage of the project, no resources for long term preservation are discussed.

5.1 Financial resources for FAIR data

This section will report regarding Project's cost for making data fair including detailed descriptions for sources for the required funds to cover the costs during the following updates of the document.

At this stage of the project, it is not possible to define whether additional financial resources need to be allocated for the data management related to FAIR guidelines. If such costs arise the consortium will agree, they would be associated with the cost of storage of collected data or fees to be submitted to public repositories.

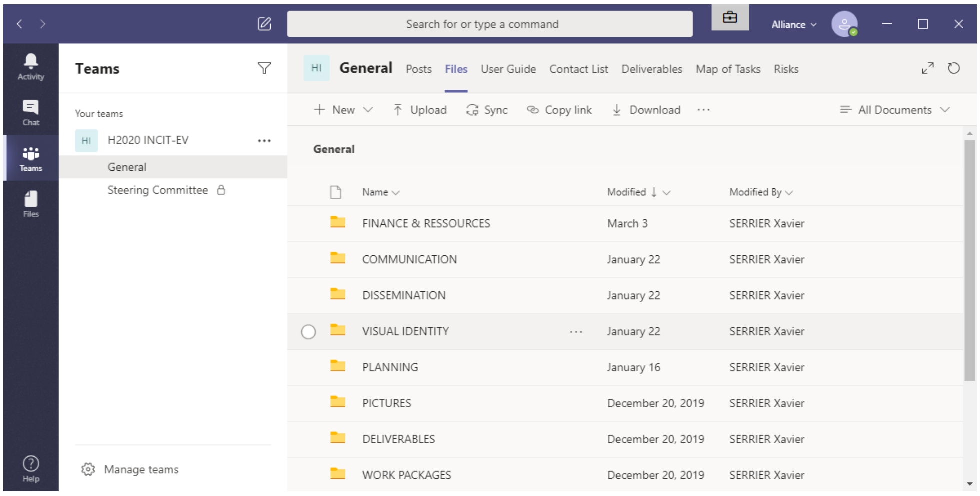
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

6 DATA SECURITY

6.1 Storage location and access level

Collected data can be categorized according to their storage location and the access level:

- **Private**: It is referred to consent forms, questionnaires and **personal data** collected by partners. In case of paper responses, these should be stored in locked compartments. In case of digitalized copies, these should be only accessed by authorized personnel and protected by password according to the regulations. The management of this type of information is regulated by GDPR and described in the section 6.2.
- **Consortium**: Renault SAS is responsible for archiving and maintaining the project data files. Renault SAS has provided a common space based on Microsoft Teams [8] which is secure and accessible to all partners. This cloud tool can configure different levels of access depending on the user credentials. The Consortium data is uploaded to this cloud tool in order to facilitate the secure access for all partners. Regular backups of Microsoft Teams have been scheduled. The following picture shows the "H2020 INCIT-EV" group configured on this tool to manage this type of information.



Name	Modified ↓	Modified By
FINANCE & RESSOURCES	March 3	SERRIER Xavier
COMMUNICATION	January 22	SERRIER Xavier
DISSEMINATION	January 22	SERRIER Xavier
VISUAL IDENTITY	January 22	SERRIER Xavier
PLANNING	January 16	SERRIER Xavier
PICTURES	December 20, 2019	SERRIER Xavier
DELIVERABLES	December 20, 2019	SERRIER Xavier
WORK PACKAGES	December 20, 2019	SERRIER Xavier

Figure 1: INCIT-EV Microsoft Teams

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

- **Open**: The project results will be made available openly through different tools like: Zenodo [3] , ResearchGate [11] and GitHub [12].

6.2 GDPR and DPIA

6.2.1 GDPR requirements

6.2.1.1 General principles

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR) [2] comes into force on 25 May 2018. The GDPR applies to organisations processing and holding personal data of data subjects residing in the European Union, regardless of the organization's location.

Below are some useful definitions from the GDPR:

- Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- Processor means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

The general principles pursued by the GDPR requirements are that personal data shall be

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and further processed for scientific purposes.
- Adequate, relevant and limited to what is necessary for the purposes for which they are processed.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

The GDPR sets specific requirements for processing of special categories of personal data (for example revealing race, health, politics, religion), but such data will not be collected or processed in INCIT-EV.

6.2.1.2 Data subject's consent to the processing

According to the GDPR a lawful basis for processing of personal data exists when the individual (the data subject) has given clear consent to process his/her personal data for a specific purpose. The following should be ensured when requesting a data subject to give consent:

- the request for consent should be prominent and separate
- the request for consent should be written in clear, plain, easy to understand language
- it should include:
    - the identity and the contact details of the Controller
    - the contact details of the Data Protection Officer (DPO)
    - the purposes of the processing
    - the recipients of the personal data
    - the period for which the personal data will be stored
    - the existence of the subject's rights to request access / rectification / erasure / restriction of processing, object to processing, data portability, withdraw consent, lodge a complaint with a supervisory authority
    - the existence of automated decision-making, including profiling. If this exists, then meaningful information should be provided about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
- subjects should be asked to positively opt in
- subjects should be asked to consent separately to different purposes and types of processing

Consent should not be a precondition of a service and subjects who wish to withdraw their consent should not be penalised.

Furthermore, the consents should be regularly reviewed to check that the processing and purposes have not changed from what was told to the subjects. Therefore, processes should be established to refresh consent at appropriate intervals.

6.2.1.3 Data subject's rights

According to the GDPR, the data subject has the following rights.

Right to be informed

Fair processing information should be provided to the subjects. The information should be concise, transparent, intelligible, and easily accessible. It should be written in clear and plain language and it should be given free of charge.

Right of access

Individuals have the right to obtain confirmation as to whether or not personal data are being processed. If processing takes place, they have the right to access the data and to the information provided in order to get

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

consent. The subjects should be aware and should be able to verify the lawfulness of the processing. The right of access should be given free of charge unless it is unfounded or excessive. If requested, the information must be provided without delay, at the latest within one month of receipt of the request.

Right to rectification

Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete. If requested, a response should be given within one month from the request.

Right to erasure

This is granted in specific circumstances:

- When data is no longer necessary.
- When the individual withdraws consent.
- When the individual objects to the processing.

Right to restrict processing

Individuals have the right to block processing of personal data under certain conditions, in which case data can be stored but not processed.

Right to data portability

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. Therefore, personal data should be easily copied, moved, transferred from one IT environment to another in a safe and secure way and free of charge. This means that, if requested by the subject, personal data should be provided in a structured, commonly used and machine-readable form (for example as a csv file).

Right to object

Individuals have the right to object to processing. Processing must stop as soon as an objection is received. Individuals must be informed of their right to object “at the point of first communication”. This right should be presented clearly and separately from other information.

Rights related to automated decision-making including profiling

Profiling includes algorithms to analyse or predict behaviour, location or movements. In such cases:

- Meaningful information about the logic involved in profiling should be provided together with the significance and consequences.
- Appropriate mathematical or statistical procedures should be involved for the profiling.
- Measures to enable the correction of inaccuracies and to minimise risk of errors should be implemented.

Automated decision making must not concern children and must not be based on processing special categories of data.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

6.2.1.4 Controller's and Processor's obligations

The Controller should implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR requirements. Appropriate measures for data protection should be implemented, such as pseudonymisation and data minimisation. The latter means that only personal data which are necessary for the processing will be processed. This applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

The Processor should process the personal data only on documented instructions from the Controller, should ensure that persons authorised to process the personal data have committed themselves to confidentiality and should delete or return all the personal data to the Controller after the end of the processing.

The Controller should maintain a record of processing activities, which must contain the following information:

- The name and contact details of the Controller and the Data Protection Officer.
- The purposes of the processing.
- A description of the categories of data subjects and of personal data.
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.
- The envisaged time limits for erasure of the different categories of data.
- A general description of the technical and organisational security measures.

The Controller should implement appropriate technical and organisational measures to ensure data security. These may include:

- The pseudonymisation and encryption of personal data.
- The assignment of processing and access rights responsibilities.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

In the case of a personal data breach, the Controller should without undue delay notify the breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller should communicate the breach to the data subject without undue delay.

6.2.2 DPIA

According to Article 35 of the GDPR, a Data Protection Impact Assessment (DPIA) should contain at least four essential aspects. The first is a systematic description of the processing operations and the purposes of the processing. It should also assess the necessity and proportionality of the processing in relation to the purposes. The risks to the rights and freedoms of the data subjects must also be included, as well as the measures taken to address the risks. These measures can include safeguards, security measures and other mechanisms to protect personal data. DPIA must be performed before the processing begins. The controller has the responsibility to ensure this requirement is satisfied. Consultation with a Data Protection Officer (DPO) is also advised, but not mandatory. Another important aspect is to look at compliance with any codes of conduct when performing the DPIA [13] .

6.3 Cybersecurity protection

6.3.1 INCIT-EV approach

INCIT-EV's data repositories will be protected to control unauthorised access, only authorized and authenticated personnel will have access to data collected. Therefore, a dedicated security approach will be followed, to ensure confidentiality, integrity, and availability. The security approach will be defined by a methodical assessment of security risks followed by their impact analysis.

Responsibilities will be clearly assigned for the management and control of research data and the controlling of access rights issues of data security will directly inform the Data Protection Board, the Steering Committee and the project coordinator following INCIT-EV governance and management procedures that will be detailed in the D1.1 - Project Handbook.

The main procedures implemented by the INCIT-EV Consortium are the following:

- All partners agree that all personal data collected will be treated as confidential and no actions will be undertaken unless the partners have the consent by the users (data subjects).
- Users that will participate in any testing or demonstration activity or in any other of its events will be asked to sign beforehand a consent form on the terms of data collection, treatment, and further use.
- Users that will participate in any testing or demonstration activity or in any other of its events will be provided with access to their data when requested and will have the right to force the deletion of said data.

Personal data will not be in any case shared with or disclosed to anyone outside the research team. Only if necessary or required, will this data be shared with the European Commission. However, the consortium may disclose collected data to the extent that it is required to do so by law, in connection to any legal proceedings or prospective legal proceedings and in order to establish, defend or exercise its rights.

INCIT-EV will use a data minimisation policy, meaning that only data strictly necessary for the validation activities will be collected and processed. Personal data, if any, collected and stored and for the purpose of the project activities will be permanently and irrevocably erased on the project completion. Nevertheless, only if an individual participant has provided his/her free, specific, written, and informed consent will personal data be included in project outputs. If such a consent is not provided by the individual participant, only information that may be processed in a way that inhibits tracing his/her opinions back to him/her (anonymised information) can be included.

Apart from organisational measures to ensure data protection, technological measures are also foreseen to be used during system implementation. Although, there is a dedicated section where INCIT-EV Cybersecurity Services (ICS) is defined, the following measures will be applied when relevant:

- Pseudonymisation/anonymisation of personal data.
- Data minimisation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

- Applied cryptography (e.g. encryption and hashing).
- Usage of data-protection focused service providers and storage platforms.
- Arrangements that enable data subjects to exercise their fundamental rights (e.g. as regards direct access to their personal data and consent to its use or transfer).

6.3.2 Consortium Security Tool

The information related to the Consortium will be managed throughout Microsoft Teams.

Microsoft Teams [8], also referred to as simply Teams, is a unified communication and collaboration platform that combines persistent workplace chat, video meetings, file storage (including collaboration on files), and application integration. The service integrates with the Office 365 subscription office productivity suite and features extensions that can integrate with non-Microsoft products. Microsoft Teams is a competitor to services such as Slack and is the evolution and upgrade path from Microsoft Skype for Business.

6.3.3 Open Access Security Tools

The information to be distributed openly will be managed throughout the following tools:

- The INCIT-EV webpage managed by CIRCE. CIRCE will make regular backup of this webpage with its public deliverables.
- Zenodo [3]: this tool provides clear security guarantees. All data files are stored in CERN Data Centres, primarily Geneva and replicated in Budapest. Data files and metadata are backed up on a nightly basis. Files are regularly checked against their checksums (using MD5 algorithm) to assure that file content remains constant. In case of closure of the repository, Zenodo ensures that efforts will be made to integrate all content into suitable alternatives.

6.3.4 Private Access Security Tool

The Cybersecurity services are referred to the implementation of the cybersecurity protection measures to secure access to the system and APIs. The project will define different roles and actors with their associated responsibilities that will be tracked (end-users, DSO, CPO…).

Regarding the technologies that will be used to implement this security mechanisms, ATOS FUSE platform provides authentication and authorization mechanisms based on existing tools like Keycloak [14] and Kong [15] .

More specific detailed information of the INCIT-EV specific adaptation of the security mechanisms will be detailed in the next version of this document.

7 ETHICAL ASPECTS

The INCIT-EV consortium is fully aware that several ethical, privacy and data protection issues will be raised during the performance of the activities defined for the project. For avoidance of repetitions the reader is advised to refer to the following already submitted deliverables:

- D11.1 H- Requirement No. 1
- D11.2 POPD - Requirement No. 2

D11.1 H- Requirement No. 1 define and describe the ethics management strategy for the project duration. The consortium declares that will comply with all the ethics requirements considering Humans (INCIT-EV Grant Agreement section 5.1.3 on Ethical Policy) as further described in the D11.1 H- Requirement No. 1.

During project implementation, among other things, INCIT-EV will enforce:

- The procedures and criteria that will be used to identify/recruit research participants will be submitted as a deliverable before the start of the ethically relevant task.
- The description of the informed consent procedures that will be implemented for the participation of humans will be submitted as a deliverable before the start of the ethically relevant task.
- The templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) will be kept on file.
- Copies of opinions/approvals by ethics committees and/or competent authorities for the research with humans will be kept on file.

D11.2 POPD - Requirement No. 2 sets out ethics requirements considering protection of personal data (POPD) that INCI-EV project must comply with. Therefore, the consortium declares:

- INCIT-EV Consortium will check if special derogations pertaining to the rights of data subjects or the processing of genetic, biometric and/or health data have been established under the national legislation of the country where the research takes place and submit a declaration of compliance with respective national legal framework(s).
- The host institution will confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project will be submitted as a deliverable.
- Justification for the processing of sensitive personal data must be submitted as a deliverable.
- A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/ research participants must be submitted as a deliverable. Description of the anonymisation/ pseudonymisation techniques that will be implemented must be submitted as a deliverable.
- In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679, must be submitted as a deliverable. In case personal data are transferred from

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected must be submitted as a deliverable.

- Detailed information on the informed consent procedures regarding data processing must be kept on file.
- Templates of the informed consent forms and information sheets (in language and terms intelligible to the participants) must be kept on file.
- Ethical standards and related guidelines of Horizon 2020 and applicable regulatory frameworks are always respected.

Both documents detail the ethics methodology that will be used during INCIT-EV performance to ensure compliance with all the applicable ethics requirements to ensure ensures that the ethical standards and related guidelines of Horizon 2020 framework are always respected.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

8 MONITORING

This chapter will be updated to register the information related to the data management monitoring and compliance with the GDPR legal framework. Also, this document will monitor the integration of cyber-protection mechanisms to prevent access to INCIT-EV resources to actors and users not granted.

Special attention regarding the management of sensitive information will be paid on the following actions:

- Task 2.3 (M7-M27): This task will address the online questionnaires across at least 10 European Countries. We must pay special attention to the data management of this information that will be followed according to section 6 (Data Security)
- Task 2.4 (M25-M48): This task will address a pilot study to identify the behaviour and perception of users regarding the electric mobility. This study includes behavioural cues provides by eye-tracking systems and body reactions provided by biosensors (GSR, heart rate, EEG).
- Task 5.5 (M4-M36): This task will integrate cyber-protection mechanisms to prevent access to INCIT-EV ICT resources to actors and users not granted. Special attention will be paid on Table 6 - Datasets related to Software Components.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

9 FURTHER SUPPORT IN DEVELOPMENT INCIT-EV DMP

The Research Data Alliance provides a Metadata Standards Directory that can be searched for discipline-specific standards and associated tools.

The EUDAT B2SHARE tool includes a built-in license wizard that facilitates the selection of an adequate license for research data.

Useful listings of repositories include:

- Registry of Research Data Repositories.
- Some repositories like Zenodo [3], an OpenAIRE [4] and CERN collaboration), allow researchers to deposit both publications and data, while providing tools to link them.
- Other useful tools include DMP online and platforms for making individual scientific observations available such as ScienceMatters.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

10 CONCLUSIONS

This deliverable describes the data management plan of INCIT-EV identifying the data to be collected and generated in the project, stablishing the bases on how the consortium will ensure the data management will comply with FAIR data principles. Furthermore, data protection, cybersecurity and ethical issues were also analysed.

At this stage, this document gives a preliminary information about the data types collected and generated by the project, therefore this document is considered as a working document which will be further updated during the project lifetime. More detailed information of the data types will be provided in next versions.

Other important aspects covered in this document is referred to the sharing data collected in the project and the storage.

Currently, the monitoring section set the most important action points regarding the data management and is intended to collect the monitoring results during the project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein

11 REFERENCES

[1] 'EUR-Lex - 32016R0679 - EN - EUR-Lex'. https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed Jun. 08, 2020).

[2] 'Open access - H2020 Online Manual'. https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/open-access_en.htm (accessed Jun. 08, 2020).

[3] 'Zenodo - Research. Shared.' https://zenodo.org/ (accessed Jun. 10, 2020).

[4] 'OpenAIRE Guidelines — OpenAIRE Guidelines documentation'. https://guidelines.openaire.eu/en/latest/ (accessed Jun. 18, 2020).

[5] 'DataCite Schema', *DataCite Schema*. https://schema.datacite.org/ (accessed Jun. 18, 2020).

[6] N. Paskin, 'Toward unique identifiers', *Proc. IEEE*, vol. 87, no. 7, pp. 1208–1227, Jul. 1999, doi: 10.1109/5.771073.

[7] 'Creative Commons — Attribution-NonCommercial 3.0 Unported — CC BY-NC 3.0'. https://creativecommons.org/licenses/by-nc/3.0/ (accessed Jun. 16, 2020).

[8] 'Chat, Meetings, Calling, Collaboration | Microsoft Teams'. https://www.microsoft.com/en-us/microsoft-365/microsoft-teams/group-chat-software (accessed Jun. 17, 2020).

[9] admin, 'INCIT-EV Project | Electric charging solutions for Electric Vehicles', *INCIT-EV Project*. http://www.incit-ev.eu/ (accessed Jun. 16, 2020).

[10] 'h2020-hi-oa-data-mgt_en.pdf'. Accessed: Jun. 08, 2020. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

[11] 'Home Feed', *ResearchGate*. https://www.researchgate.net/ (accessed Jun. 16, 2020).

[12] 'Build software better, together', *GitHub*. https://github.com (accessed Jun. 16, 2020).

[13] 'DPIA - What it is, When is it Needed and Why', *EU GDPR Compliant*, Sep. 01, 2017. https://eugdprcompliant.com/dpia-guidelines/ (accessed Jun. 10, 2020).

[14] 'Keycloak'. https://www.keycloak.org/ (accessed May 20, 2020).

[15] KongHQ, 'Open-Source API Management and Microservice Management', *Kong*. https://docs.konghq.com (accessed May 20, 2020).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 875683. Disclaimer: The sole responsibility for any error or omissions lies with the editor. The content does not necessarily reflect the opinion of the European Commission. The European Commission is also not responsible for any use that may be made of the information contained herein