SAFEWAY

GIS-Based Infrastructure Management System for Optimized Response to Extreme Events of Terrestrial Transport Networks

Data Management Plan (DMP) V2 (D1.5)

February 2020 (V1.0)

PUBLIC

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 769255.

SAFEWAY

GIS-BASED INFRASTRUCTURE MANAGEMENT SYSTEM FOR OPTIMIZED RESPONSE TO EXTREME EVENTS OF TERRESTRIAL TRANSPORT NETWORKS

Grant Agreement No. 769255

Data Management Plan (DMP) V2

WP 1 Overall Project Coordination

Deliverable ID	**D1.5**
Deliverable name	**Data Management Plan (DMP) V2**
Lead partner	**UVIGO**
Contributors	DEMO, PNK, UMINHO, IMC

PUBLIC

SAFEWAY Project Synopsis

According to European TEN-T guidelines, due consideration must be given to the risk assessments and adaptation measures during infrastructure planning, in order to improve resilience to disasters. SAFEWAY's aim is to design, validate and implement holistic methods, strategies, tools and technical interventions to significantly increase the resilience of inland transport infrastructure. SAFEWAY leads to significantly improved resilience of transport infrastructures, developing a holistic toolset with transversal application to anticipate and mitigate the effects extreme events at all modes of disaster cycle:

1. **"Preparation":** substantial improvement of risk prediction, monitoring and decision tools contributing to anticipate, prevent and prepare critical assets for the damage impacts;
2. **"Response and Recovery":** the incorporation of SAFEWAY IT solutions into emergency plans, and real-time optimal communication with operators and end users (via crowdsourcing and social media);
3. **"Mitigation":** improving precision in the adoption of mitigation actions (by impact analysis of different scenarios) together with new construction systems and materials, contributing to the resistance & absorption of the damage impact.

SAFEWAY consortium has 15 partners that cover multidisciplinary and multi-sectorial business fields associated with resilience of transport infrastructure in Europe: national transport infrastructure managers & operators, a main global infrastructure operator, partners able to provide various data sources with large coverage in real time, comprehensive ITC solutions, and leading experts in resilience, risk databases, remote sensing-based inspection, and decision systems based on predictive modelling.

SAFEWAY will carry-out 4 real case studies distributed through 4 countries, linked to 5 corridors of the TEN-T Core Network. SAFEWAY has as main expected impacts:

1. at least 20% improvement in mobility; and
2. at least 20% lower cost of infrastructure maintenance.

Document Information

Document Name	Data Management Plan (DMP) V2
Version No.	V1.0
Due date Annex I	29/02/2020
Report date	28/02/2020
Number of pages	86
Lead Author	Carlos Perez-Collazo (UVIGO)
Other Authors	Belén Riveiro (UVIGO) Vanesa Alarcón (Ayming)
Dissemination level	Public

Document History

Ver.	Date	Description	Authors	Checked by
0.1	15/12/2019	Creation of the document	C. Perez-Collazo	
0.2	22/01/2020	Content update with feedback from Ethics Mentor	C. Perez-Collazo	V. Alarcón
0.3	28/01/2020	Content update with feedback from Ethics Mentor	C. Perez-Collazo	V. Alarcón
0.4	06/02/2020	Updated datasets	C. Perez-Collazo	V. Alarcón
0.5	20/02/2020	Included feedback from EM	C. Perez-Collazo	V. Alarcón
0.6	24/02/2020	Quality Control	C. Perez-Collazo	PTC
0.7	26/02/2020	Crowd-sourced datasets added	C. Perez-Collazo	S. Bollars
1.0	27/02/2020	Final Quality Check	C. Perez-Collazo	V. Alarcón

Document Approval

Ver.	Name	Position in project	Beneficiary	Date	Visa
1.0	Dr. Belén Riveiro	Project Coordinator	UVIGO	27/02/2020	BR

Executive Summary

This document describes the second version of the Data Management Plan (DMP) for the SAFEWAY project. The DMP provides an analysis of the main elements of the data management policy that will be used throughout the SAFEWAY project by the project partners, with regard to all datasets that will be generated by the project. The documentation of this plan is a precursor to the WP1 Management. The format of the plan follows the Horizon 2020 template "Guidelines on Data Management in Horizon 2020"[1].

[1] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-datamgt_en.pdf

Table of Contents

Glossary of Terms

DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
E&BP	Exploitation and Business Plan
E&IM	Exploitation & Innovation Manager
EM	Ethics Mentor
GDPR	General Data Protection Regulation
GFS	Global Forecast System
GIS	Geographic Information System
IMS	Information Management System
INEA	Innovation and Networks Executive Agency
IPMA	Instituto Português do Mar e da Atmosfera
IPR	Intellectual Property Rights
MMS	Mobile Mapping System
PTC	Project Technical Committee
WP	Work Package

1. Introduction

The main aim of the Data Management Plan (DMP) is to serve as a guideline for SAFEWAY partners to address all issues related with data management.

Due to the importance of research data to support publications, it is necessary to define a data management policy. This document contains the second version of the project DMP where the different datasets to be produced by the SAFEWAY project identified in the previous version are reviewed to together with the proposed measures to management them. The document also includes the main exploitation perspectives for each of those datasets and major management principles the project will implement to handle those datasets. Finally, this updated version gives an overview on the monitoring of the different datasets.

Although the DMP is a Deliverable to be submitted in Month 6 (D.1.3), this is also a live document throughout the lifetime of the project. This initial version will evolve during the project according to the progress of project activities.

Table 1: Planed calendar for submission of the DMP and its updates

Deliverable Number	Deliverable Title	Due date
D1.3	Data Management Plan (DMP) V1	M6
D1.5	**Data Management Plan (DMP) V2**	**M18**
D1.7	Data Management Plan (DMP) V3	M30
D1.9	Data Management Plan (DMP) V4	M42

The DMP will cover the complete data life cycle as shown in Figure 1.

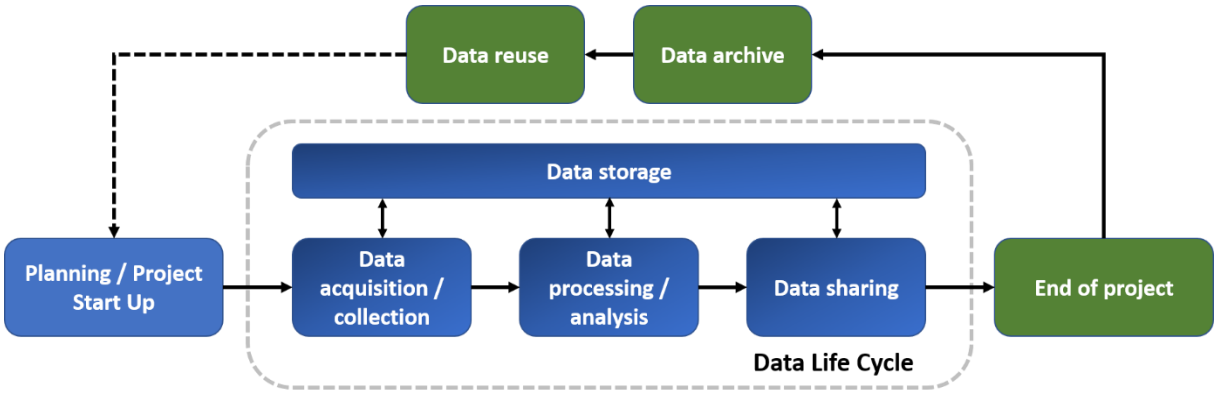

Figure 1. Data life cycle

1.1 Updates to DMP included in this version

This second version of the DMP includes the following updates:

- Section 2.5 on Data Security has been updated, in particular safety measures 5 and 9 have been better defined.
- An additional dataset on Stakeholders Feedback has been added to sections 3 and 4.
- An additional dataset on crowd-sourced data has been added to sections 3 and 4.
- SAFEWAY datasets tables have been updated.
- An outlook towards the expected content to be included in version 3 of this report has been included in section 5.
- The ethical aspects of the project, including an up-to-date report from the Ethics Mentor has been included in Section 6.
- Appendix 1 and Appendix 2 were updated to reflect the changes introduced to D11.2 in M16, to reflect the change in UVIGO's Data Protection Officer (DPO).
- Appendix 3 has been added to include some guidelines for partners to follow when elaborating a survey.
- Appendix 4 has been added to include a guidance document, for partners, on interoperability and exchange of data.

2. General Principles

2.1 Pilot on Open Research Data

The SAFEWAY Project is fully aware of the open access to scientific publications article (Article 29.2 of the H2020 Grant Agreement), as well as to the open access to research data article (Article 29.3 of the H2020 Grant Agreement). However, project partners have opted to be out of the Open Research Data due to a possible conflict with protecting results; SAFEWAY results will be close to market and results' disclosures should be taken with care and always considering exploitation/commercialization possibilities.

2.2 IPR management and security

The SAFEWAY project strategy for knowledge management and protection considers a complete range of elements leading to the optimal visibility of the project and its results, increasing the likelihood of market uptake of the provided solution and ensuring a smooth handling of the individual intellectual property rights of the involved partners in view or paving the way to knowledge transfer:

IPR protection and IPR strategy activities will be managed by Laura TORDERA from FERROVIAL (leader of WP10) as Innovation and Exploitation Manager with the support of the H2020 IPR Helpdesk. The overall IPR strategy of the project is to ensure that partners are free to benefit from their complementarities and to fully exploit their market position. Hence, the project has a policy of patenting where possible. An IPR Plan will be included in the Exploitation & Business Plans (D10.4).

Regarding Background IP (tangible and intangible input held by each partner prior to the project needed to the execution of the project and/or exploiting the results) it will be detailed in the Consortium Agreement, defining any royalty payments necessary for access to this IP. Regarding Foreground IP (results generated under the project) they will belong to the partner who has generated them. Each partner will take appropriate measures to properly manage ownership issues. When several beneficiaries had jointly carried out generating results and where their respective share of work cannot be ascertained, they will have joint ownership of such results. They will stablish an agreement regarding the allocation of terms of exercising the joint ownership, including definition of the conditions for grating licenses to third parties.

2.3 Allocation of resources

The Project Technical Committee (PTC) will be responsible of collecting the knowledge generated and defining protection strategy and the necessary access rights for results exploitation, as well as propose fair solutions to any possible conflict related to IPR. Complementarily, the PTC through the Exploitation & Innovation Manager (E&IM) will keep a permanent surveillance activity on the blocking IP or new IP generated elsewhere in the EU landscape to ensure SAFEWAY freedom to operate. The output of this activity will be included in the Exploitation and Business Plan (E&BP), which will be updated during the project time frame.

2.4 Personal data protection

For some of the activities to be carried out by the project, it may be necessary to collect basic personal data (e.g. full name, contact details, background), even though the project will avoid collecting such data unless deemed necessary.

Such data will be protected in compliance with the EU's General Data Protection Regulation, Regulation (EU) 2016/679. National legislations applicable to the project will also be strictly followed.

All data collected by the project will be done after giving data subjects full details on the experiments to be conducted, and after obtaining signed informed consent forms. Such forms, provided in the previous deliverable D11.2 POPD – Requirement No 2, are also included in Appendix 1 of this document. Additionally, the overall information about procedures for data collection, processing, storage, retention and destruction were also provided in D11.2, which are annexed to the present DMP in Appendix 2.

2.5 Data security

SAFEWAY shall take the following technical and organizational security measures to protect personal data:

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of SAFEWAY's information security program.
2. Audit and risk assessment procedures for the purposes of periodic review, monitoring and maintaining compliance with SAFEWAY policies and procedures, and reporting the condition of its information security and compliance to senior internal management.
3. Maintain Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them.
4. Password controls designed to manage and control password strength, and usage including prohibiting users from sharing passwords.
5. Security and communication protocols, following Big Data analytics, will be developed as required. SAFEWAY solutions will anticipate security not only technically, but also regarding Data Protection Regulation 2016/679 changes in the Data Protection Regime as of May 2018. It is also recommended to consider any other security measures in an institutional, national or international way, like other guidelines or regulations – such as ISO 27002 and ISO 15713.
6. SAFEWAY solutions will not centralise all the native data in a common database, but instead will retrieve data with values for the platform functionalities on demand. The services layer of the platform includes communication application proceeding information disclosure.
7. Operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal.

8. Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to SAFEWAY technology and information assets.
9. Incident management procedures designed to investigate, respond to, mitigate and notify of events related to SAFEWAY technology and information assets, data protection incidents and procedure of notification to the authorities included.
10. Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
11. Data could wherever be processed in anonymised or pseudo-anonymised form.
12. Data will be processed ONLY if it is really adequate, relevant and limited to what is necessary for the research ('data minimisation principle').
    a) Personal data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
    b) The minimum amount of personal data necessary to fulfil the purpose of SAFEWAY will be identified.
    c) No more personal data than necessary for the purpose of SAFEWAY will be achieved and stored.
    d) Whenever it is necessary to process certain particular information about certain individuals, it will be collected only for those individuals.
    e) Personal data will not be collected if it could be useful in the future.

These guidelines will be of special application for INNOVACTORY and TØI CENTRE, the two project partners who have a more intensive role in the use of personal data. In the Deliverable D11.1-Ethics Requirements are annexed the exact treatment of the data made by these two entities.

2.6 Ethical aspects

An ethical approach will be adopted and maintained throughout the fieldwork process. The Ethics Mentor (appointed in D11.3 GEN Requirement 3) will assure that the EU standards regarding ethics and Data Management are fulfilled. Each partner will proceed with the survey according to the provisions of the national legislation that are adjusted according to the respective EU Directives for Data Management and ethics.

The consortium will ensure the participants' right to privacy and confidentiality of data in the surveys, by providing participants to the survey with the Informed Consent Procedures:

- for those participating in the surveys being carried out within Task 4.3, by the Institute of Transport Economics-Norwegian Center for Transport Research

These documents will be sent electronically and will provide information about how the answers will be used and what is the purpose of the survey. Participants will be assured that their answers, or personal data, will be used only for the purposes of the specific survey. The voluntary character of participation will be stated explicitly in the Consent Form.

As it is established in Deliverable D11.3, an Ethics Mentor is appointed to advise the project participants on ethics issues relevant to protection of personal data.

The Ethics Mentor will advise and supervise the following aspects of the Project:

- Data protection by design and default. The Project will require data control to implement appropriate technical and organisational measures to give effect to the GDPR's core data-protection principles.
- Informed consent to data processing. Whenever any personal data is collected directly from research participants, their informed consent will be sought by means of a procedure that meets the standards of the GDPR.
- Use of previously collected data ('secondary use'). If personal data is processed in the Project without the express consent of the data subjects, it will be explained how those data are obtained, and their use in the Project will be justified.
- Data protection processors. If there is any Data Processor who works with information that belongs to the responsible, a Data Processor agreement shall be formalised.
- Data protection impact assessments (DPIA). If the Project involves operations likely to result in a high risk to the rights and freedoms of natural persons, this document will be conducted.
- Profiling, tracking, surveillance, automated decision-making and big data. If the Project involves these techniques, a detailed analysis will be provided of the ethics issues raised by this methodology. It will comprise an overview of all planned data collection and processing operations; identification and analysis of the ethics issues that these raise, and an explanation of how these issues will be addressed to mitigate them in practice.
- Data security. Both ethical and legal measures will be conducted to ensure that participants' information is properly protected. These may include the pseudo-anonymization and encryption of personal data, as well as policies and procedures to ensure the confidentiality, integrity, availability and resilience of processing systems
- Deletion and archiving of data. Finally, the collected personal data will be kept only as long as it is necessary for the purposes for which they were collected, or in accordance with the established auditing, archiving or retention provisions for the Project. These must be explained to your research participants in accordance with informed consent procedures.
- Best practices Code. It is recommended to implement a code where data protection best practices are informed and fully explained. This document may be personalised depending on type of employee or partner is working with this information. Also may be described if employee, freelance or partner can work with personal devices or not (Bring your own device Policies) when working with this information.

3. Data Set Description

SAFEWAY is committed to adopt whenever possible the FAIR principles for research data; this is, data should be findable, accessible, interoperable and re-usable.

SAFEWAY partners have identified the datasets that will be produced during the different phases of the project. The list is provided below, while the nature and details for each dataset are given in Section 4.

This list is indicative and allowing an estimation of the data that SAFEWAY will produce – it may be adapted (addition/removal of datasets) in the next versions of the DMP to take into consideration the project developments.

Table 2: SAFEWAY Dataset overview

No	Dataset name	Responsible partner	Related Task
1	Mobile Mapping System (MMS) data	UVIGO	T3.2
2	Historic weather dataset	UVIGO	T3.1 & T3.3
3	Global Forecast System (GFS) data	UVIGO	T3.1 & T3.3
4	Satellite data	PNK	T3.2
5	Experts interviews	TØI	T4.3
6	Data on risk tolerance	TØI	T4.3
7	Sociotechnical system analysis	TØI	T4.3
8	Infrastructure assets data	UMINHO	T5.1
9	Information on the value system	IMC	T6.1
10	Stakeholder contacts collection	UVIGO	WP10
11	Dissemination events data	UVIGO	T10.3
12	Stakeholder feedback	UVIGO	WP10
13	Crowd-sourced data	INNOVACTORY	T4.1 & T5.1

Table 3: Datasets description and purpose

No	Dataset name	Description	Purpose	Legitimation
1	MMS data	Data from the different sensors equipped in the Mobile Mapping System (MMS) employed for the monitoring of the infrastructures, including data from some or all the following sources: LiDAR sensors, RGB cameras, thermographic cameras, and Ground Penetrating Radar.	Inspection of the infrastructure critical assets to quantify condition. From this data, the input information for predictive models (WP5) and SAFEWAY IMS (WP7) will be extracted.	No personal data collected. No needed any informed consent or accept any policies in this sense.
2	Historic weather dataset	Observational quantitative meteorological data measured with hourly (or less) temporal frequency over the Instituto Português do Mar e da Atmosfera (IPMA) weather stations network. Relevant variables are air temperature, atmospheric pressure, wind speed and direction, maximum wind gusts speed and direction, relative air humidity, instant rain and solar radiation.	Main source of observational info for meteorological data interpolation and short-term prediction systems. Base dataset for meteorological activities on WP3.	No personal data collected. No needed any informed consent or accept any policies in this sense.
3	Global Forecast System (GFS) data	Predictive quantitative meteorological data calculated with hourly temporal frequency over a planetary-wide ~11 km horizontal spatial resolution by the National Oceanic and Atmospheric Administration Global Forecast System (GFS) numerical model. Relevant variables are those most analogous to the Historic weather dataset ones.	Complementary source of observational info for meteorological data interpolation and short-term prediction systems. Used on the same way than the Historic weather dataset.	No personal data collected. No needed any informed consent or accept any policies in this sense.

No	Dataset name	Description	Purpose	Legitimation
4	Satellite data	Sentinel-1 satellite imagery from Copernicus Open Access Hub, to optimize the Rethicus® displacement service based on MTInSAR algorithms.	Geospatial information acquired from satellite are key to detect and quantify terrain displacement and deformation (e.g. landslides, subsidence, etc.)	No personal data collected. No needed any informed consent or accept any policies in this sense.
5	Experts interviews	The data contain transcriptions and notes from expert interviews with researchers and policy makers. They will be either conducted personally, on the phone (or skype) or they can also be conducted in written form. Include findings from completed/ongoing EU projects	The aim is to identify and collect sources of knowledge on how the different users think/act in extreme situations, as well as their level of preparedness and risk tolerance, and identify case studies for analysis of risk tolerance	No personal data collected. No needed any informed consent or accept any policies in this sense.
6	Data on risk tolerance	This includes the evaluation of risk tolerance of different actors and scheduling for use in focus groups, and follow-up surveys with different user representatives.	To make findings on varying levels of risk tolerance and preparedness for a range of short- and long-term extreme events, among the user groups	No personal data collected. No needed any informed consent or accept any policies in this sense.
7	Sociotechnical system analysis	Selected cases will be documented to represent a range of event types occurring in Europe. Interviews and template analysis will be conducted with people both managing and caught up in the extreme events studied.	These analyses along with established sociotechnical system principles will inform on optimal social and technical arrangements for IMS.	No personal data collected. No needed any informed consent or accept any policies in this sense.

No	Dataset name	Description	Purpose	Legitimation
8	Infrastructure assets data	Database of infrastructures with identification, conservation state, inspections and structural detailing	Databased needed to define the input data to the development of predictive models.	No personal data collected. No needed any informed consent or accept any policies in this sense.
9	Information on the value system	The information on the value systems, decision making processes and key performance indicators that transportation infrastructure agencies and stakeholders within the project use in management of their assets.	The monetized direct and indirect consequences of inadequate infrastructure performance is needed as input to develop the value system that will allow to prioritize the intervention of stakeholders related to transport infrastructure.	Data is collected by the informed consent – following the model from appendix 1 where the project obtains the legitimation to process this data
10	Stakeholder contacts collection	The data contain information on the main stakeholders of SAFEWAY along the major stakeholder groups. They include infrastructure managers, operators, public administrations, researchers, practitioners, policy makers. The contact information that is collected includes the name, institutional affiliation, position, email address, phone number and office address.	The collection will be used for contacting the respondents for the validation of the project outcomes. It also provides the basis for the dissemination of the project and for promoting the SAFEWAY IT solutions.	Data is collected by the informed consent – following the model from appendix 1 where the project obtains the legitimation to process this data

No	Dataset name	Description	Purpose	Legitimation
11	Workshops data	The data contain protocols, written notes and summaries that were done at the three workshops, which are organized in different countries. The workshops aim at developers and providers of technical solutions. This dataset also includes the collection of contact information of attendees that includes the name, institutional affiliation, position, email address, phone number and office address.	The information gathered at the workshops will support the development of the SAFEWAY methodologies and tools.	Data is collected by the informed consent – following the model from appendix 1 where the project obtains the legitimation to process this data
12	Stakeholders feedback	Dataset containing responses from key stakeholders and Advisory Board members to different technical feedback surveys that will be produced during the project to gather feedback about the technical implementation of the project.	The information gathered though the surveys will support the development of the SAFEWAY methodologies and tools, The information will also contribute to quantify SAFEWAY's impact.	Data is collected by the informed consent – following the model from appendix 1 where the project obtains the legitimation to process this data
13	Crowd-sourced data	Flow and incident data from TomTom. TomTom will collect this data by merging multiple data sources, including anonymized measurement data from over 550 million GPS-enabled devices.	Databased needed to define the input data to the development of predictive models.	No personal data received from TomTom, No needed any informed consent or accept any policies in this sense.

4. SAFEWAY Datasets

4.1 Dataset No 1: MMS data

Mobile Mapping System (MMS) data	
Data identification	
Dataset description	This dataset comprises all the data collected by the mapping technologies proposed by UVIGO in WP3. Therefore, it contains data from the different sensors equipped in the Mobile Mapping System (MMS) employed for the monitoring of the infrastructures, including data from some or all the following sources: LiDAR sensors, RGB cameras, thermographic cameras, and Ground Penetrating Radar. Data from different LiDAR sensors (Terrestrial or Aerial) that may be employed for the fulfilment of the different monitoring tasks will be comprised in this dataset as well.
Source	Sensor data gathered from the Mobile Mapping System (MMS) owned by UVIGO.
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	UVIGO; N/A
Partner in charge of the data collection	UVIGO
Partner in charge of the data analysis	UVIGO
Partner in charge of the data storage	UVIGO
Related WP(s) and task(s)	WP3: -Task 3.1 (Data acquisition). -Task 3.2 (Data pre-processing). -Task 3.3 (Data processing and automation of monitoring)

Mobile Mapping System (MMS) data	
Standards	
Info about metadata (production and storage dates, places) and documentation?	Point cloud data from LiDAR sensors will be produced in real time when the monitoring of the infrastructures is carried out. The metadata of that information, stored in '.las' format, has its documentation in http://www.asprs.org/wp-content/uploads/2019/03/LAS_1_4_r14.pdf Imagery will be produced together with the point cloud data, and the metadata will have the specifications of the correspondent image file format.
Standards, format, estimated volume of data	Data recorded from the different sensors of the MMS dataset will be stored in standard formats: - Point cloud data obtained from the LiDAR sensors will be stored either in standard binarized format (.las) or (less likely) as plain text (.txt). - Imagery will be stored in standard image file formats (.jpg, .tiff…)
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	The recorded data will be used for the monitoring of the infrastructures within the case studies of the project. The raw data acquired by the set of sensors equipped in the monitoring system will be processed to extract meaningful information about the infrastructure that can feed different attributes of the Infrastructure Information Model that is being developed in Task 3.3, and also for three-dimensional visualization of the monitored infrastructure.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Only the partner in charge of the data collection will have access to the raw data of the dataset. The results of the data processing tasks (mainly attribute fields required by the Infrastructure Information Model) will be shared with other members as they will be integrated into the SAFEWAY database. Any relevant three-dimensional visualization of the data could be made public for presenting final results.

Mobile Mapping System (MMS) data	
Data sharing, re-use, distribution, publication (How?)	Data sharing and re-use at the end of the project will be subjected to the permission of the infrastructure owners. Nevertheless, data will be available for research purposes (development of future data processing algorithms) provided that datasets are fully anonymized in such a way they cannot be associated to real structures.
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	Data collected from this dataset will not intentionally include any personal data. In the event of an identifiable individual within the imagery part of the dataset, these data will be pre-processed to ensure that it is anonymised or pseudo-anonymised. Particularly, the imagery is being pre-processed before being available for the project. The pre-processing consists of applying an algorithm that detects and blurs faces and car plates to images before being available for further analysis.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in secured servers of the partner in charge of the dataset, where only research members will be granted access to the information within the dataset. The Consortium will take into account that for the purposes of the SAFEWAY project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues this will be 5 years.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017. In this particular case the Spanish national public administration's guidelines on electronic dada destruction will be considered.

4.2 Dataset No 2: Historic weather dataset

Historic weather dataset	
Data identification	
Dataset description	IPMA's Portugal Weather Dataset.
Source	Instituto Português do Mar e da Atmosfera. Web: http://www.ipma.pt/pt/index.html
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	IPMA.
Partner in charge of the data collection	IP.
Partner in charge of the data analysis	UVIGO.
Partner in charge of the data storage	UVIGO.
Related WP(s) and task(s)	WP3, tasks 3.1, 3.3.
Standards	
Info about metadata (production and storage dates, places) and documentation?	Observation weather data is continuously generated by the automated meteorological stations belonging to the IPMA's network with a 1 hour (or 10 minutes) frequency. IPMA will provide a subset of such data, limited to the requested variables, for the considered stations and timespan.
Standards, format, estimated volume of data	JSON, XML or SQL formats for storing meteorological data. Hour-interval numeric values for each of the 9 required meteorological variables (air temperature, atmospheric pressure, wind speed and direction, maximum wind gusts speed and direction, relative air humidity, instant rain and solar radiation), for each of the provided observation weather stations (number between 30 and 100), during the Portuguese meteorological case study time lapse.

Historic weather dataset	
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	Input for interpolation and short-term prediction algorithms used in WP3.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Confidential.
Data sharing, re-use, distribution, publication (How?)	Collected data will potentially be used in future scientific research papers.
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	No personal data.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be permanently stored in UVIGO computer facilities for the duration of the SAFEWAY project.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data will be stored indefinitely, with no planned destruction.

4.3 Dataset No 3: GFS data

Global Forecast System (GFS) data	
Data identification	
Dataset description	GFS Portugal Weather Dataset.
Source	National Oceanic and Atmospheric Administration's Global Forecast System weather forecast model. Web: https://www.ncdc.noaa.gov/data-access/model-data/model-datasets/global-forcast-system-gfs
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	NOAA.
Partner in charge of the data collection	UVIGO.
Partner in charge of the data analysis	UVIGO.
Partner in charge of the data storage	UVIGO.
Related WP(s) and task(s)	WP3, tasks 3.1, 3.3.
Standards	
Info about metadata (production and storage dates, places) and documentation?	Forecast weather data is generated during the 4 cycle daily executions of the GFS model, with an hourly temporal resolution, for a global grid with ~11 km horizontal spatial resolution. UVIGO will gather a subset of such data, limited to the requested variables, for the considered geographic area and timespan.
Standards, format, estimated volume of data	SQL formats for storing meteorological data. Hour-interval numeric values for each of the 9 required meteorological variables (air temperature, atmospheric pressure, wind speed and direction, maximum wind gusts speed and direction, relative air humidity, instant rain and solar radiation), for each of the considered grid points (number 1000-2000) during the Portuguese meteorological case study time lapse.

Global Forecast System (GFS) data	
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	Input for interpolation and short-term prediction algorithms used in WP3.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Confidential.
Data sharing, re-use, distribution, publication (How?)	Collected data will potentially be used in future scientific research papers.
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	No personal data.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be permanently stored in UVIGO computer facilities for the duration of the SAFEWAY project.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data will be stored indefinitely, with no planned destruction.

4.4 Dataset No 4: Satellite data

Satellite data	
Data identification	
Dataset description	Sentinel-1 images
Source	Copernicus Open Access Hub
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	Any **Sentinel data** available through the Sentinel Data Hub will be governed by the Legal Notice on the use of Copernicus Sentinel Data and Service Information.
Partner in charge of the data collection	Planetek Italia
Partner in charge of the data analysis	Planetek Italia
Partner in charge of the data storage	Planetek Italia
Related WP(s) and task(s)	WP3 – Displacement monitoring of infrastructures (roads and railways)
Standards	
Info about metadata (production and storage dates, places) and documentation?	The metadata information are stored within a product.xml file
Standards, format, estimated volume of data	OGC standard format. Volume: about TB.
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	The Sentinel-1 images will be exploited using the Multi-Temporal Interferometry algorithm through the Rheticus® platform.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Confidential

Satellite data	
Data sharing, re-use, distribution, publication (How?)	Access through the Rheticus ® platform protected by Username and Password.
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	No personal data
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	The data will be stored within the cloud service platform Rheticus® owned by Planetek Italia for the entire duration of the project.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	The data will be deleted in the cloud platform Rheticus® five years after the end of the project.

4.5 Dataset No 5: Experts interviews

EXPERTS INTERVIEWS	
Data identification	
Dataset description	The data contain transcriptions and notes from expert interviews with researchers and policy makers. They will be either conducted personally, on the phone (or skype) or they can also be conducted in written form. Include findings from completed/ongoing EU projects
Source	Interviews with experts
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	N/A
Partner in charge of the data collection	TØI
Partner in charge of the data analysis	TØI
Partner in charge of the data storage	TØI
Related WP(s) and task(s)	WP4 and 6
Standards	
Info about metadata (production and storage dates, places) and documentation?	Production August 2019, anonymised data stored on secure server
Standards, format, estimated volume of data	Word documents
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	Gather state-of-the-art knowledge on risk tolerance, aspects of psychology and behaviour of different user groups.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Confidential

EXPERTS INTERVIEWS	
Data sharing, re-use, distribution, publication (How?)	Scientific articles
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	Informed Consent Forms are defined in Appendix 1.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in secured servers of the partner in charge of the dataset, where only research members will be granted access to the information within the dataset. The Consortium will take into account that for the purposes of the SAFEWAY project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues this will be 5 years.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017.

4.6 Dataset No 6: Data on risk tolerance

DATA ON RISK TOLERANCE	
Data identification	
Dataset description	This includes the evaluation of risk tolerance of different actors and scheduling for use in focus groups, and follow-up surveys with different user representatives.
Source	Focus groups and surveys
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	TØI
Partner in charge of the data collection	TØI
Partner in charge of the data analysis	TØI
Partner in charge of the data storage	TØI
Related WP(s) and task(s)	WP4, 6
Standards	
Info about metadata (production and storage dates, places) and documentation?	Production circa Jan 2020, anonymised data stored on secure server
Standards, format, estimated volume of data	Word documents
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	Gather knowledge on risk tolerance, aspects of psychology and behaviour of different user groups.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Confidential

DATA ON RISK TOLERANCE	
Data sharing, re-use, distribution, publication (How?)	Scientific articles
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	Consent will be gathered following templates in Appendix 1 and Appendix 2.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in secured servers of the partner in charge of the dataset, where only research members will be granted access to the information within the dataset. The Consortium will take into account that for the purposes of the SAFEWAY project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues this will be 5 years.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017.

4.7 Dataset No 7: Sociotechnical system analysis

SOCIOTECHNICAL SYSTEM ANALYSIS	
Data identification	
Dataset description	Selected cases will be documented to represent a range of event types occurring in Europe. Interviews and template analysis will be conducted with people both managing and caught up in the extreme events studied.
Source	Document analyses
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	TØI
Partner in charge of the data collection	TØI
Partner in charge of the data analysis	TØI
Partner in charge of the data storage	TØI
Related WP(s) and task(s)	WP4 and 6
Standards	
Info about metadata (production and storage dates, places) and documentation?	Production circa June 2020, anonymised data stored on secure server
Standards, format, estimated volume of data	Word documents
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	Gather knowledge on risk tolerance, aspects of psychology and behaviour of different user groups.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Confidential

SOCIOTECHNICAL SYSTEM ANALYSIS	
Data sharing, re-use, distribution, publication (How?)	Scientific articles, report
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	N/A
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in secured servers of the partner in charge of the dataset, where only research members will be granted access to the information within the dataset. The Consortium will take into account that for the purposes of the SAFEWAY project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues this will be 5 years.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017.

4.8 Dataset No 8: Infrastructure assets data

INFRASTRUCTURE ASSETS DATA	
Data identification	
Dataset description	Database of infrastructures with identification, conservation state, inspections and structural detailing
Source	Infraestruturas de Portugal; Ferrovial; Network Rails
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	Infraestruturas de Portugal; Ferrovial; Network Rails
Partner in charge of the data collection	University of Minho; University of Cambridge; Infrastructure Management Consultants Gmbh
Partner in charge of the data analysis	University of Minho; University of Cambridge; Infrastructure Management Consultants Gmbh
Partner in charge of the data storage	University of Minho
Related WP(s) and task(s)	WP5 – Task 5.1
Standards	
Info about metadata (production and storage dates, places) and documentation?	N/A
Standards, format, estimated volume of data	Tables (.xls format) and georeferenced maps (.klm format)
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	Development of predictive models for projecting risks of future infrastructure damage, shutdown and deterioration. Based on the database, and analytical and stochastic/probabilistic approaches, the most suitable models for risk and impact projections will be selected.

INFRASTRUCTURE ASSETS DATA	
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Confidential
Data sharing, re-use, distribution, publication (How?)	Database is to be used by members of the Consortium and the derived results are to be reviewed by the partner owner of data prior to publication
Embargo periods (if any)	Not applicable.
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	There is no personal data
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in a physical external disk for storage during the duration of the project. A copy will also be accessible on a restricted online server for the partners involved in Task 5.1.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data will be retained five years after the project ends. Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017.

4.9 Dataset No 9: Information on the value systems

INFORMATION ON THE VALUE SYSTEM	
Data identification	
Dataset description	The information on the value systems, decision making processes and key performance indicators that transportation infrastructure agencies and stakeholders within the project use in management of their assets. The contact information that is collected includes email addresses, names and affiliations.
Source	On-line survey developed on a freeware software platform.
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	IMC; N/A
Partner in charge of the data collection	IMC
Partner in charge of the data analysis	IMC
Partner in charge of the data storage	IMC
Related WP(s) and task(s)	WP6, Task 6.1
Standards	
Info about metadata (production and storage dates, places) and documentation?	None.
Standards, format, estimated volume of data	.xls (MS Excel format).
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	The data will be used in WP6 – for development of a robust decision support framework for short and medium to long-term maintenance planning.

INFORMATION ON THE VALUE SYSTEM	
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Currently confidential. Perhaps public after the project completion.
Data sharing, re-use, distribution, publication (How?)	See under data access policy.
Embargo periods (if any)	See under data access policy.
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	Yes, there are. It is planned to include related consent as a part of the survey, so subjects may comply. This will be done considering the templates from Appendix 1 and 2.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in secured servers of the partner in charge of the dataset, where only research members will be granted access to the information within the dataset. The Consortium will take into account that for the purposes of the SAFEWAY project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues this will be 5 years.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017.

4.10 Dataset No 10: Stakeholders contact collection

STAKEHOLDERS CONTACT COLLECTION	
Data identification	
Dataset description	The data contain information on the main stakeholders of SAFEWAY along the major stakeholder groups. They include infrastructure managers, operators, public administrations, researchers, practitioners, policy makers. The contact information that is collected includes the name, institutional affiliation, position, email address, phone number and office address.
Source	Archives of SAFEWAY partners.
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	UVIGO; N/A
Partner in charge of the data collection	UVIGO
Partner in charge of the data analysis	UVIGO
Partner in charge of the data storage	UVIGO
Related WP(s) and task(s)	WP10: -Task 10.1 (Dissemination, communication and IP management). -Task 10.2 (Standardization activities) -Task 10.3 (Technology transfer activities) -Task 10.4 (Collaboration and clustering)
Standards	
Info about metadata (production and storage dates, places) and documentation?	N/A
Standards, format, estimated volume of data	This dataset can be imported from, and exported to a CSV, TXT or Excel file.

STAKEHOLDERS CONTACT COLLECTION	
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	This dataset is only used to disseminate the results obtained through SAFEWAY project.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	As this dataset can contain personal data, only the partner in charge of the data collection will have access to the raw data. Data that is publicly available will be share among consortium partners.
Data sharing, re-use, distribution, publication (How?)	None
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	This dataset can include some personal data. Before collecting any personal data that is not publicly available, informed consents from subjects will be gained. Consent will be gathered following the template from Appendix 1.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in secured servers of the partner in charge of the dataset, where only research members will be granted access to the information within the dataset. The Consortium will take into account that for the purposes of the SAFEWAY project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues this will be 5 years.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017. In this particular case the Spanish national public administration's guidelines on electronic dada destruction will be considered.

4.11 Dataset No 11: Dissemination events data

Dissemination events Data	
Data identification	
Dataset description	The dataset contains the contact information of attendees to events organised by SAFEWAY (SAFEWAY workshop, Parallel Events, SAFEWAY Webcast), provided during their registration to the event. The collected contact information, may include: name, institutional affiliation, position, email address, phone number and office address. In addition a voluntary survey will be circulated at the end of the event to collect the feedback from the attendees in order to continuously increase quality.
Source	Archives of SAFEWAY partners.
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	UVIGO; N/A
Partner in charge of the data collection	UVIGO
Partner in charge of the data analysis	UVIGO
Partner in charge of the data storage	UVIGO
Related WP(s) and task(s)	WP10: -Task 10.3 (Technology transfer activities)
Standards	
Info about metadata (production and storage dates, places) and documentation?	N/A
Standards, format, estimated volume of data	This dataset can be imported from, and exported to a CSV, TXT or Excel file.

Dissemination events Data	
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	This dataset is only used for dissemination of the results obtained through SAFEWAY project.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	As this dataset can contain personal data, only the partner in charge of the data collection will have access to the raw data. Data that is publicly available will be shared among consortium partners.
Data sharing, re-use, distribution, publication (How?)	None
Embargo periods (if any)	N/A
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	This dataset can include some personal data. Before collecting any personal data that is not publicly available, informed consents from subjects will be gained. Consent will be gathered following the template from Appendix 1.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in secured servers of the partner in charge of the dataset, where only research members will be granted access to the information within the dataset. The Consortium will take into account that for the purposes of the SAFEWAY project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues this will be 5 years.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017. In this particular case the Spanish national public administration's guidelines on electronic dada destruction will be considered.

4.12 Dataset No 12: Stakeholders feedback

STAKEHOLDERS FEEDBACK	
Data identification	
Dataset description	Dataset containing responses from key stakeholders and Advisory Board members to different technical feedback surveys that will be produced during the project to gather feedback about the technical implementation of the project.
Source	A set of on-line surveys developed on a freeware software platform.
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	UVIGO; N/A
Partner in charge of the data collection	UVIGO
Partner in charge of the data analysis	UVIGO
Partner in charge of the data storage	UVIGO
Related WP(s) and task(s)	WP10
Standards	
Info about metadata (production and storage dates, places) and documentation?	N/A
Standards, format, estimated volume of data	This dataset can be imported from, and exported to a CSV, TXT or Excel file.
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	The information gathered though the surveys will support the development of the SAFEWAY methodologies and tools. The information will also contribute to quantify SAFEWAY's impact.

STAKEHOLDERS FEEDBACK	
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	Confidential
Data sharing, re-use, distribution, publication (How?)	Database is to be used by members of the Consortium and the derived results are to be reviewed by the partner owner of data prior to publication
Embargo periods (if any)	Not applicable.
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	Surveys will be anonymised or when not possible pseudo- anonymised. Only restricted project personnel have access to the raw survey data. When transferred to the ".XMS" (MS Excel) database, personal data (in case these exists) will be omitted. Consent will be gathered following the template from Appendix 1.
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Data will be stored in secured servers of the partner in charge of the dataset, where only research members will be granted access to the information within the dataset. The Consortium will take into account that for the purposes of the SAFEWAY project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues this will be 5 years.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	Data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation, and international standards such as ISO 27002:2017. In this particular case the Spanish national public administration's guidelines on electronic dada destruction will be considered.

4.13 Dataset No 13: Crowd-sourced data

Crowd-sourced data	
Data identification	
Dataset description	TomTom Traffic Incidents delivers information on the current observed congestion and incidents on roads in all countries where we offer this service. Traffic 'incidents' in this context include traffic jams, road closures, lane closures, construction zones, and accidents. TomTom Traffic Flow delivers a detailed view of the current observed speed and travel times on the entire road network in all countries where TomTom Traffic is available. This product is designed for easy integration into routing engines to calculate precise travel times.
Source	Real-time traffic products are created by merging multiple data sources, including anonymized measurement data from over 550 million GPS-enabled devices. Using highly granular data, gathered on nearly every stretch of road, we can calculate travel times and speeds continuously.
Partners activities and responsibilities	
Partner owner of the data; copyright holder (if applicable)	Innovactory; TomTom
Partner in charge of the data collection	Innovactory
Partner in charge of the data analysis	N/A
Partner in charge of the data storage	N/A
Related WP(s) and task(s)	WP4 task T4.1 WP5 task T5.1
Standards	
Info about metadata (production and storage dates, places) and documentation?	https://developer.tomtom.com/traffic-api/traffic-api-documentation-traffic-flow/flow-segment-data

Crowd-sourced data	
Standards, format, estimated volume of data	Traffic Incidents via TPEG2-TEC / Traffic Flow via TPEG2-TFP as well as OpenLR to deliver reports that describe incidents or congestion on any road, on any map. DATEX II is an industry standard for information exchange between service providers, application developers and traffic management centers.
Data exploitation and sharing	
Data exploitation (purpose/use of the data analysis)	The data will be used in WP4 and WP5 and can only be used in the setting of SAFEWAY under the conditions Innovactory agreed with TomTom. Data for later use are available but under different commercial agreements.
Data access policy / Dissemination level: confidential (only for members of the Consortium and the Commission Services) or Public	No personal data are supplied, Privacy data which are collected by TomTom will be within 24 hours automatically and irreversibly destroyed at TomTom side. Data that would allow TomTom to identify users from their location data are destroyed. Innovactory only receives the merged incident and flow data which are supplied to Safeway.
Data sharing, re-use, distribution, publication (How?)	Only for SAFEWAY demo purpose.
Embargo periods (if any)	None
Personal data protection: are there personal data? If so, have you gained (written) consent from data subjects to collect this information?	Data provided by TomTom to Innovactory do not contain any personal data and it has been made sure that the information contained in data cannot allow to the identifications of any person or personal data. In order to ensure personal data protection, a continuous monitoring approach will be followed. In this sense, the personal data protection systems/procedures implemented by TomTom will be reviewed, every six months, to detect any posible changes.

Crowd-sourced data	
Archiving and preservation (including storage and backup)	
Data storage (including backup): Where? For how long?	Innovactory does not store flow or incident data.
Data destruction. How is data destruction handled? Compliance with EU / national legislation.	If there is a need for buffering the incident/flow data, this data destruction will be carried out following the partner's guidelines on data destruction, which will always comply with EU and national legislation. Innovactory is implementing currently ISO 27001 (target finished Q2 2020).

5. Outlook Towards Next DMP

As stated in Table 1 of the Introduction, the next iteration of the DMP will be prepared in month 30 of the project, just after WPs 3, 4 and 5 will finish. Also, every other work package (apart from WP2 which ends in M18) and their tasks will be underway. Most of the data included in the dataset described in this document will either being under collection or have been collected Therefore, the upcoming DMP will provide an update regarding the status of each one of the dataset and the planned work until the expected action until the end of the project. Furthermore, in case additional datasets are identified as necessary for the completion of the project, this will be reported in the upcoming version of the DMP. For this purpose, and to ease the identification of possible needs to ensure personal data protection, a guidance document has been produced (Appendix 4) for partners to consult, and identify (if is the case) potential additional datasets.

6. Update of the Ethical Aspects

At this stage of the project, two are the main ethical aspects to review. In first place the outcome of the continuous monitoring process on ethical aspects, in particular regarding vehicle data crowdsourcing and interviews or surveys carried out during the development of WP4. Then, the report of the Ethics Mentor.

6.1 Ongoing monitoring

The ongoing monitoring regarding SAFEWAY ethical aspects has been focused, at a first stage, in identifying those tasks with relevance for data protection within the different activities of the project. It was concluded that the data protection risk posed by SAFEWAY is fairly limited, as the only task that might involve personal data collection is related to dissemination activities in workshops and meetings (see Sections 4.10 and 4.11), and an explicit and verifiable consent will be obtained prior to any data collection, as required by the GDPR. Furthermore, procedures for collection, processing, storage, retention and destruction of data have been defined to ensure its compliance with the legislative framework (see tables in Section 4). In addition, for those activities that require it (interviews and surveys) an informed consent form, together with an information sheet about the research study, were defined (see Appendices 1 and 2). In addition, any website or online based form, used for surveys, or for people to register to attend dissemination events or meetings, would require for the person filling it to accept a Privacy Policy that also complies with the GDPR requirements, such as the one contained in Appendix 2 or in the link (https://www.safeway-project.eu/en/personal-data).

6.2 Report of the Ethics Mentor

The Appointed Ethics Mentor (EM) for SAFEWAY is Ms Vanesa Alarcón Caparrós (see deliverable D11.3). Following are summarised the tasks carried out by the EM until the submission of this deliverable:

- The EM has reviewed documents linked to the project that could contain any personal data treatment, situations or other documents, where SAFEWAY Partners have had any doubt, or where these may represent any data treatment or risks. Following the review, the EM has always indicated the corresponding measures or recommendations for partners to take. As a result, for example, Appendix 2 has been updated several times. Last version is attached in this DMP.
- The EM has kept a continuous monitoring where the project in any of its different phases - as mentioned in section 3 - is collecting or doing any personal data treatment. In this sense it has been detected that large amount of data has been or will be collected by the project, however, the majority of this data do not contain personal information.
- The EM has delivered a guidance to avoid future risks in data treatment (see Appendix 3). The guidance describes several advices and recommendations for partners when preparing surveys during the project, in order to identify if there are data that cannot be collected. Furthermore, the guidance also

proposes ways to collect these data, such as online or physical forms (an informed consent on data treatment must be collected always that personal data are considered, however, the ways to collect it differs depending on the format on how the information is collected). See details in Appendix 3.

- The EM has provided a questionnaire (see Appendix 4) about the interoperation and exchange of data, in order to detect if there is any potential risk regarding to personal data treatment, when the project is collecting information.
- The EM has recommended to establish a procedure for data destruction, not only to delete personal information but also confidential information (see section 4).
- The EM has recommended to prepare a Code of Best Practices for employees, partners and freelances when working with personal information. It must be personalised for this type of professionals because every professional could be affected in different ways. In particular, it is recommended to establish a Bring Your Own Device policy when needed.
- The EM has suggested, for technical implementation of data management and destruction, to follow the instructions of ISO 27002:2017 or similar procedures validated in the market.
- The EM has provided feedback to the present version of the Data Management Plan. In particular, regarding the introduction of some corrections and to add some fields to consider more aspects connected with personal data treatments.

The EM has been in close contact with the coordinator (UVIGO) via direct mail, phone and regular meeting and has had access to all the information about the activities of the project that could imply ethically relevant aspects via email and accessing the common repository of SAFEWAY. Following are described the expected actions to be carried out by the EM in the upcoming month.

- The DMP will be updated in months 30 and 42, as indicated in Section 1. As part of this update the status of each dataset must considered, however, SAFEWAY Partners must be conscious on any possible doubts regarding data treatment, in which case these doubts will be addressed to the EM. In this sense and in compliance with proactivity principle established in European regulation a communication must be sent by the coordinators of the project informing the partners about this obligation.
- The EM will schedule regular meetings with the Coordinator, every six months until month 42, to check if there are doubts or any situation that must be considered or reviewed by the EM.
- The EM will be available to attend formal project meetings remotely or in person, if required partners will notify it in advance by including the pertinent action/s in the meeting agenda.

Acknowledgements

This deliverable was carried out in the framework of the GIS-Based Infrastructure Management System for Optimized Response to Extreme Events of Terrestrial Transport Networks (SAFEWAY) project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 769255.

SAFEWAY

GIS-BASED INFRASTRUCTURE MANAGEMENT SYSTEM FOR OPTIMIZED RESPONSE TO EXTREME EVENTS OF TERRESTRIAL TRANSPORT NETWORKS

Grant Agreement No. 769255

Data Management Plan (DMP) V1 - Appendices

WP 1 Overall project coordination

Deliverable ID	**D1.3**
Deliverable name	**Data Management Plan (DMP) V1**
Lead partner	UVIGO
Contributors	DEMO, PNK, UMINHO, IMC

PUBLIC

Appendices Contents

Appendix 1. Informed Consent Form

SAFEWAY

GIS-Based Infrastructure Management System for Optimized Response to Extreme Events of Terrestrial Transport Networks

INFORMED CONSENT FORM

Project acronym	SAFEWAY
Project name	GIS-BASED INFRASTRUCTURE MANAGEMENT SYSTEM FOR OPTIMIZED RESPONSE TO EXTREME EVENTS OF TERRESTRIAL TRANSPORT NETWORKS
Grant Agreement no.	769255
Project type	Research and Innovation Action
Start date of the project	01/09/2018
Duration in months	42
This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 769255.	
Disclaimer: This document reflects only the views of the author(s). Neither the Innovation and Networks Executive Agency (INEA) nor the European Commission is in any way responsible for any use that may be made of the information it contains.	

SAFEWAY event:

Date: **Location:**

General Data Protection Regulation (GDPR) Compliance

Data that is collected and processed for the purposes of facilitating and administering SAFEWAY workshops and events is subjected to GDPR to the EU General Data Protection Regulation (GDPR) which became applicable from the 25th of May 2018. Please see the document "POPD SAFEWAY.pdf" for further guidance on our data management policies. To process your application, we require your consent to the following (please check each box as appropriate).

Please circle as necessary		
I give my consent for all personal information provided by registering to the SAFEWAY (*workshop/event name*) to be stored and processed by relevant SAFEWAY project partners for Data Management Purposes.	**Yes**	**No**
I give my consent for all personal information provided by registering to the SAFEWAY (*workshop/event name*) to be stored and processed by SAFEWAY partners for the purpose of administering the SAFEWAY (*workshop/event name*).	**Yes**	**No**
I give my consent for all personal information provided by registering to the SAFEWAY (*workshop/event name*) to be processed by the SAFEWAY (*workshop/event name*) organizers to evaluate and decide on my application where workshop places are limited.	**Yes**	**No**
I give my consent for all personal information provided by registering to the SAFEWAY (*workshop/event name*) to be stored and processed by UVIGO for the purpose of overall coordination of the SAFEWAY project.	**Yes**	**No**
I give my consent for all personal information provided by registering to the SAFEWAY (*workshop/event name*) to be passed to UVIGO and FERROVIAL for storage and processing for the purposes of supporting exploitation and dissemination of workshop related information.	**Yes**	**No**
I give my consent for the following personal information to be passed on to the European Commission in case my workshop application is approved: name, surname, title, organization, position, email address, phone number.	**Yes**	**No**
I give my consent for the following personal information to be published on the Internet and elsewhere for the purposes of project transparency: name, surname and organisation affiliation.	**Yes**	**No**
I give my consent for my e-mail address to be published on the Internet or elsewhere to assist others to contact me (optional).	**Yes**	**No**

PARTICIPANT CERTIFICATION

I have read the *PROTECTION OF PERSONAL DATA WITHIN SAFEWAY (*https://www.safeway-project.eu/en/personal-data*)* and answered to all the questions on the table above. I have had the opportunity to ask, and I have received answers to, any questions I had regarding the protection of my personal data. By my signature I affirm that I am at least 18 years old and that I have received a copy of this Consent and Authorization form.

……

Name and surname of participant

……

Place, date and signature of participant

NB: Attach this completed form to your SAFEWAY *(workshop/event name)* application.

Further information: for any additional information or clarification about Data Protection treatment please contact the SAFEWAY coordinator at UVIGO (safeway@uvigo.es), or alternatively the University of Vigo's Data Protection Officer (DPO), Ana Garriga Domínguez with address at: Faculty of Law, As Lagoas s/n, 32004, Ourense, Spain (dpd@uvigo.es). This consent form does not remove any of your rights under GDPR but provides us with the necessary permissions to process your application and manage SAFEWAY workshops and events.

Appendix 2. Protection of Personal Data Within SAFEWAY

GIS-Based Infrastructure Management System for Optimized Response to Extreme Events of Terrestrial Transport Networks

PROTECTION OF PERSONAL DATA WITHIN SAFEWAY

Project acronym	SAFEWAY
Project name	GIS-BASED INFRASTRUCTURE MANAGEMENT SYSTEM FOR OPTIMIZED RESPONSE TO EXTREME EVENTS OF TERRESTRIAL TRANSPORT NETWORKS
Grant Agreement no.	769255
Project type	Research and Innovation Action
Start date of the project	01/09/2018
Duration in months	42
This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 769255.	
Disclaimer: This document reflects only the views of the author(s). Neither the Innovation and Networks Executive Agency (INEA) nor the European Commission is in any way responsible for any use that may be made of the information it contains.	

PROTECTION OF PERSONAL DATA WITHIN SAFEWAY

INTRODUCTION

The SAFEWAY project assumes the responsibility of complying with current legislation on data protection, guaranteeing the protection of personal information in a lawful and transparent manner in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the protection of individuals with regard to the processing of personal data and their free circulation (GDPR), with the national, regional and the University of Vigo's internal[2] regulations regarding the protection of personal data.

This document informs in detail the circumstances and conditions of the processing of personal data and the rights that assist the interested persons.

As coordinator of the action, the University of Vigo is the data controller for all personal data being collected for workshops and other communication and dissemination events. The University of Vigo has appointed as Data Protection Officer (DPO) to: Ana Garriga Domínguez with address at: Faculty of Law, As Lagoas s/n, 32004, Ourense, Spain (dpd@uvigo.es).

PURPOSE:

SAFEWAY partners will only collect the personal data strictly necessary in relation to the purposes for which they are treated, in accordance with the principles set in Article 5 of the GDPR. The information necessary to guarantee a fair and transparent treatment will be provided to the interested persons at the moment of collection, in accordance with the provisions of articles 13 and 14 of the GDPR.

The data collected by SAFEWAY for the dissemination activities aims to reach the widest audience to disseminate SAFEWAY project outcomes and to communicate the knowledge gained by its partners during the duration of the project.

The workshops or meetings with stakeholder are focused to present and discuss all project results, not only among project partners but also open to stakeholders and other target groups. The events will be targeted to technology innovators on infrastructure management, including end-users, materials and technology suppliers, the research community, regulatory agency, standardization bodies and all the potential players interested in fields associated to innovative resilience of transport infrastructure with special focus on their application in railway and roads.

PROCESSING OF PERSONAL DATA:

Your Personal Data is freely provided. Where it is specified in the registration form, the provision of Personal Data is necessary to provide you with the services

[2] *Instrución conxunta 5/2019, do 1 de marzo, da xerencia e da secretaría xeral para o desenvolvemento de medidas de tratamento de datos de carácter persoal na Universidade de Vigo https://secretaria.uvigo.gal/uv/web/normativa/public/show/273).*

expected from the dissemination event, and the access to SAFEWY project results. if you refuse to communicate these Data, it may be impossible for the Data Controller to fulfil your request. On the contrary, with reference to Personal Data not marked as mandatory, you can refuse to communicate them and this refusal shall not have any consequence for your participation and attendance to SAFEWAY dissemination activities.

The provision of your Personal Data for publication of your contact details on the Internet or elsewhere for networking implemented by the Data Controller is optional, consequently you can freely decide whether or not give your consent, or withdraw it at any time. Therefore, if you decide not to give your consent, SAFEWAY dissemination responsible will not be able to carry out the aforementioned activities.

SAFEWAY will never collect any special categories of Personal Data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation – Art. 9 of GDPR). SAFEWAY asks you expressly to avoid providing these categories of Data. In the event in which you voluntarily choose to give us these Data, the Company may decide not to process them or to process them only with your specific consent or, in any event, in compliance with the applicable law.

In the event of accidental processing of third party Personal Data is communicated to SAFEWAY, you become an autonomous Data Controller and assume all the related obligations and responsibilities provided by the law. In this regard, SAFEWAY is exempt from any liability arising from any claims or requests made by third parties, whose Data have been processed by us because of your spontaneous communication of them to us, in violation of the law on the protection of Personal Data. In any event, if you provide or process third party Personal Data, you must guarantee as of now, assuming any related responsibility, that this particular hypothesis of processing is based on a legal basis pursuant to Art. 6 of GDPR.

DATA STORAGE AND RETENTION:

The personal data provided will be kept for the time necessary to fulfill the purpose for which they are requested and to determine the possible liabilities that could derive from the same purpose, in addition to the periods established in the regulations on files and documentation. Unless otherwise stated, the data will be retained for a period of five years after the end of the project as this data can support the report of some of the implemented activities.

During this period, the data will be stored in a secured area with access by a limited number of researchers. SAFEWAY data managers will apply appropriate technical and organizational measures to guarantee a level of safety appropriate to the risk

and in accordance with the provisions of article 32 of the GDPR. The system also allows tracking of use of data. Five years after the end of the project, the data will be destructed at the surveillance of the Data Protection Officer at University of Vigo, as coordinating organization of SAFEWAY.

RIGHTS OF THE DATA SUBJECT:

Any person, as the holder of personal data, has the following rights recognized in the terms and under the conditions indicated in articles 15-22 of the GDPR:

- Right of Access: obtain from the controller confirmation as to whether or not personal data concerning you are being processed, more information on the processing and copy of the personal data processed.
- Right to Rectification obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning you and the right to have incomplete personal data competed.
- Right to Erasure: obtain from the controller, without undue delay, the erasure of personal data concerning you.
- Right to Restriction of Processing: obtain the restriction of the processing in the event you assume that your data are incorrect, the processing is illegal or if these data are necessary for the establishment of legal claims.
- Right to Data Portability: receive the personal data concerning you, which you have provided to a controller, in a structured, commonly used and machine-readable format, in order to transfer these data to another Controller.
- Right to Object: Object, on grounds relating to your particular situation, to the processing of personal data concerning you, unless the controller demonstrates compelling legitimate grounds for the processing. You can also object to processing your data where them are processed for direct marketing purposes.
- Right to withdraw the Consent: withdraw the consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

The subject may exercise their rights without any cost and will have the right to receive a response, within the deadlines established by current legislation on data protection, by contacting SAFEWAY project coordinators at: safeway@uvigo.es, or by contacting the Data Protection Officer at: dpd@uvigo.es.

CONTACT PERSON

For any additional information or clarification please contact SAFEWAY coordinators at UVIGO (safeway@uvigo.es). This consent form does not remove any of your rights under GDPR but provides us with the necessary permissions to process your application and manage SAFEWAY workshops and events.

Appendix 3. Guidelines for the Elaboration of Surveys

In general, most surveys considered within SAFEWAY (see Section 4) are not intended to collect personal data. The overall recommendation, when designing a survey, is that neither the name or other personal data (e.g., email, address, affiliation) of the person filling the survey should be collected in the survey. For instance, in the case of the survey being collected by means of physical forms, this means that the forms should not account with any space where this information is requested. Alternatively, when the survey is collected online appropriate mechanisms to avoid the collection of personal data must be implemented –e.g., although it is possible to send a link to the online platform where the survey is content, when sending this by means of an email targeted to a generic group of people or to targeted individuals, it must be ensured that neither the online platform where the survey is hosted, or the survey itself does collect any personal data – this includes the email address to which the link was originally sent.

For those cases where surveys are intended to collect personal data (see Sections 4.10 and 4.11), these should be designed in such a way that they just collect the information needed for the purposes that the project has. For example, it would be reasonable to collect personal data, such as name, age, studies or profession of someone that could potentially be interested in the services or products offered by SAFEWAY, however, it would not be acceptable to collect the personal address, an image or a picture of the person.

Under no circumstances personal data collected in surveys must be beyond the requirements of the information needed for the purpose of the survey/project. The following list summarises the most common type of personal data usually collected in similar type of surveys to those described in Section 4.10 and 4.11. In any case, the SAFEWAY partner in charge of the survey, together with the Project Coordinator, must analyse the main aim and objectives of the survey and identify which kind of personal data could be justified to be collected by the project, or not.

- Name
- Surname
- ID card number
- Personal address
- The country of residence or origin
- A picture or image of a person
- Personal email
- Corporate email
- Phone number
- A fingerprint
- Level of studies or studies
- Ideology or credos
- Political beliefs
- Race
- Sex life
- Health
- Bank account number

- Financial information
- Social media profiles
- Hobbies

If, after conducting this analysis, it is still decided to collect any kind of personal information, an informed consent (see Appendix 1) must be included together with the survey. The informed consent must inform the person answering the survey on who is responsible of the data treatment and on the ways to contact them, on the purpose of the data treatment, if there is any information that it is not mandatory to answer, and on the possibility to exercise their data protection rights. Together with the informed consent a copy of the Protection to Personal Data policy stablished by the SAFEWAY project (see Appendix 2) must be included, or alternatively the link to where this can be find in the SAFEWAY website (https://www.safeway-project.eu/en/personal-data).

Appendix 4. Interoperability and Exchange of Data

SAFEWAY

Interoperability and Exchange of Data

(Questions for when; a project begins, a new phase of the project begins or a new method or need for collecting data is introduced)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 769255. The sole responsibility for the content of this presentation lies with the author. It does not necessarily reflect the opinion of the European Union. Neither the Innovation and Networks Executive Agency (INEA) nor the European Commission are responsible for any use that may be made of the information contained therein.

Questions to determine Privacy and Confidentiality requirements

- These questions must be answered when; the project intends to collect new data or information, a new phase of the project begins that requires the collection of personal or confidential information, the project uses new programs or systems to collect or process data, or simply when a new project begins that could require data collection.
- Through this questionnaire we want to ensure the protection of the information collected, not only because of privacy or data protection, but also in regards to issues of confidentiality related to the project.
- The aim of these questions is to detect or prevent situations that could pose risks for the project, such as legal issues, security issues or ethical issues.

Previous recommendations

- When you answer the following questionnaire please take note of whether your answer requires checking another document such as, FAQS or other documents or links

- When you answer the questionnaire and your answer implies a RISK, you should contact your DPO or Ethics Advisor in order to define the type of risk and to consider possible ways to limit or minimize such a risk.

Are you currently using any system that allows for the exchange of personal data?

YES

NO

Are you currently using a system that allows for the exchange of confidential information?

YES

What type of confidential information?

Please describe*:

Any confidential information, information that must be protected by confidentiality or anything related to the know-how of a company. Sometimes it is necessary to store this type of information in safety systems, encrypted or similar (see Recommendations at the end)

Are you currently using any mechanisms or security measures to protect this information?

Please detail what type of measures you are adopting:

- ❑ Systems with standard and usual security measures (see document at the end)
- ❑ Encryption
- ❑ Anonymization
- ❑ Pseudoanonyimization

Encryption is recommended when sharing important or confidential company information (see Recommendations at the end)

Are you currently using any system that allows for the exchange of personal data?

YES

What type of personal data are you collecting?

- ❑ Name and surname
- ❑ Address
- ❑ ID Card
- ❑ E-mail
- ❑ Bank accounts
- ❑ Information about loans, debts…
- ❑ Hobbies, interests, preferences
- ❑ Image
- ❑ Information about crime commission
- ❑ Health information
- ❑ Biometrics
- ❑ Genetics information
- ❑ Ideologies, beliefs
- ❑ Sexual life
- ❑ Political information
- ❑ Beliefs or ideology
- ❑ Human race or ethnical information
- ❑ People affected by gender violence
- ❑ Union activity
- ❑ Information about minors

The information written in purple needs to be protected and processed in a special way. See recommendations at the end

How are you collecting this information?

- ❑ Forms (physical)
- ❑ Website/App/Platform

→ Please indicate URL or link:

- ❑ Via third parties

→ Pease indicate:

- ❑ How
- ❑ Why
- ❑ Who is the third party?
- ❑ Have you formalised any agreement with this party?

- ❑ Other methods

→ Please describe:

NO

If not… **RISK**

If yes… **Look at the end (Note 1)**

Are you informing individuals about the treatment and use of their personal data?

YES

How are you advising them?

- ❑ Forms
- ❑ In person
- ❑ Website/register
- ❑ Privacy policy displayed on website
- ❑ Other, please specify:

NO

RISK

**Please contact DPO or Ethics Mentor*

Have you received the expressed consent of these individuals?

YES

How have you received this consent? Please describe method in detail:

- ❑ Check box
- ❑ Signature
- ❑ Mail in which user accepted the treatment
- ❑ Other, please specify (see if there is any risk):

RISK

NO

RISK

How are you processing these type of information?

What type of programs do you use to process or store the information?

- ❑ It is a program licensed?
- ❑ I don't use any program to process the information
- ❑ It is a program developed for the company/project?

→ RISK

- ❑ Have you accepted the terms and conditions of the License?
- ❑ Is there any mention to privacy or confidentiality?
  - ❑ Yes, to both
  - ❑ No → RISK
  - ❑ Yes, but only privacy → RISK
  - ❑ Yes, but only confidentiality → RISK

It is important to make a PIA or EIPD or a small analysis of risks → RISK

Do you share information about the project?

- NO
- YES → That information contents personal or confidential information?
  - YES → How is shared?
    - ❑ By mail in the same network
    - ❑ By mail but different networks or connections → RISK*
    - ❑ Through our platform
    - ❑ Other, please specify (see if there is any risk): → RISK*
  - NO

** Look at the end (Note 2)*

What are you doing with the personal data after the project?

- ❑ We will delete the information → **RISK** **Please contact DPO or Ethics Mentor*
- ❑ Store for the legal time period and delete once this period has elapsed → What measures will you take to do this? Please specify:
  - ❑ Delete documentary information through a shredder
  - ❑ Delete digital information formatting the information
  - ❑ Overprint with 0 and 1 the information after deleting or formatting
  - ❑ Demagnetize

  (see recommendations at the end)
- ❑ Store forever → **RISK**

**Please contact DPO or Ethics Mentor or look at Good Practices Code*

Recommendations

- **General recommendations**
- **Security measures**
- **Some recommendations about encryption**
- **Technical and physical measures**
- **FAQs**
- **Summary of terms**
- **More info or interesting links good to know**

General recommendations

- On any platform where you are presenting your idea or Project to the public you must include; a Legal Advice, a Cookies Policy (if applicable) and a Privacy Policy (if you collect personal data through the platform – website, app, landing page, form, etc)

- When you use a form to collect personal data you must include a checkbox that links to your Privacy Policy that can be marked or clicked, and indicates something similar to, “I have read and I accept the Privacy Policy”.

- Even if you do not collect personal data but you collect corporate or companies information and this could be considered as a confidential information, you should consider to implement the security measures recommended in the following pages to protect this information

Security Measures recommended

- Usual measures for normal information:

  - Protocol specifying the backup procedures of the information collected
  - Systems controlled by users with controlled access, with properly defined profiles and roles
  - Use of programs that comply with data protection protection regulation or that ensure confidentiality or security of this type of information
  - Inventory of computers, tools, programs and systems used
  - Inventory of users that can access to the Project
  - Protocol where is described the way to give Access to the systems of the Project; ways to change roles or Access permits; ways to remove Users, among others
  - Password login must change almost once a year
  - Procedures for the exercise of rights of users/clients
  - Procedures to register any important incident with data and to communicate it to the competent authority or user afected

Security Measures

- Extra measures for special category of data:
  - Register that oversees or supervises who can or has accessed to the systems and programs and which actions has done
  - Register to write the movements inside/outside the company or Project with information with special category of data
  - Special and technical measures to protect special category of data like encryption, double opt-in to Access to special information

Some considerations about encryption

- **Mandatory encryption:**
  - When imposed by law like in the treatment or collection of data considered as a special category
  - When a Code of Conduct or of a sector requires it
  - When PIA or EIPD recommends it
  - To minimize or solve risks
- **Convenient encryption:**
  - Security breaches
- **Voluntary encryption:**
  - Dissociated information or when it applies art. 11 GDPR

- **Particular cases when encryption is required:**
  - When it is needed for the risk that implies to treat this type of information or the meaning of a breach of this information
  - To avoid the needs to inform about a security breach
- **Encryption is mandatory in the following sectors:**
  - Health
  - Prevention of money laundering
  - Telecommunications
  - National Defense or National Security
  - Legal issues
  - Journalism and press (to prevent filtration of information resources)
  - To protect Intellectual Property and know-how of companies

What technical and physical measures do we need to consider?

- A lot of security incidents can be due to the theft or loss of equipment, the abandonment of old computers, or hard-copy records being lost, stolen or incorrectly disposed of. Therefore security measures include both physical and technical protection for computer and IT security.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

When considering **physical security,** you should look at factors such as:

- The quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV.
- How you control access to your premises and how visitors are supervised.
- How you dispose of any paper waste and electronic waste.
- How you keep IT equipment, particularly mobile devices, secure.

What technical and physical measures do we need to consider?

When considering cybersecurity, you should look at factors such as:

- System security – the security of your network and information systems, including those which process personal data.
- Data security – the security of the data you hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely.
- Online security – the security of your website and any other online service or application that you use.
- Device security – including policies on Bring-your-own-Device (BYOD) if you offer this.

More info:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

FAQs

- It is obliged to implement data protection measures always when we collect data?
  - Not, only if we collect personal data, we must implement this type of measures and measures will depend on the risks and categories of data (special or not)
  - However, it could be necessary to take measures in order to protect, not personal data; when information collected is confidential, for example
- Have we to sign a Data Processor agreement with every Provider we have?
  - Not, only if Provider has access or treats personal data. If a Provider only can access to the building or premises of the company not working with data, only will be recommended to sign a letter of compromise of confidentiality
- It is possible to collect data without informing user affected for the treatment?
  - Not, user always must be informed, and we need the express consent unless law establishes another requirements or possibilities
  - It is not permitted a not express consent
- Are all measures and preventions explained in this document?
  - Not, only are described general aspects (please review with DPO or Ethics Mentor the impact your situation can mean for the project)

Note 1: Data Processors:

Data Processors are providers that provide a service that means a treatment of Personal Data. These providers shall follow concrete security measures like they were the Data Responsible because they are working with data that belongs to the Responsible.

It is mandatory to sign an agreement between Data Processor and Data Responsible that regulates the provision of the services in this sense. This agreement must include type of Access to data by the Provider, type of Data the Provider can Access and security measures implemented to comply with the corresponding obligations.

Type of obligations of the Data Controller:

- To follow the instructions of Responsible on the treatment of data when it is providing the service
- To implement the same security measures as the Responsible when the provision of services means working with the same information than the Responsible and see which categories of data are processed (sensible or special data according to GPDR)

Note 2: Sharing information

It is important to consider when two or more parties are sharing personal information:

(i) To review the legitimation to achieve or collect this information. Is the user or customer informed about the personal data treatment and who is collecting her/his data?

(ii) Company/Companies that collect this information, if they are more than one, have sign an agreement between parties?

(iii) Do they share the information because both are working in the same Project and could be co-responsibles of the treatment or do they share information to foreign or third parties?

(iv) Do they have taken the corresponding security measures?

(v) The Sharing of this information means to use platforms to share information that imply a treatment or management of data outside the European Union? In this case it is mandatory to analyse this situation, in particular.

Summary of Terms

- **Anonymization:** Is a type of information sanitization whose intent is privacy protection. It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous. The European Union's new General Data Protection Regulation demands that stored data on people in the EU undergo either an anonymization or a pseudonymization process (source: Wikipedia).
- **Pseudonymization:** is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable while remaining suitable for data analysis and data processing. Pseudonymization (or pseudonymisation) can be one way to comply with the European Union's new General Data Protection Regulation demands for secure data storage of personal information. Pseudonymized data can be restored to its original state with the addition of information which then allows individuals to be re-identified, while anonymized data can never be restored to its original state (source: Wikipedia).
- **Cybersecurity:** This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them (source: ICO.UK).
- **Encryption:** Is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users (source: Wikipedia).
- **PIA:** Privacy Impact Assessment. Is an analysis which assists organizations in identifying and managing the privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships. This normally must be done when starting a new business that implies treatment of personal data; or when a company opens a new branch or service that implies a new treatment of data.
- **EIPD or DPIA:** Is a Privacy impact assessment to help companies to identify and minimize the data protection risks of a project in any moment is needed.

- More information about Best Practices in Data and Confidentiality world:
  - About DPIA/PIAs: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
  - About reports in GPDR/Data Protection: https://edpb.europa.eu/about-edpb/board/annual-reports_en
  - About erasure:
  - https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_en
  - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/
  - About delete information in accordance with GDPR:
    - https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

SAFEWAY

TITLE MEETING