

Deliverable 7.3

Data Management Plan (final)

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



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

The sole responsibility for the content of this document lies with the authors. It does not necessarily reflect the opinion of the European Union. Neither CINEA nor the European Commission are responsible for any use that may be made of the information contained therein.

Document Control Page

Deliverable number	7.3
Deliverable title	<i>Data Management Plan</i>
Deliverable version	2.4
Work Package number	WP7
Work Package Title	<i>Project Management</i>
Due date of delivery	31/JULY/2026
Actual date of delivery	1/JULY/2026
Dissemination level	<i>Public</i>
Type	<i>Document</i>
Editor(s)	<i>Dr Sam Chapman, The Floow (version a & b)</i>
Contributor(s)	<i>Sam Chapman, The Floow (version a & b) Mark Burke, The Floow (version a & b) Ana Maria Perez Zuriaga, UPV, (version a) Alexios Aivaliotis, OSeven, (version a) Andrejus Laugman, iRAP, (version a) Alenka Volk, Eira, (version a) Stefania Pesavento, Factual, (version a)</i>
Reviewer(s)	<i>Mark Brackstone, Aimsun, (version a) Alexios Aivaliotis, OSeven, (version a) Athina Tympakianaki, Aimsun, (version b) Haris Sideris, OSeven, (version b)</i>
Project name	<i>Predictive Approaches for Safer Urban Environments</i>
Project Acronym	<i>PHOEBE</i>
Project starting date	01/11/2022
Project duration	45 months
Rights	<i>PHOEBE consortium</i>



PM efforts per beneficiary that contributed to the deliverable

#	Partner	PM effort in the Deliverable
1	FLOOW	0.3
2	AIMSUN	0.02
3	IRAP	0.0
4	EIRA	0.0
5	TUD	0.0
6	TUM	0.0
7	NTUA	0.0
8	FC	0.0
9	UPV	0.0
10	O7	0.02
11	POLIS	0.0
Total	<i>PHOEBE Consortium</i>	<i>0.34</i>



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
2.0	20/NOV/2024	Sam Chapman, The Floow	Amended release to reflect new regulation and good practice for AI processing management
2.1	25/NOV/2025	Sam Chapman, The Floow	Amended version to add: 1) better mention of the UK's DUAA legislation, 2) better mention EU's Data Act, 3) details about how ZENODO is related to FAIR reporting with reference in the document to the outputs according to the DMP
2.2	9/MAR/2026	Sam Chapman, The Floow	Further additions to the document regarding the use of Zenodo and FAIR reporting. Additional notes



Version	Date	Beneficiary	Description
			have been added in respect to CRA and DORA regulation.
2.3	15/JUN/2026	Sam Chapman, The Floow	Stronger details on end-of-project preservation, FAIR implementation evidence and long term stewardship. Additions and changes throughout the document for revised updated version.
2.4	1/JUL/2026	Sam Chapman, The Floow	Incorporating internal review comments to prepare final version of 7.3 – mostly typos and formatting changes only.



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 FLOW LIMITED	UK	FLOW
INTERNATIONAL ROAD ASSESSMENT PROGRAMME	UK	IRAP



List of abbreviations and acronyms

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



Table of Contents

<i>Project Executive Summary</i>	<i>5</i>
<i>PHOEBE pilot cities</i>	<i>5</i>
<i>Project Partners</i>	<i>6</i>
<i>List of abbreviations and acronyms</i>	<i>7</i>
<i>Deliverable executive summary</i>	<i>10</i>
1 Introduction	11
1.1. Project Data Background	11
1.2. Data Management Plan Objectives	12
1.3. Data Management Plan Scope	12
1.4. Related documents and guidance to the Data Management Plan	13
2 Project Data	15
2.1 Data Summary	17
2.2 Data privacy and protection (GDPR)	21
2.3 AI processing and record keeping	23
2.4 FAIR Data	23
2.5 FAIR Data Opt-Out restrictions	24
2.6 Making data ‘findable’	24
2.6.1 Zenodo open data community	25
2.7 Making Data openly accessible	25
2.8 Making data interoperable	26
2.9 Making data re-usable	26
2.10 Final data legacy and preservation	26
3 Allocation of Resources	28
3.1 Data Management Plan – related deliverables	28
4 Ethical Aspects	30
5 Risk Aspects	30



TABLE OF FIGURES AND TABLES

Figure 1 - Zenodo open data community which details both deliverables and open data from the PHOEBE project.
25

Table 1 - DMP core tasks [please note that later in the project life secondary data sets beyond planned scope extended from these core areas - these are detailed later in this document]. 11

Table 2 - Related Legislation and guidance to the Data Management Plan that PHOEBE seeks to align its processes and practices towards. [UPDATED in NOV 2024, DEC 2025 and MAR 2026] 14

Table 3 - The Data Management Plan Data Sets (DMPDS) within project PHOEBE. Each is aligned to Data Management Plan Tasks – highlighted rows indicate dataset types that may contain PII that must be handled in accordance with GDPR [This table was updated throughout the project life] 17

Table 4 - PHOEBE dataset formats and repository information. Highlighted rows contain potential PII data with controlled needs only sharing between partners [This table was updated throughout the project life without further change from March 2026]. 20

Table 5 - GDPR and AI processing article 30 register for processing and AI tasks related to the PHOEBE project. 21

Table 6 - Template example of DPIA records used for all tasks in the PHOEBE project. 22

Table 7 - Example of the AI register tracking AI usage in support of the PHOEBE project and review of the risks for such usage. All risks are regarded as LOW (MARCH 2026). 23

Table 8 – Final data and legacy table detailing the longer-term preservation and persistence of project materials. 28

Table 9 - Related deliverables to the Data Management Plan. 30



Deliverable executive summary

The PHOEBE Data Management Plan (DMP) satisfies Deliverable 7.3 for the PHOEBE project (agreement number 101076963). This document contains the final version of the DMP. The DMP describes how the PHOEBE project managed data used, gathered or created during the course of the project. In addition, the DMP details best practice approaches applied for the project handling of 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) and controls to ensure legal and suitable data handling.



1 Introduction

The scope of the final version of the PHOEBE Data Management Plan (DMP) details how research data has been handled during and beyond the end of the project. This document details the data that has been collected, the processing performed on that data, and what outputs are generated as a result of that processing. This will detail methodology and standards when used. The DMP details the extent of future curation and preservation of project datasets. The DMP targets ‘findable’, ‘accessible’, ‘interoperable’ and ‘reusable’ (FAIR) data handling.

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). Project-supporting data will be collated, gathered, processed or produced within each region. At times, for the purposes of validation or evaluation beyond the use case regions, additional 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 [please note that later in the project life secondary data sets beyond planned scope extended from these core areas - these are detailed later in this document].

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. This document also aims to act as a guide for data management beyond the project to framework users and future researchers.

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 had to notify the coordinator and work package leaders regarding any changes in the data they are collecting or processing during the project to maintain an up-to-date DMP. This was undertaken within WP2 in the D2.1 task but also supported in WP5 and WP7 activity to support this. A long-standing item review of data management has been added to quarterly work package leader reviews to update when needed about this area which is reported in WP7 updates.

UPDATE AND REVIEW: Any changes in data, processing or practice updated 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 1 JUL 2026]



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	<i>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 D7.4 activities.</i>
ISO27001	<i>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 Flow and OSeven.</i>
ISO26000	<i>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.</i>
ISO9001	<i>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 Flow.</i>
AI Act	<i>This legislation (enforced from JAN 2025) extends legal data protection and processing to ensure wider data protection for citizens. This enact into law the principals of risk identification related to AI processing when it could impact others. Compliance checks are required ahead of JAN 2025 to ensure coverage for AI processing tasks is suitable recorded. This ensures that AI like processing tasks will be graded LOW / MED / HIGH to set appropriate data management and handling built into wider data management plans. Working with anonymised data in AI tasks it is expected that all project tasks will likely be graded LOW. Exceptions to this could be camera image recognition tasks and RISK estimations that could impact individuals.</i>
Generalised Data Protection Regulation	<i>GDPR 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.</i>
Data Protection Act 2018 (UK only)	<i>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.</i>



Related Guidance / Legislation	Area of relevance to PHOEBE and its data management plan and processes
Data (Use and Access) Act 2025 (UK only)	23 OCT 2024 new legislation was introduced impacting UK partners or data transfer between them and EU partners. This law is not yet active but has a second reading before passing into legislation following NOV 2024. This when enacted places stronger adequacy protection between UK/EU, increases ICO (regulator) enforcement powers, revised "common law" standards for data transfer and rights between data traffic between EU/UK. This legislation also increased e-Privacy rules and penalties for breaches of this regulation. Despite the new law these add weight to GDPR and common EU practice and agreed approaches between EU/UK to ensure effective delivery of GDPR. Law impacting the project and its safeguards remains unchanged.
European Data Protection Board guidelines	EDPB provides guidance on EU GDPR regulation with notices detailing legal interpretation as supported by GDPR law. These notices should be considered as legislation according to GDPR as and when introduced as guidance. This guidance added strong guidance in sub processor guidance and processor responsibilities to ensure adequate protection for GDPR or EQUIVALENT processing under article 28. Transparency of sub processors is recommended with GDPR equivalent protection of data detailed. This guidance may ask all partners processing that uses third party processing to list sub processors. Each partner is individually responsible for its transparency under this guidance and provides as may be required details on any sub processors and equivalent protective processing. This guidance also introduced enhanced cross boarder enforcement for GDPR breaches and clarification of legitimate interest following recent ECJ rulings. These rulings indicate that legitimate interest should not be relied upon as a legal basis to justify processing in a wider range of cases than previously applied. Following a review on 18/Nov/2024 [FLOOW], these changes do not impact project processing and ethical data.
Cyber Resilience Act (Regulation 2024/2847)	The Cyber Resilience Act (CRA) aims to ensure secure hardware and software connected products meeting high regulatory standards to protect consumers of products and services. The PHOEBE framework is not a commercially delivered capability meaning it is not regulated under the CRA regulation. However, it should be noted that CRA is potentially still applicable to software and hardware products that may exist in connection with the PHOEBE framework. For instance, third party sensors, telematics devices, or commercial modelling software. In such areas CRA will likely be applicable, including for software only products. Although these are out of scope regarding the research and operation of the PHOEBE framework, it may apply to aspects of connected data and services used to supply inputs into the framework. For PHOEBE it therefore remains essential to ensure credible CRA regulated products and services where these may be applicable to the project needs.
Digital Operational Resilience Act	DORA regulation aims at stronger data security standards within critical financial and ICT critical service providers. This regulation is sector specific without direct impact to PHOEBE or its framework. Despite this the PHOEBE framework may utilise data from a wide range of sources including those where DORA restrictions may be applicable. These are most likely in financial products relating to the insurance sector which are regulated under DORA. In these areas these external systems will have strict regulations and controls. The use of PHOEBE is restricted to anonymised outputs from these regulated environments.

Table 2 - Related Legislation and guidance to the Data Management Plan that PHOEBE seeks to align its processes and practices towards. [UPDATED in NOV 2024, DEC 2025 and MAR 2026]

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)
<i>DMPDS1 - Partner Information, mailing lists and project coordination groups including external entities</i>	<i>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).</i>	<i>IRAP, EIRA (and all partners)</i>	<i>DMPTask 1 – Project management data</i>	<i>WP7 (T7.1, T7.2)</i>
<i>DMPDS2 - Stakeholder mapping and related data around individuals and use cases</i>	<i>PII – Contact details and meta data related to use cases and stakeholder events.</i>	<i>NTUA (GR) FC (ESP) FLOOW (UK)</i>	<i>DMPTask 2 – External Engagement Data</i>	<i>WP2 (T2.1.1, T2.2.3) WP4 (T4.1, T4.4)</i>
<i>DMPDS3 - Data exploration and prioritisation records and registers</i>	<i>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)</i>	<i>FLOOW (supported by all partners)</i>	<i>DMPTask 3 – Data Exploration</i>	<i>WP2 (T2.2)</i>
<i>DMPDS4 - Collated data from the use case regions and stakeholders</i>	<i>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.</i>	<i>NTUA (GR) FC (ESP) FLOOW (UK)</i>	<i>DMPTask 4 – Data Collation</i>	<i>WP2 (T2.3)</i>
<i>DMPDS5 - New data creation and gathering</i>	<i>Data is 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.</i>	<i>NTUA (GR) FC (ESP) FLOOW (UK)</i>	<i>DMPTask 5 – Data Creation</i>	<i>WP2 (T2.3)</i>
<i>DMPDS6 - Preprocessed data (from DMPTask 4 and 5)</i>	<i>Data converted into formats filtered for use in the project. (No PII)</i>	<i>NTUA (GR) FC (ESP) FLOOW (UK)</i>	<i>DMPTask 6 – Data Pre-processing</i>	<i>WP2 (T2.4)</i>
<i>DMPDS7 - Normalised data (from DMPTask 6)</i>	<i>Data normalised for usage in framework and models. (No PII)</i>	<i>NTUA (GR) FC (ESP) FLOOW (UK)</i>	<i>DMPTask 7 – Data Normalisation</i>	<i>WP2 (T2.4)</i>

Dataset name	Dataset contents	Owning Project Partner	DMPTask(s) related (see Table 2)	Related PHOEBE WP(s)
<i>DMPDS8 - Test and evaluation data</i>	<i>Data supporting scientific testing, quality control and analysis activity in the project across a range of work packages. Shared data should not contain PII.</i>	<i>Various - as per WP and task involved leaders.</i>	<i>DMPTask 8 – Data Evaluation</i>	<i>WP3 (T3.3.4, T3.4.5) WP4 (T4.2, T4.3) WP5 (T5.1, T5.2, T5.3)</i>
<i>DMPDS9 - Model and framework configuration and output data</i>	<i>Data about use-case scenarios or regions detailing configurations or outputs of risk analyses or models. This data does not contain PII.</i>	<i>Various - as per WP and tasks involved leaders.</i>	<i>DMPTask 9 – Data Outputs</i>	<i>WP4 (T4.5) WP5</i>
<i>DMPDS10 - Dissemination data</i>	<i>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.</i>	<i>POLIS</i>	<i>DMPTask 10 - Dissemination</i>	<i>WP6 (T6.1-6.6)</i>
<i>DMPDS11 - Collated Data from the use case regions and stakeholders - VIDEO DATA</i>	<i>Data from use case regions that may record or process traffic and VRU video data. This data may contain (when in high enough resolution) images of vehicle registration plates, faces of individuals.</i>	<i>NTUA (GR) iRAP (UK) UPV (ES) FC (ESP) FLOOW (UK)</i>	<i>DMPTask 4 – Data Collation (Video data only)</i>	<i>WP2 (T2.3) - specifically in video data collection</i>
<i>DMPDS12 - website analytics for reporting to funders</i>	<i>Website visitor analytics, including user ID, location, browser details.</i>	<i>POLIS (BE)</i>	<i>DMPTask 10 - Dissemination - website usage tracking</i>	<i>WP6 (T6.1-6.6)</i>
<i>DMPDS13 - Collated Survey Data from the use case regions citizens - behaviour</i>	<i>Survey based data collection for behavioral modelling, contains anonymised entries of participant survey responses including, propensity of non compliance road usage behavioral data, demographic data and other survey response questions. Although this data includes non compliance data of participants this data does not contain any PII to enable linking to individual recipients to constitute PII.</i>	<i>TUD (NL)</i>	<i>DMPTask 4 – Data Collation</i>	<i>WP2 (T2.3), WP3 (surveys - behavioural modelling)</i>



Dataset name	Dataset contents	Owning Project Partner	DMPTask(s) related (see Table 2)	Related PHOEBE WP(s)
<i>DMPDS14 - Collated Survey Data from the use case regions citizens - mode choice</i>	<i>Survey based data collection for mode choice behaviour modelling, contains anonymised entries of participant survey responses including, mode choice response data, demographic data and other survey response questions. This data although capturing data from citizens it captures no direct identifiers or PII. A post code is gathered to allow approximate location to be determined without precision to determine individual participants.</i>	<i>TUM (DE)</i>	<i>DMPTask 4 – Data Collation</i>	<i>WP2 (T2.3), WP3 (surveys - mode choice modelling)</i>

Table 3 - The Data Management Plan Data Sets (DMPDS) within project PHOEBE. Each is aligned to Data Management Plan Tasks – highlighted rows indicate dataset types that may contain PII that must be handled in accordance with GDPR [This table was updated throughout the project life]

Beyond this scope of core processing new processing tasks have been added in the life of the project supplementing GDPR and AI Processing article 30 Registers. These include processing tasks that require DPIA or AI controls that may be needed by the project for instance processing CCTV and public realm video data or undertaking AI risk estimation tasks to meet the needs of the EU AI ACT.

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	End of project data summary table
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 have been released following peer review to support WP6 dissemination activity - all releases ensured GDPR consent and compliance when required with consideration for transfer and adequacy.	FAIR STATUS: RESTRICTED DATA PUBLIC/RESTRICTED: RESTRICTED DOIs: No DOIs (not findable) PRESERVATION PLAN: Retained under GDPR by separate partners data retention and preservation strategies with shared project related storage under joint control
DMPDS3 - Data exploration, with prioritisation records and registers	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	FAIR STATUS: FAIR (on final resources) PUBLIC/RESTRICTED: Public (on final resources) DOIs: YES on final public output materials PRESERVATION PLAN: Zenodo
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)	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.	FAIR STATUS: FAIR/UPON REQUEST/RESTRICTED PUBLIC/RESTRICTED: Partial DOIs: YES on FAIR resources PRESERVATION PLAN: Zenodo / originating source locations / held and managed by partners for longer term use

Dataset Name(s)	Data formats and repository location	End of project data summary table
DMPDS8 - Test and evaluation data	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. Some aspects of this data will be released to support dissemination, evaluation and scientific publications.	
DMPDS9 - Model and framework output data	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.	FAIR STATUS: FAIR / UPON REQUEST / RESTRICTED PUBLIC/RESTRICTED: Partial DOIs: YES on FAIR resources PRESERVATION PLAN: Zenodo / held and managed by partners for longer term use
DMPDS11 - Collated Data from the use case regions and stakeholders - VIDEO DATA	Video data from traffic cameras: 1) traffic data positioned at intersections and routes within the use cases. This will be held by data originators and shared directly with data processors (needs must sharing of data). Processing controls have been established that will ensure no manual or automated processing of vehicle registration numbers (beyond anonymisation as may be needed to create materials for dissemination) or peoples faces (beyond anonymisation as may be needed to create materials for dissemination).	FAIR STATUS: RESTRICTED DATA PUBLIC/RESTRICTED: RESTRICTED DOIs: No DOIs (not findable) PRESERVATION PLAN: Retained under GDPR by separate partners data retention and preservation strategies with shared project related storage under joint control
DMPDS12 - website analytics for reporting to funders	Website visitor analytics data and records. Data is held by Google Analytics with servers accessible to the US.	FAIR STATUS: RESTRICTED PUBLIC/RESTRICTED: RESTRICTED DOIs: No PRESERVATION PLAN: removal upon data retention period expiry - maintained by WP6 leaders



Dataset Name(s)	Data formats and repository location	End of project data summary table
<i>DMPDS13 - Collated Survey Data from the use case regions citizens - behaviour</i>	<i>Surveys using third party tool, Qualtrics is GDPR compatible acting as a data processor under direction of a project participant organisation (TUD). Qualtrics allow configuration such that data will be stored within the EEA region. Data stored does not contain PII so is low threat not requiring specific DPIA for privacy, transfer or onward processing. The data is held by Qualtrics at point of capture in server persistence with access by TUD in XML export formats. Data will be taken from the Survey responses and shared to selected project participants who will each hold the data for processing related to the project work as the data lacks PII no processing controls are required. The finalised data will be made available for project participants in a secure EEA based environment.</i>	<i>FAIR STATUS: FAIR/RESTRICTED</i> <i>PUBLIC/RESTRICTED: PARTIAL</i> <i>DOIs: DOIs on FAIR released materials</i> <i>PRESERVATION PLAN: Retained under GDPR by separate partners data retention and preservation strategies</i>
<i>DMPDS14 - Collated Survey Data from the use case regions citizens - mode choice</i>	<i>Surveys using a third party tool, LimeSurvey, LimeSurvey is GDPR compatible when using its data storage in Germany. Data stored does not contain PII so is a low threat not requiring specific DPIA for privacy, transfer or onward processing. The data is held by LimeSurvey at point of capture in server persistence with access by TUM programmatically. Data will be taken from the Survey responses and shared to selected project participants who will each hold the data for processing related to the project work as the data lacks PII no processing controls are required. The finalised data will be made available for project participants in a secure EEA based environment.</i>	<i>FAIR STATUS: FAIR/RESTRICTED</i> <i>PUBLIC/RESTRICTED: PARTIAL</i> <i>DOIs: DOIs on FAIR released materials</i> <i>PRESERVATION PLAN: Retained under GDPR by separate partners data retention and preservation strategies</i>

Table 4 - PHOEBE dataset formats and repository information. Highlighted rows contain potential PII data with controlled needs only sharing between partners [This table was updated throughout the project life without further change from March 2026].

When datasets contain PII they necessitated following defined processes to control access and further processing. These data 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 or video surveyor camera data containing faces and registration numbers of vehicles)
- Telemetry data (containing journey paths and times relating to individuals)
- Questionnaire, survey and interview data or commentary (including participant details and preferences)

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

Special consideration was put in place to ensure data captured maintains data protection, when performing new data creation or gathering (**DMPDS5**), these considerations are detailed more in T5.4.2 and T7.4.2. This consideration ensured that **PII** is consented for release/reuse/transfer or redacted/removed 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. The approaches follow not only GDPR good practice but also the amended updates of the European Data Protection Board (EDPB) guidance materials as may be introduced from time to time. 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 - these established a record for GDPR data retention targets
 - Data transfers - these established 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. Despite this Standard Contractual Clauses (SCCs), adequacy decisions, transfer mechanisms and cloud hosting locations where required are still reviewed.
 - 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	No	Use of secure project repository and project communications. Each partner is seperately accountable for its security measures	ALL

Table 5 - GDPR and AI processing article 30 register for processing and AI tasks related to the PHOEBE project.

This register can be used to present records of project related processing and AI 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:

SCREENING QUESTIONS - if the answer 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 decisions 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 6 - 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.

It should be noted that review within The PHOEBE framework does not include full sector specific laws that may apply to data origins that may also require consideration at the point of origin software and systems, e.g. under regulation like DORA and CRA that only applies to sector specific areas.

2.3 AI processing and record keeping

Given new requirements (during the project life) and good practice maintaining records for AI processing with suitable review of risk and safeguards new registers were added (NOV 2024) to track AI usage and controls across the project work. These additions satisfy EU AI ACT and EU Data ACT needs as well as general good practice recommendations to maintain records and review risks across AI tasks.



PHOEBE AI Register

OWNER

FLOWW

LAST UPDATE 20-Nov-24

DETAILS

This register describes AI or AI like systems that may be used in the project work to ensure record keeping and review of AI systems. This includes approaches that provide prediction, estimation, models, automated analysis or other areas that may or not include AI algorithms. This register aims to capture risk levels and any needed mitigations for any such system, program or tool usage to access where it may have any impact upon individuals, the environment or wider

AI REGISTER CAVEAT

Despite this register each partner is separately has its own responsibilities under the EU AI ACT and EU DATA ACT that may pertain to AI management. This register creates a record indicating ownership of AI system and project based risk reviews and mitigations. The AI system owner and responsible party may have additional details about AI systems beyond this register in its own compliance activities. Each partner is separately accountable for AI system usage and any risks this may bring.

ARTICLE 30 REGISTER

AI SYSTEM OWNER AND RESPONSIBLE PARTY(S)	AI SYSTEM AND USAGE	TYPES OF PERSONAL DATA *	POTENTIAL IMPACTS OF AI PROCESSING IMPACTING INDIVIDUALS / ENVIRONMENT / SOCIETY	RISK LEVEL FROM AI IMPACTS	SPECIFIC MITIGATION MEASURES FOR AI PROCESSING OR ITS OUTPUTS
IRAP	AI meeting notes (Microsoft Teams Pro) - used in meetings to capture records of some project meetings for use strictly within the project coordination, running and record keeping.	PII - names and connected informations about individuals in connection to the PHOEBE project.	Automated approaches may capture in part or full additional details about meeting participants mentioned within meetings that can be captured in meeting records. All meeting records are used within the confines of the collaboration agreement and the project contract including its terms for protection and confidentiality.	LOW	Outputs are reviewed by humans and used only within the project activity subject to confidentiality.
IRAP	RAP risk assessment models - using road feature data and models as developed and changed in the course of the project. System outputs indicate estimated risk potential, fatal and serious injury estimations and recommendations for interventions to reduce harm on road networks.	No PII data - processing exempt from GDPR	Assignment of estimated risk to networks may influence change programs on road networks which can impact citizens safety positively and changes to the public realm.	LOW	Outputs are reviewed by humans before any changes are made that may impact fundamental human safety or the built environment. (Positively)
NTUA	YOLO (You only Look Once) algorithm provides means to perform object detection on imagery data to aid image analysis and data gathering tasks. This is used in PHOEBE to understand road safety near miss scenarios and potentially counts, trajectory or traffic components by mode from fixed camera locations in use case regions.	Video data - that may contain vehicle registration number (graphically - not extracted or processed) and human faces (graphically not extracted or processed)	Imagery contains PII in terms of faces and number plates as well as times of movement. Despite this faces and number plate details are not stored processed or output to be used in the project. The output data can be used to understand locational behaviours without reference to individuals. Output data is used in research work, model development and risk estimation in use case regions that could impact future risk mitigations in the regions of application.	LOW	Outputs are reviewed by humans before any use in scientific, model or other work. Any changes informed by such data are made by humans albeit they may impact fundamental human safety or the built environment. (Positively)

Table 7 - Example of the AI register tracking AI usage in support of the PHOEBE project and review of the risks for such usage. All risks are regarded as LOW (MARCH 2026).

2.4 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.

2.5 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 was supported within WP2 and will be included in the D2.1 and D2.2 reporting deliverables to enable continuous tracking. These tracking efforts extend into WP5 activity and are reported in WP7 data management deliverables. Deliverables (particularly WP2) 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.

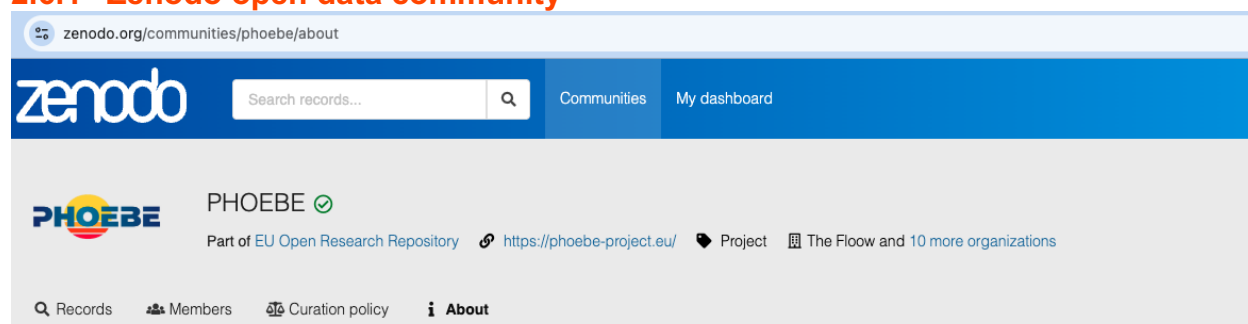
2.6 Making data ‘findable’

Activity under WP2 (detailed in D2.1) includes 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, or on public open data communities like Zenodo) 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).



2.6.1 Zenodo open data community



This community and its members collate research data and materials in relation to the **PHOEBE project** to ensure onward scientific usage support **FAIR** principles. It contains data and outputs in relation to the scientific and use case work in the project. Data may concern:

- Gathered data collated for the project
- Output data related to scientific work
- Deliverables or reports may be included when useful for public dissemination and to further fair principles

For more details about the project, its aims, news and updates please see <https://phoebe-project.eu/>

Details about data are held in the following resource <https://doi.org/10.5281/zenodo.16737146>

Figure 1 - Zenodo open data community which details both deliverables and open data from the PHOEBE project.

To support the project with findable data an open community has been setup which enables open sharing of public resources in the project. This is found at <https://zenodo.org/communities/phoebe/> this contains open registers of data used in the project as well as open resources for all public deliverables and data. To aid findability metadata is added about each resource to aid in findability.

To support findability the PHOEBE Zenodo community has been recognised as party of the official outputs as a sub part of the 'EU Open Research Repository'. Also to support findability DOIs have been established to make a globally unique URI for each recorded item held within the repository. Each published work is linked to all relevant affiliated organisations using Research Organisation Registry listings (ROR) where available. Published items are also linked to authors via ORCID to recorded related works to each assigned author. In all cases the materials available are linked to funded grants that backed project work generations using the project grant ID (101076963) as well as UKRI UK partner funding grant numbers. Where fitting the nature of resources standardised keywords and indexing terms are used to support findability. These include the use of 'GEneral Multilingual Environmental Thesaurus' (GEMET) tagging to help identify resources to areas such as 'Road Safety'. Each resource and the repository links to alternative stores where applicable for project information and also the project website and where helpful is also linked to social media connections e.g. to linkedin via (<https://www.linkedin.com/company/phoebe-project/>). The findable nature of the project was also enhanced with direct links to alternative listings such as OpenAIRE across deliverable content uploaded. These best practices extend beyond the guidance of the current 'Open Science recommendations'.

2.7 Making Data openly accessible

All project data was 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 is held by individual partners prior to aggregation or anonymisation for use in the project.

Shared data is openly available to project partners via the project repositories (website and Zenodo), or the shared drive folder, which is authorised for use by all project participants only. 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 risk framework and modelling, these will be available in the project as needed even if not suited to open sharing due to proprietary platforms. In some cases, data with PII are utilised to aid data protection and data minimisation principals shared only following GDPR data processing guidelines and on a need only basis with minimal individuals to minimise risk exposure of protected or sensitive data.

The register of data and its accessibility attributes is openly published in the following register <https://doi.org/10.5281/zenodo.16737146>.

2.8 Making data interoperable

The project sought to use standard file formats and naming conventions to ease interoperability. The collection of metadata followed a single approach, as detailed in D2.1. This process was supported by WP2 activity throughout the project and in WP7 and WP5 activities following the end of WP2 activity to maintain good data practices in later work. To aid data reuse metadata about resources are utilised to help organise and inform on content these use the DataCite Metadata Schema. This approach uses baseline Dublin Core concepts linking to resource type categorisations (e.g., dataset, image, software, publication, interactive resource). These help support interoperability.

2.9 Making data re-usable

Within the project a range of tasks specifically sought 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. To support re-usability license controls are added on Zenodo content with a strict focus (where not prevented) on Creative Commons Attribution 4.0 International license to facilitate open reuse. For individual data releases internal usage always occurred first before open release to ensure verification, testing and active usage such that data quality is assured. To also support reuse of data where needed details and guidance about individual data is also included to aid future reuse.

2.10 Final data legacy and preservation

For each data set each has been considered in terms of its longer-term reuse and retention for further use and impact. These are each now detailed below.

Dataset	Preserved?	Repository	Retention
DMPDS1 DMPDS2	No, not public. Preservation in partners as per individual retention and data handling controls to protect PII.	Contractually and privacy restricted	Partners may retain some material as per individual organisational data protection controls (not shared).



Dataset	Preserved?	Repository	Retention
DMPDS3 DMPDS4 DMPDS5 DMPDS6 DMPDS7	Yes	Zenodo (prime source and register of all sources - with available data referenced by DOI or URI)	Long-term
	Yes	Zenodo registers in some cases link to materials available already from third party locations referencing original source materials via originator repositories.	Long-term
	Yes but gated	Some (limited) data sources are available upon request only to protect IP and commercial sensitivities for project partners. Locations and contact detailed in Zenodo.	Long-term
	Yes but no public access	Some data sources are indicated as proprietary and are not shared albeit preserved by individual partners for protected reuse.	Long-term (but retention can be variable)
DMPDS8 DMPDS9	Yes	KPI outputs in use cases	Long-term
	Partial	Test and validation data (some when supporting publications and reports is shared but others in proprietary or temporary formats is not shared and does require longer term preservation past point of consent and continued data utility)	Various
	Yes but no public access	Detailed model outputs in model proprietary formats	Various but not publicly shared
DMPDS10	Yes	Project website (https://phoebe-project.eu/)	3 years from project end
	Yes	Publications (OpenAire+Zenodo+wider)	Long-term
	Yes	Social media (LinkedIn)	Long-term
	Yes	Presentations	Various - via websites for prior events

Dataset	Preserved?	Repository	Retention
DMPDS11	No	Privacy restricted for contained PII	Partners may retain some material as per individual organisational data protection controls (not shared).
DMPDS12	No	Privacy restricted with access to WP6 lead partners only	Rolling 26 months
DMPDS13 DMPDS14	Yes but no public access to full results (containing PII)	Partial - Full data withheld due to PII of participants. Extracts are released via Zenodo without PII.	Long-term

Table 8 – Final data and legacy table detailing the longer-term preservation and persistence of project materials.

To encourage reuse all materials preserved in Zenodo are released under Creative Commons Attribution 4.0 International license to facilitate open reuse.

3 Allocation of Resources

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

3.1 Data Management Plan – related deliverables

The DMP was 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 explored related literature and the state of the art. The review helped set the data expectations for the project including in the areas of data management.
D1.2	Theoretical principles and methodological approach of the PHOEBE framework and selection of tools	TUD	D1.2 directly informed the principles for expected processing and identified the data required in the project subject to management under the DMP. This work led to refinement of the DMP.
D2.1	Consolidated data requirements and use case region data availability report	FLOOW	D2.1 solidified data requirements and owners, as well as requirements that may restrict the accessibility of the data.

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
D2.2	Data register, feature report and accreditation	FLOOW	This register detailed all data used in the technical project delivery subject to the DMP. The register also documents conformance for use in framework models. The register helps to make data 'findable' by documenting suitable metadata and forms a long-term index for project data.
D3.1	New and enhanced models/simulation environments and user support materials (Beta ed.)	iRAP	D3.1 identified and defined the 'data consumer's needs from stored data to enable new and enhanced models. These placed 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 detailed the finalised models and risk framework, part of which included documenting the ongoing needs and accessibility of the data managed by the DMP.
D4.1	Use case experimental designs	EIRA	This activity defined the specific data needs for each use-case region, as well as relevant scenarios. The DMP was modified to document required data in particular new data additions the project needed.
D4.2	Consolidated use-case evaluation and assessment report	EIRA	This evaluation helped to establish the impact of data in support of validation and assessment of the work in each region.
D5.1	Consolidated PHOEBE framework methodology, network-level demonstration results and tools	NTUA	This demonstration framework detailed the data needed for dissemination (DMPTask 10).
D5.2	User interface and implementation	POLIS	This interface details needed dissemination, which is documented under DMPTask 10.
D6.1	Communication, dissemination and exploitation plan	POLIS	This detailed the plan for dissemination and communication beyond the project supporting wider dissemination (DMPTask 10) for which data retention and persistence of materials was considered.
D6.2	Final exploitation, IPR and replication plans	FC	This detailed exploitation plans, registers and materials that required data management. This deliverable supported DMP aims to maintain data after the project ends (DMPTask 10).
D7.1	Project Management Handbook	iRAP	This document defined 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.



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
D7.2	<i>Data Management Plan (initial)</i>	FLOOW	<i>The original (DMP) version - legacy.</i>
D7.3	<i>Data Management Plan (final)</i>	FLOOW	<i>This document (DMP) most recently released as D7.3 - the final version.</i>
D7.4	<i>Ethics Management Plan</i>	FLOOW	<i>This document should be read alongside the DMP; it contains the ethical management plan for the project and its delivery.</i>

Table 9 - 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 (D7.4). The ethical management plan was also subject to continuous update and should be considered alongside the DMP. Additions in the project life beyond its first version included reviews for new regulation as well as reviews for the use of new data such as video footage that contained public realm imagery of people and vehicle movements.

5 Risk Aspects

Risk management related to data was handled throughout the project and remains captured in the project risk register (D7.1). Risks related to data access were raised and closed in the life of the project without impact on the overall delivery.