Deliverable 7.2

Data Management Plan

UK participants in Horizon Europe Project PHOEBE are supported by UKRI grant numbers 10038897 (The International Road Assessment Programme – iRAP) and 10056912 (The Floow)

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101076963

Document Control Page

Deliverable number	*7.2*
Deliverable title	*Data Management Plan*
Deliverable version	*1.0*
Work Package number	*WP7*
Work Package Title	*Project Management*
Due date of delivery	*30/APR/2023*
Actual date of delivery	*30/APR/2023*
Dissemination level	*Public*
Type	*Document*
Editor(s)	*Dr Sam Chapman, The Floow*
Contributor(s)	*Sam Chapman, The Floow* *Mark Burke, The Floow* *Ana Maria Perez Zuriaga, UPV,* *Alexios Aivaliotis, OSeven* *Andrejus Laugman, iRAP* *Alenka Volk, Eira*
Reviewer(s)	*Mark Brackstone, Aimsun* *Alexios Aivaliotis, OSeven*
Project name	*Predictive Approaches for Safer Urban Environments*
Project Acronym	*PHOEBE*
Project starting date	*01/11/2022*
Project duration	*45 months*
Rights	*PHOEBE consortium*

PM efforts per beneficiary that contributed to the deliverable

#	Partner	PM effort in the Deliverable
1	*FLOOW*	*0.4*
2	*AIMSUN*	*0.17*
3	*IRAP*	*0.0*
4	*EIRA*	*0.03*
5	*TUD*	*0.0*
6	*TUM*	*0.0*
7	*NTUA*	*0.0*
8	*FC*	*0.4*
9	*UPV*	*0.0*
10	*O7*	*0.07*
11	*POLIS*	*0.0*
Total	*PHOEBE Consortium*	*1.07*

Document History

Version	Date	Beneficiary	Description
0.1	*10/DEC/2022*	*Sam Chapman, The Floow*	*Internal draft*
0.2	*16/DEC/2022*	*Sam Chapman, The Floow*	*internal shared version*
0.3	*4/JAN/2023*	*Mark Burke, The Floow* *Sam Chapman, The Floow*	*Internal review*
0.4	*6/JAN/2023*	*Sam Chapman, The Floow*	*Draft for all partners – shared version*
0.5	*31/JAN/2023*	*Sam Chapman, The Floow*	*Refinement of DMP following comments from across project partners – addition of section 4 risk*
0.6	*7/MAR/2023*	*Sam Chapman, The Floow*	*Minor change to deliverable tables – connection to DMP only*
0.7	*5/APR/2023*	*Sam Chapman, The Floow*	*Final comment changes – new addition of GDPR management process.*
0.8	*12/APR/2023*	*Sam Chapman, The Floow*	*Conversion into latest deliverable format for formal review*
0.9	*12/APR/2023*	*Sam Chapman, The Floow* *Alexios Aivaliotis, OSeven*	*Minor comments and amendments before public release*
1.0	*30/APR/2023*	*Sam Chapman, The Floow*	*Public release*

Project Executive Summary

The EU-funded ‘Predictive Approaches for Safer Urban Environment’ (PHOEBE) project aims to develop an integrated, dynamic human-centred predictive safety assessment framework in urban areas. This will be achieved by bringing together the interdisciplinary power of traffic simulation, road safety assessment, human behaviour, mode shift and induced demand modelling and new and emerging mobility data.

Focused on vulnerable road users' safety, the 3.5-year-long PHOEBE project will draw inspiration from real-world scenarios in the three pilot cities of Athens (GR), Valencia (ES) and West Midlands (UK). Testing activities will be performed across the use cases to simulate and forecast the impact of changes on safety in different scenarios of disruptions or transitions across urban transport networks.

Predicting and visualising the safety and socioeconomic outcomes of new forms of transport, new technologies, or regulatory and behavioural changes from the individual (micro) level up to the network-wide (macro) level will also be a significant game-changer for urban stakeholders. The results of PHOEBE can be used as a blueprint by other European cities to develop their knowledge products, such as socioeconomic analysis model, urban road safety assessment, human behaviour and choice modelling.

PHOEBE pilot cities

List of participating cities:

- Athens (Greece)
- Valencia (Spain)
- West Midlands (United Kingdom)

Social Links:

https://twitter.com/Project_PHOEBE

https://www.linkedin.com/company/phoebe-project/

https://www.youtube.com/@phoebeproject

For further information please visit **WWW.PHOEBE-PROJECT.EU**

Project Partners

Organisation	Country	Abbreviation
EVROPSKI INSTITUT ZA OCENJEVANJE CEST - EURORAP	SI	**EIRA**
ETHNICON METSOVION POLYTECHNION	EL	**NTUA**
TECHNISCHE UNIVERSITEIT DELFT	NL	**TUD**
TECHNISCHE UNIVERSITAET MUENCHEN	DE	**TUM**
AIMSUN SLU	ES	**AIM**
POLIS AISBL	BE	**POLIS**
FACTUAL CONSULTING SL	ES	**FC**
UNIVERSITAT POLITECNICA DE VALENCIA	ES	**UPV**
OSEVEN SINGLE MEMBER PRIVATE COMPANY	EL	**O7**
THE FLOOW LIMITED	UK	**FLOOW**
INTERNATIONAL ROAD ASSESSMENT PROGRAMME	UK	**iRAP**

List of abbreviations and acronyms

Acronym	Meaning
CSV	Comma-separated values
D	Deliverable
DMP	Data management plan
DMPDS	Data management plan data set
DMPTask	Data management plan task area
DPA	Data Protection Act 2018 (UK)
DPDIB	Data Protection and Digital Information Bill
DPIA	Data Privacy Impact Assessment
EC	European Commission
EU	European Union
FAIR	Findable, accessible, interoperable and re-usable
GDPR	General Data Protection Regulation
HE	Horizon Europe
IPR	Intellectual property rights
ISO26000	International Standards Organisation – Social Responsibility
ISO27001	International Standards Organisation – Data Security
ISO9001	International Standards Organisation – Quality Management
PII	Personally Identifiable Information
SoA	State of the art
T	Task (sub part of a WP activity)
WP	Work package

Table of Contents

Contents

List of figures

List of tables

Deliverable executive summary

The PHOEBE Data Management Plan (DMP) satisfies Deliverable 7.2 (D7.2) for the PHOEBE project (agreement number 101076963). This document contains the first version of the DMP which will be reviewed and updated as needed in project delivery. The DMP describes how the PHOEBE project will manage the datasets that will be gathered or created during the course of the project. In addition, the DMP details the terms of best practice for handling metadata and storage in order to ensure that data is findable, accessible, interoperable, and reusable (FAIR). This document relates the core tasks with the data related to those tasks and details the safe handling of any personal identifiable information (PII).

LIVE DOCUMENT

Please note the Data Management Plan is a LIVE document so is subject to continuous improvements as are internal DPIA GDPR and related registers. This document may be updated periodically so as to present the best view of data management as evolution may occur during the work of the project.

1 Introduction

The scope of the first version of the PHOEBE Data Management Plan (DMP) is to detail how research data will be handled during and after the end of the project. This document will detail the data that is to be collected, the processing that will be performed on that data, and what outputs will be generated as a result of that processing. This will detail methodology and standards when used. The DMP will also detail the extent to which data will be shared as well as plans for the future curation and preservation of each dataset. The DMP will target '*findable*', '*accessible*', '*interoperable*' and '*reusable*' (FAIR) data handling where possible to support.

1.1. Project Data Background

The PHOEBE project is a Horizon Europe (HE) project funded by the European Commission (EC) with the aim to advance risk assessment frameworks and models for urban roads. The investigative work, development and evaluation will take place within three use-case regions; Athens (Greece), Valencia (Spain) and The West Midlands (United Kingdom). Within each region project supporting data will be collated, gathered, processed or produced. At times for the purposes of validation or evaluation beyond the use case regions wider data could also be gathered and processed to ensure applicability of approaches beyond the use case regions.

In particular the project work will undertake the following core data management tasks:

DMPTask id	DMPTask title	Core data management task activity within PHOEBE
DMPTask 1	Project Management Data	Undertake management of: staff, finances, timekeeping and wider project organisation. This includes activity at various levels: individually per partner and also to aid in project coordination where needed across partners and use case stakeholders.
DMPTask 2	External Engagement Data	Undertake stakeholder questionnaires, interviews and review, which requires the retaining and processing of results.
DMPTask 3	Data Exploration	Identify and prioritise the data required for supporting risk frameworks and models.
DMPTask 4	Data Collation	Collate data from regional stakeholders related to the usage or features of roads for the project work and its evaluation.
DMPTask 5	Data Creation	Produce means for generating new data to aid risk frameworks in the scenarios and use cases.
DMPTask 6	Data Pre-processing	Normalise and pre-process data to make it suitable for reuse in agreed formats.
DMPTask 7	Data Normalisation	Establishing data specifications such that data can be conformed to standard formats and quality.
DMPTask 8	Data Evaluation	Evaluate the extent to which additional data can be used to help investigate and understand road risk.

DMPTask 9	Data Outputs	Determine how new data sources can be incorporated into create a new risk framework and modelling approach.
DMPTask 10	Dissemination	Create research articles, papers, deliverables, presentations and media content.

Table 1- DMP core tasks

1.2. Data Management Plan Objectives

The data management plan (DMP) details data management processes and registers within the PHOEBE project in order to ensure strong data management practices. These approaches are aligned to the Horizon Europe Guidelines on FAIR data management (European Commission 2016)[1] and support strong data management aligned to legislation like GDPR and embrace good practice approaches.

The core objectives of the DMP are:

- To detail the approaches for handling operational data and research data within and beyond the project lifespan.
- To define how project datasets will be made 'FAIR' (Findable, Accessible, Interoperable and Reusable) and any restrictions to these terms aiming to be "as open as possible, as closed as necessary".
- To define the allocation of resources for data management aligned to wider workplan and deliverable activity to ensure continuous review and improvement of the plan.
- To define procedures for data security during the project and for data preservation.

1.3. Data Management Plan Scope

AUDIENCE: The intended target for the DMP is primarily the project partners to ensure good practice data handling. This is however a public document and may be viewed by wider stakeholders or other parties as needed.

RESPONSIBILITY AND OWNERSHIP: It is the responsibility of each partner to follow the data management plan and any related guidance and deliverables to ensure continuous review and improvement.

NOTIFICATION: Each partner must notify the coordinator and work package leaders regarding any changes in the data they are collecting or processing during the project to maintain up to date DMP. This is undertaken within WP2 in the D2.1 task and to support this a standing item review of data management has been added to quarterly work package leader reviews to update when needed this area.

UPDATE AND REVIEW: Any changes in data, processing or practice may in the future update this document and the overall data management plan to support required refinement to the project data handling as the project progresses.

[1] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/agr-contr/general-mga_horizon-euratom_en.pdf [LAST ASSESSED 12 APR 2023]

1.4. Related documents and guidance to the Data Management Plan

Related Guidance / Legislation	Area of relevance to PHOEBE and its data management plan and processes
Horizon Europe Guidelines on FAIR Data Management	This details the expected requirements for Horizon Europe research activities to ensure where appropriate FAIR data. Setting requirements and guidance for this document to detail data types handled, data protection and links to the ethical management D7.2 activities.
ISO27001	This standard details good practice for data security to ensure data handled is gathered, stored and processed safely in a managed and reviewed framework. Key Partners related to secure commercial data handling are accredited via external audit for ISO 27001, such as The Floow and OSeven
ISO26000	This standard details good practice for social responsibility in processes. This has relevance to guide the required data to ensure positive impacts to society aligned to research principles of the European Commission. All Partners within the project follow these high-level principles regarding data handling and usage to follow good practice in data management.
ISO9001	This standard details good practice for quality management and continuous improvement. The DMP follows this principle with continuous review, named ownership of areas within the DMP and standing action points to review to enable continuous improvement. Key Partners use standardised approaches to quality management such as The Floow
AI DATA ACT	This proposed legislation extends legal data protection for citizens to cover technologies that use artificial intelligence (AI). Although not yet enacted into law, the principles of risk identification related to processing are added into the risk review process (T7.3) to build in compliance ahead of expected law. Any AI processing tasks will be graded as low, medium or high risk in order to set appropriate risk management. We anticipate that the majority of project tasks will be graded as low risk.
GDPR	Generalised Data Protection Regulation provides legal mandates for data privacy, consent and its legal protection. This impacts the implementation of the DMP which must fully adhere to GDPR and wider good practice for its data handling.

	Each partner separately adheres to GDPR with the majority of project data and processing operating upon anonymised data (these are better explained alongside each data type the project handles, detailed below). The full aspects of GDPR adherence is addressed in section 3.2 which remains under continuous review throughout the project.
Data Protection Act 2018 (UK only)	The DPA recognises the separated legal framework for handling data in the UK. Two PHOEBE associate partners are based in the UK, which means that we must understand the implications of how the UK legal framework differs from that of the EU in respect to data transfer and adequacy. This legislation impacts the delivery of the DMP in relation to permitted data transfer, storage and consent. The implications of the DPA are further addressed in T5.4.2 and T7.4.2, relating to data privacy for the project. At present this legislation presents no significant impact to the project which expects to follow GDPR good practice.
Data Protection and Digital Information Bill (DPDIB) (UK only)	DRAFT UK legislation adjusting UK GDPR interpretation. The project will track this legislation and any impacts upon the project data handling.

Table 2 - Related Legislation and guidance to the Data Management Plan that PHOEBE seeks to align its processes and practices towards.

2 Project Data

Each of the core data management tasks (DMPTasks) have separate data needs and characteristics. The below table details each data task and its corresponding dataset. The table also details the responsible project partner and related WP tasks for each dataset.

Dataset name	Dataset contents	Owning Project Partner	DMPTask(s) related (see Table 2)	Related PHOEBE WP(s)
DMPDS1 - Partner Information, mailing lists and project coordination groups including external entities	**PII** - Contact details and metadata about project partners, staff and advisory contacts supporting project execution, steering and coordination including other project related external personal connection points (such as the monitoring officer).	IRAP, EIRA (and all partners)	DMPTask 1 – Project management data	WP7 (T7.1, T7.2)
DMPDS2 - Stakeholder mapping and	**PII** – Contact details and meta data related to use cases and stakeholder events.	NTUA (GR)	DMPTask 2 – External	WP2 (T2.1.1, T2.2.3)

related data around individuals and use cases		FC (ESP) FLOOW (UK)	Engagement Data	WP4 (T4.1, T4.4)
DMPDS3 - Data exploration and prioritisation records and registers	Project data exploration and analysis records. Registers of data for infrastructure, road behaviours, users, modes. (**Data should contain no PII** except information relating to data owners – held in DMPDS2)	FLOOW (supported by all partners)	DMPTask 3 – Data Exploration	WP2 (T2.2)
DMPDS4 - Collated data from the use case regions and stakeholders	Data from use-case regions related to anonymised data (**Data should contain no PII** but each dataset shall be reviewed and handled accordingly). Data relating to infrastructure, road behaviours, users, modes.	NTUA (GR) FC (ESP) FLOOW (UK)	DMPTask 4 – Data Collation	WP2 (T2.3)
DMPDS5 - New data creation and gathering	Data created or gathered by new means in relation to project needs in the use-case regions. **Data shared in the project between partners should not contain PII**.	NTUA (GR) FC (ESP) FLOOW (UK)	DMPTask 5 – Data Creation	WP2 (T2.3)
DMPDS6 - Preprocessed data (from DMPTask 4 and 5)	Data converted in formats filtered for use in the project. (**No PII**)	NTUA (GR) FC (ESP) FLOOW (UK)	DMPTask 6 – Data Pre-processing	WP2 (T2.4)
DMPDS7 - Normalised data (from DMPTask 6)	Data normalised for usage in framework and models. (**No PII**)	NTUA (GR) FC (ESP) FLOOW (UK)	DMPTask 7 – Data Normalisation	WP2 (T2.4)
DMPDS8 - Test and evaluation data	Data supporting scientific testing, quality control and analysis activity in the project across a range of work packages. **Shared data should not contain PII.**	Various - as per WP and task involved leaders.	DMPTask 8 – Data Evaluation	WP3 (T3.3.4, T3.4.5) WP4 (T4.2, T4.3) WP5 (T5.1,

				T5.2, T5.3) WP4 (T4.5) WP5
DMPDS9 - Model and framework configuration and output data	Data about use-case scenarios or regions detailing configurations or outputs of risk analyses or models. **This data does not contain PII.**	Various - as per WP and tasks involved leaders.	DMPTask 9 – Data Outputs	
DMPDS10 - Dissemination data	This data contains authored content and public reporting materials as well as materials and distribution details for dissemination. This includes project website, materials for the public domain and external presentation. **This may contain contact details to support both dissemination or invite contact about the project.**	POLIS	DMPTask 10 - Dissemination	WP6 (T6.1-6.6)

Table 3 - The Data Management Plan Data Sets (DMPDS) within project PHOEBE. Each is aligned to Data Management Plan Tasks – highlighted rows indicate data that may contain PII that must be handled in accordance with GDPR.

2.1 Data Summary

PURPOSE - The scope of data collection and generation within PHOEBE is to explore, develop and enhance road risk estimation frameworks and models.

RELATIONSHIP TO PROJECT OBJECTIVES – The data gathered, produced and processed is aligned to the DMP Tasks (table 2), which align to the project aims and workplan. All data and processing is in line with these core aims.

DATA FORMATS – The data formats across the project differ for each DMPTask and its corresponding data sets. The table below details data formats for each data type.

Dataset Name(s)	Data formats and repository location
DMPDS1 - Partner Information, mailing lists and project coordination groups including external entities **DMPDS2** - Stakeholder mapping and related data around individuals and use cases **DMPDS10** - Dissemination data	The data is stored in three locations: 1) Email between authorised participants (managed securely and in line with GDPR) – Format(s): Email 2) In the project shared repository (access controlled to project participants) – Format(s): Documents, Presentations, Tables, Consented Video records of meetings, Images (format specification provided in D7.1 section 8) 3) Website, publications, public deliverables and dissemination materials (each approved for release via peer review and privacy check) then made available to the public domain or external organisations – Format(s): Documents, Presentations, Tables, Video, Images and printed media (only containing consented PII release) **Key aspects of this data will be released following peer review to support WP6 dissemination activity - any release will ensure GDPR consent and compliance when required.**
DMPDS3 - Data exploration, with prioritisation records and registers **DMPDS4** - Collated Data from the use case regions and stakeholders **DMPDS5** - New data creation and gathering **DMPDS6** – Pre-processed data (from DMPTask 4 and 5) **DMPDS7** - Normalised data (from DMPTask 6) **DMPDS8** - Test and evaluation data	The data is stored in one location: 1) In the project shared repository (access controlled to project participants) – Format(s): Documents, Tables. **Key aspects of this data will be released in D2.1** These data are stored in a number of repositories depending upon the data size, security, type and access criteria. These data can be categorised into the following types: 1) Road Infrastructure, mapping and geographical context data and information related to place: These data may be in graphical, raster, shapefile or flat file tabular or node/edge graph formats. 2) Road user behaviour data and information. These data may be in graphical, raster, tabular, image or video formats. These data may be subject to an anonymisation process before sharing, in order to remove any PII. 3) Road user data. This may include count data or other measured details about road users. These data may be subject to anonymisation before sharing, in order to remove PII. 4) Mode choice data. This may be in tabular mode data or other measured details about mode. These data may be

	subject to anonymisation before sharing, in order to remove PII.
DMPDS9 - Model and framework output data	**Some aspects of this data will be released to support dissemination, evaluation and scientific publications.** Output data will be stored in relation to the use-case areas and scenarios. These data will be held by project partners or shared via repositories with access control to relevant parties. **Model outputs will be included into wide deliverables and reports.**

Table 4 - PHOEBE dataset formats and repository information. Highlighted rows contain potential PII data that may be shared between partners.

When datasets contain PII they will require processes to control access and further processing. These data may include details related to individuals in the form of:

- Name
- Affiliation
- Country
- Mailing address
- Professional background
- Job title
- IP addresses
- Photo
- Video footage (from meetings)
- Questionnaire and interview data (for stakeholders – aligned projects)

Special consideration is required to protect IPR and privacy where collated data is used (**DMPDS4)**. Analysis will be undertaken in WP2 which will ascertain the potential for such data to be *accessible* and *findable* to third parties.

Where special consideration may be needed to ensure data captured maintains data protection, when performing new data creation or gathering (**DMPDS5),** these considerations will be detailed in T5.4.2 and T7.4.2. This consideration will ensure that **PII** is consented for release/reuse or redacted before such data is shared or processed.

2.2 Data privacy and protection (GDPR)

To ensure alignment to legislation a specific GDPR and DPIA process has been established following GDPR best practices and record keeping. This aims to provide additional monitoring and ensure compliance in project based processing. This provides:

- A list of data controllers - to enable data protection notices, reviews or queries to be provided to legal data controller contact points. Please note that all organisations are separately classed as data controllers as per the terms of the collaboration agreement.

- A list of data processing tasks undertaken across the project for each processing area. This list aims to meet the needs of GDPR article 30 where a retained processing record is advised. For each data processing area it details the extent and scope of processing including:
    - Data retention - to establish a record for GDPR data retention targets
    - Data transfers - to establish a record of permitted data transfers beyond the EEA legal region to ensure data adequacy. The PHOEBE project expects to have no data transfer out of this region.
    - Third Party Processing - to establish a record of any sub processors that may be utilised. The PHOEBE project expects to have minimal third party processing.
    - Use of special category data - to establish the use of sensitive category data related to individuals. The PHOEBE project expects to have zero special category data.
    - Mitigating security measures to protect data - to detail high level controls to mitigate risks for data protection.

ARTICLE 30 REGISTER

TITLE *	PROCESSING PURPOSE *	TYPES OF PERSONAL DATA *	DATA RETENTION PERIOD *	DATA TRANSFER TO/FROM ANOTHER COUNTRY *	THIRD PARTY PROCESSORS * NO/DETAILS	SPECIAL CATEGORIES OF PERSONAL DATA? * YES/NO	SPECIFIC ORGANISATIONAL SECURITY MEASURES FOR PROCESSING *	PRINCIPAL ORGANISATIONS
DMPDS1 processing	Processing of partner information, mailing lists, external contacts for project coordination, communication, emails and collaborative working including analysis of gathered data in relation to contracted or 'opt-in' individuals for the purpose of advancing the PHOEBE project. EACH PARTNER IS SEPERATELY A DATA CONTROLLER FOR THIS PURPOSE.	PII - names and connected informations about individuals in connection to the PHOEBE project.	Data may be held upto 7 years from any point of consented processing within the project work. Individual stores may have lesser retention periods depending upon partner organisations and seperated stores that may be used.	Data will be held ONLY in EEA region with full data adequacy agreements and support for GDPR legislation. No partner will transfer data beyond EEA region boundaries.	None (all processing is undertaken by project partners without 3rd party processing)	No	Use of secure project respository and project communications. Each partner is seperately accountable for its security measures	ALL

Figure 1 - GDPR article 30 processing register for processing tasks related to the PHOEBE project.

This register can be used to present records of project related processing as needed for any third party data request or to provide comfort on permitted processing..

- A register of Data Privacy Impact Assessments (one for each data processing task) with each follows a stepped process of:
    1. screening,
    2. purpose validation,
    3. checks for suitable consultation,
    4. checks for suitable necessity,
    5. checks for suitable proportionality,
    6. a consideration of risks,
    7. named sign off for the impact assessment and acceptance of details.

The template for this process is detailed in the following template:

SCREEENING QUESTIONS - if the anser is YES ALL other fields must be completed					
Does the task process PII?	Does the task share PII?	Is PII used for a new purpose?	Is privacy intrusive technology used? (e.g. Camera/geospatial tracking)	Are automated decsions made using PII data?	Is contact to individuals required that is not already consented?
PURPOSE QUESTIONS (only if ANY screening questions are yes)					
PURPOSE (what the task tries to achieve)		PURPOSE FITS WITHIN ARTICLE 30 (see A30 tab)	NATURE OF PROCESSING (how is data collected / used / stored / deleted - also will it be shared to whom)	SCOPE OF PROCESSING (how much data / limited by what extent / how many individuals PII are involved)	PROCESSING CONTEXT (relationship to the individuals in the PII, is the context of processing typical for the audience)
CONSULTATION, NECESSITY & PROPORTIONALITY (only if ANY screening questions are yes)					
What is the consultation process or consent obtained		Is the consultations sufficient to ensure consent or right to process		What is the lawful basis for processing	Is the lawful basis for processing proportionate and not excessive to need
RISKS (only if ANY screening are yes)					
What are the risks in the processing of the PII data?	What is the level of risk for this task	What Mitigations are in place to minimise the risk			What is the resultant level of risk for this task after mitigations
FINAL REVIEW AND SIGN OFF					
Who approves the task as acceptable for processing (right)					

Table 5 - Template example of DPIA records used for all tasks in the PHOEBE project.

These registers are updated continuously in the project with formal review quarterly by standing items in leadership meetings which considers potential new processing and needs for revisions to an ongoing GDPR register for the project.

2.3 FAIR Data

This section relies on the standard H2020 template for FAIR data ("Guidelines on FAIR Data management in Horizon 2020" - European Commission, 2016). All data collated and generated will be considered for external usage and made to be findable, accessible, interoperable, and reusable; unless an opt-out restriction is in place.

2.4 FAIR Data Opt-Out restrictions

Project partners may choose to 'opt-out' from handling data under FAIR management guidelines. FAIR Data 'Opt out' will be tracked throughout the project along with the legitimate reasons for any opt-out. This register will be supported within WP2 and will be included in the D2.1 and D2.2 reporting deliverables to enable continuous tracking. These deliverables will detail specific management for FAIR principles per data set and any opt-out exemption if applicable. Data may be opted out of FAIR principles for specific reasons, such as (but not limited to) the following:

- **To support data privacy –** for instance **DMPDS1** and **DMPDS2** which will restrict aspects of data sharing to protect privacy or financial information related to the project, stakeholders and participants in particular contact and restricted management details.
- **To support Intellectual Property Rights and project exploitation –** for instance **DMPDS4** in using existing data may have protections or limitations to enable full disclosure. The same could be found within the project whereby for example **DMPDS5** could generate capability for onward exploitation that may limit full FAIR disclosure to not harm potential exploitation that could be considered.
- **To support contractual protections –** for instance use case and scenario linked data gathered in **DMPDS4** may only be available to the consortium under contracted terms that could prevent onward sharing of data. Contractual protections may apply to use-case regions where data is sometimes owned and controlled by third party data owners.
- **To support ethical protections –** if data release could cause potential societal harm identified from stakeholder interactions in relation to data and its impacts, for instance if specific road data may harm regional activities for instance: road enforcement, public safety and security or resilience concerns.

2.5 Making data 'findable'

Activity under WP2 (detailed in D2.1) will include the collation of metadata to help support making the data findable. Such metadata will also be included in any public data releases (e.g. via the website) in order to help users identify pertinent data for their interest.

D7.1 (section 6.6) established a convention for file names to ensure a consistent and identifiable file naming system for folders, files and deliverables. This convention ensures the inclusion of project identifiers and version information into names. All deliverables and documents will include document control details (as per this document).

2.6 Making Data openly accessible

All project data will be reviewed (D2.1) to assess whether it can be made openly available pending potential opt-outs for reasons of privacy, IPR, contractual, or ethical reasons. Some data that holds PII may be held by individual partners prior to aggregation or anonymisation for use in the project.

Shared data will be openly available to project partners via the project repositories or the shared drive folder, which is authorised for use by all project participants. Where possible, data will be held in common shareable formats to allow access for all without specialised software, e.g. CSV, DOCX, XLS, PDF. Where specialised tools are needed, for instance, when performing the risk framework and modelling, these will be available in the project as needed.

2.7 Making data interoperable

The project seeks to use standard file formats and naming conventions to ease interoperability. The collection of metadata will follow a single approach, as detailed in D2.1. This process will be supported by WP2 activity throughout the project.

2.8 Making data re-usable

Within the project a range of tasks specifically seek to improve: data quality (T2.4), data formats (T1.4.1, T2.1.3, T2.3.4, & T2.2.5) and data storage handling and availability (T7.4.1). Data reuse is recorded alongside other attributes of data, as part of WP2, in order to maximise the chance of the data being reused.

3 Allocation of Resources

The project plan (WP7) is aligned to continuous monitoring and improvement in data management. Aligned deliverables from multiple WPs support the overall data management.

3.1 Data Management Plan – related deliverables

The DMP is supported by related tasks and deliverables within wider work package activities. These deliverables are detailed in the table below, together with the responsible project partner.

Deliverable Identifier	Title of deliverable	Responsible Partner	Description of deliverable and its connection and support to the DMP and its continuous implementation and refinement in the project
D1.1	SoA and end user needs review	TUD	This deliverable explores related literature and the state of the art. This review will be used to set the data expectations for the project.
D1.2	Theoretical principles and methodological approach of the PHOEBE	TUD	D1.2 will directly inform the principles for expected processing and will identify the data required in the project that is subject to management under the DMP. We expect this deliverable to lead to refinement of the DMP.

Deliverable Identifier	Title of deliverable	Responsible Partner	Description of deliverable and its connection and support to the DMP and its continuous implementation and refinement in the project
	framework and selection of tools		
D2.1	Consolidated data requirements and use case region data availability report	FLOOW	D2.1 solidifies data requirements and owners, as well as any requirements that may restrict the accessibility of the data.
D2.2	Data register, feature report and accreditation	FLOOW	This register details all data used in the technical project delivery that is subject to the DMP. The register will also document conformance accreditation for use in framework models. The register will help to make data 'findable' by documenting suitable metadata.
D3.1	New and enhanced models/simulation environments and user support materials (Beta ed.)	iRAP	D3.1 identifies and defines the 'data consumer' needs from stored data to enable new and enhanced models. These place requirements for data 'availability' to meet the needs of project partners.
D3.2	Finalised models/simulation environments methodology factsheets and user support materials	iRAP	This deliverable details the finalised models and risk frameworks, part of which will involve documenting the ongoing needs and accessibility of the data managed by the DMP.
D4.1	Use case experimental designs	EIRA	This activity defines the specific data needs for each use-case region, as well as relevant scenarios. The DMP will handle and document these data.
D4.2	Consolidated use-case evaluation and assessment report	EIRA	This evaluation helps to establish the impact of data in support of validation and assessment of the work in each region.

Deliverable Identifier	Title of deliverable	Responsible Partner	Description of deliverable and its connection and support to the DMP and its continuous implementation and refinement in the project
D5.1	Consolidated PHOEBE framework methodology, network-level demonstration results and tools	NTUA	This demonstration framework details the data needed for dissemination (DMPTask 10).
D5.2	User interface and implementation	POLIS	This interface details needed dissemination, the data for which is documented under DMPTask 10.
D6.1	Communication, dissemination and exploitation plan	POLIS	This details the plan for dissemination and communication beyond the project supporting wider dissemination (DMPTask 10).
D6.2	Final exploitation, IPR and replication plans	FC	This details exploitation plans, registers and materials that require management. This deliverable supports DMP aims for maintaining data after the project ends (DMPTask 10).
D7.1	Project Management Handbook	iRAP	This document defines operating management for the project including deliverable document storage and backup for operating documents and deliverables. This includes ownership details for the storage to meet the DMP aims.
D7.2	Data Management Plan	FLOOW	This document (DMP).
D7.3	Ethics Management Plan	FLOOW	This document should be read alongside the DMP; it contains the ethical management plan for the project and its delivery.

Table 6 - Related deliverables to the Data Management Plan.

4 Ethical Aspects

Ethical management although related to data management is detailed separately in the ethical management plan (D7.3.). The ethical management plan, also subject to continuous update, should be considered alongside the DMP.

5 Risk Aspects

Risk management related to data is handled throughout the project and will also be captured in the project risk register (D7.1).

LIVE DOCUMENT

Please note the Data Management Plan is a LIVE document so is subject to continuous improvements as are internal DPIA GDPR and related registers. This document may be updated periodically so as to present the best view of data management as evolution may occur during the work of the project.