D7.1: Data Management and Ethics - Version 1

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101069782

Project & Document Information

Grant Agreement No	101069782	**Acronym**	URBANE
Project Full Title	UPSCALING INNOVATIVE GREEN URBAN LOGISTICS SOLUTIONS THROUGH MULTI-ACTOR COLLABORATION AND PI-INSPIRED LAST MILE DELIVERIES		
Call	HORIZON-CL5-2021-D6-01		
Topic	HORIZON-CL5-2021-D6-01-08	**Type of action**	IA
Coordinator	INLECOM INNOVATION		
Start Date	01/09/2022	**Duration**	42 months
Deliverable	[D7.1]	**Work Package**	[WP 7]
Document Type	[R]	**Dissemination Level**	[PU]
Lead beneficiary	INLE		
Responsible author	Maria Kampa (INLE)		
Contractual due date	[28/02/2023]	**Actual submission date**	[28/02/2023]

Disclaimer and Acknowledgements

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101069782

Disclaimer

Copyright message

Authoring, Revision & QA Information

Deliverable Contributors	
Contributor Name	**Organisation (Acronym)**
Maria Kampa	INLE
Makis Kouloumbis	INLE
Ioanna Fergadiotou	INLE

Version History				
Version	**Date**	%	**Changes**	**Author**
0.1	[01/12/2022]	5%	Wrote the ToC	INLE
0.2	[20/12/2022]	50%	First Consolidated version	INLE
0.3	[10/1/2023]	80%	Input from WP leaders	KLU, ITL,FIT, CERTH, EITUM, POLIS, INLE
0.4	[20/11/2023]	90%	Incorporate input from LLs	INLE
0.8	[31/1/2023]	100%	Deliverable ready for review	INLE
0.9	[24/02/2023]	100%	Addressed comments in peer review	INLE
1.0	[28/02/2023]	100%	Submitted final version	INLE

Quality Control (includes peer & quality reviewing)			
Date	**Version**	**Name (Organisation)**	**Role & Scope**
[07/12/2022]	0.1	Efstathios Zavvos (VLTN)	QM ToC Approval
[17/02/2023]	0.8	Reviewed by Open Science Team (UOC)	Review
[28/02/2023]	0.9	Reviewed by QM and PC	Review

Executive summary

The current document's goal is the development of a Data Management Plan (DMP), considering the relevant parameters as established in the URBANE Grant Agreement. The relevant guidelines that need to be followed in order to ensure that the FAIR principles are met, have been also developed as part of Section 4 of the current deliverable.

The DMP defines the data lifecycle and governance and outlines the strategy for participating in the Open Data Research Pilot. The intention of the URBANE project is to publish no confidential results under Open Access, regarding all scientific publications produced along the project lifecycle. Moreover, the document describes the different datasets generated and collected within the scope of the project activities as well as the methodologies and standards to be followed in order to ensure their protection, security and confidentiality.

In addition to the above, the current document introduces the privacy and ethical policies within the project lifespan as well as after its completion. Various mechanisms to protect identities and sensitive information will be enforced as a part of the data management actions. Finally, special attention is paid to the ethical usage of AI into to the scope of the project as well as any gender issues that should be taken into account.

The DMP will remain a living document throughout the project's lifespan (+add official follow up deliverables). The present first version may evolve during the project according to the progress of project activities.

Contents

List of figures

List of tables

Glossary of Terms and Acronyms

TABLE 1 GLOSSARY OF ACRONYMS AND TERMS.

Acronym / Term	Description
AI	Artificial Intelligence
DMP	Data Management Plan
DoA	Description of Action
DOI	Digital Object Identifier
DPO	Data Protection Officer
EC	European Commission
EEA	European Economic Area
EU	European Union
FAIR	Findable, Accessible, Interoperable, and Reusable
GA	Grant Agreement
GCP	Good Clinical Practice
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol Secure
ICT	Information Communication Technologies
ID	Identification Document
PII	Personally Identifiable Information
PU	Public
SEN	Sensitive
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WP	Work Package

1 Introduction

1.1 URBANE Outputs Mapping to GA Commitments

Purpose of this section is to map URBANE's Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

TABLE 2 ADHERENCE TO URBANE'S GA DELIVERABLE & TASKS DESCRIPTIONS

URBANE GA Component Title	URBANE GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D7.1 Data Management and Ethics - Version 1	Report covering ethics, gender issues, and data management issues – updated continually. First version of Data Management Plan will be submitted on M6, and will be updated on M 18 and M36. Final DMP will be submitted on M42	*Chapter 2, 3,7*	*The current deliverable after outlining the data lifecycle and the datasets collected per WP, provides specific guidelines for ensuring the FAIR principles are followed. Next, the ethics and GDPR aspects of the datasets of the project are presented in Chapter 7 including specific sections for the AI usage in the project as well as gender issues that may arise.*
TASKS			
Task/Subtask # & Title	*Respective **extract** from formal Task/Subtask Description*	*Respective Chapters or Sections **numbers** within this document addressing GA described Task/Subtask*	*Briefly outline how addressed the respective document section(s) cover the described GA Task activities*
	In this task, the ethics requirements, the data management policies, and the data protection policies will be defined in accordance with the current EU data protection regulations (General Data Protection Regulation), the European Code of Conduct for	Chapter 2,3,7	Taking into account the relevant legislation, this project introduces the ethics guidelines that should be followed throughout all the project activities. Moreover, the GDPR aspects are analysed. The partners national legislation is

	Research Integrity and national regulations in the URBANE partner countries. The ethics requirements will ensure compliance with the above-mentioned regulations, aiming at identifying potential ethical issues in the project and in providing ethical guidelines especially with regards to applied AI, including gender policies, to be followed to ensure that the research is conducted at the highest level of integrity, quality and transparency. D1.7 will consolidate decisions on the use/development of AI software in relation to the freedoms and personal rights of the human subjects involved such as profiling and tracking of individuals through collecting and processing of personal data.		not analysed as a unique GDPR policy has been created for the purposes of the project and should be followed by all partners. Finally, in chapter 6.4 specific provisions for the usage of the AI in the scope of the project. More specifically, the personal data legislation related to the AI software development of the project.
	The data management and ethics plan will describe the data life cycle for the data to be collected, processed and generated in URBANE;	Chapter 2	Chapter 2 presents the data governance and lifecycle related to the project datasets. It presents an overview of the data collected and generated throughout the different WPs.
	information on the handling of research data during and after the end of the project; what data will be collected, processed and/or generated; which methodology and standards will be applied;	Chapter 3	Chapter 3 introduces the guidelines that need to be followed in order to ensure that the FAIR principles are met. It also provides an overview of the relevant methodologies and standards that need to be taken into account in relation to the data storage, access, security, prevention and confidentiality.
	whether data will be shared/made open access and how data will be curated and preserved (including after the end of the project).	Chapter 3,4	Chapters 3 & 6 2 include the relevant information on the data storage, archiving and preservation throughout the project as well as after its end as

			well as the relevant security aspects. Chapter 4 deals with issues related to open access of the research outputs.
	The plan will evolve during the lifetime of the project to present the status of the project's reflections on data management and whenever significant changes arise.	Chapter 8	As anticipated in chapter 8, the DMP will be updated regularly and as an official deliverable it will be resubmitted close to the end of the project

1.2 Deliverable Overview and Report Structure

The structure of the current document adheres to the EC's FAIR data management template. The document is structured as follows:

- Chapter 1 is the introductory section to the deliverable highlighting its relevance to the GA relevant descriptions and introducing an overview of the deliverable and its structure.
- Chapter 2 provides an overview of the data lifecycle and specific guidelines for each step as well as a summary of the data collected and generated throughout the project.
- Chapter 3 presents the guidelines in order the project to follow the FAIR principles, as well as specific processes to be followed in that respect.
- Chapter 4 explains how the research outputs should be handled.
- Chapter 5 explains the Allocation of resources and the roles of the different partners within the URBANE Consortium about the DMP responsibilities.
- Chapter 6 discusses the methodologies and standards for the data security, access, storage and confidentiality aspects.
- Chapter 7 outlines the ethical aspects of the different project activities as well as the personal data protection measures.
- Chapter 8 concludes the deliverable.

2 Data Summary

The definition of data collection concepts and data purposes as they relate to the project's work-breakdown structure is the first step in preparing a DMP. The purpose of this section in this context is to define the means of data collection, the format of data collected, their origin, and any other information deemed necessary.

The input information is collected through a questionnaire circulated for input to all URBANE partners (available in Annex II).

In this regard, what follows is an overview of the data governance and lifecycle, followed by a detailed description of the data produced or processed for each of the URBANE WPs.

2.1 Data Governance & Lifecycle

Data Governance is defined as "the organization and implementation of policies, procedures, structure, roles, and responsibilities that outline and enforce rules of engagement, decision rights, and accountabilities for the effective management of information assets." [1]

In this regard, the URBANE Data Governance in URBANE serves two primary purposes:

a) Provide a mechanism for the control of changes to data, data processes, and data architecture, as well as connectivity, storage, and data sharing. The Data Protection Officers exercise and monitor governance. All project partners have complete control over how the project data is managed, accessed, and stored, as well as how this data is disseminated via ORDP, as this will apply to specific data sets that will be identified.

b) establish rules and policies for identifying and resolving data-related issues, involving processes, resources, specific content, and stakeholders. Because data can and must be shared, they must provide necessary metadata information such as data definitions, data types, and change tracking, data compliance, data quality procedures, and metrics.

In order to better understand the Data Governance in the project, it is also important to first have a better overview of the data lifecycle. The entire data lifecycle occurring in the project is described and analysed in this section. This means that the various stages at which data will be generated, managed, or processed during and after project execution are analysed.

In this regard, in the following sections, an analysis of the data lifecycle as well as high level measures for controlling, managing, and reporting on the related data are presented. An indicative typical data lifecycle is presented in Figure 1, without excluding any alternative data flows if needed during the project execution. The specific methodologies for ensuring the FAIR data management principles are respected have been included in section 3.

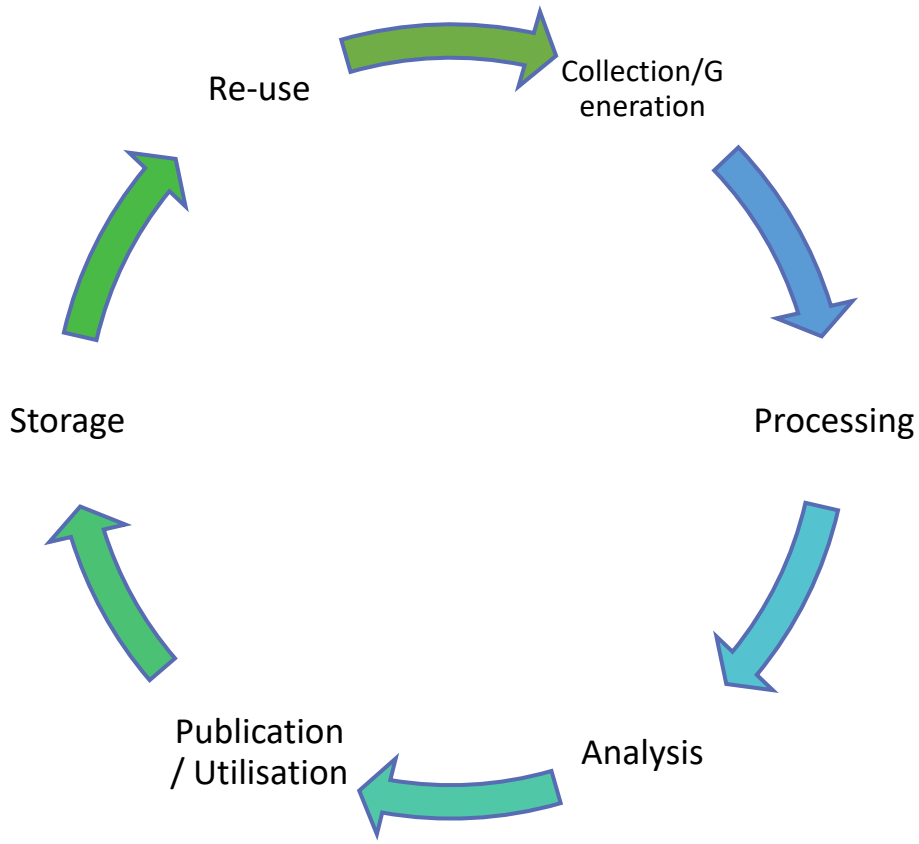

FIGURE 1 DATA LIFECYCLE

2.1.1 Creation/Generation

The data creation process is initiated with the data generation and/or collection, which is closely connected with the various data generated during project activities, as detailed in section 2.4. This step primarily refers to the data generation by each data owner as well as the collection of this datasets for further processing by the rest of the URBANE Consortium in the context of the execution of the project activities as described in the DoA. It is important to highlight that that this data must be collected in a structured manner and in appropriate formats and layouts in order be easily further processed.

In the table below, specific guidelines have been developed to ensure compliance with the applicable rules.

Topic	Guideline -Means to ensure compliance
Format	Compliance with existing standards of data exchange
Availability and Readability	Whole package of data available, non-corruption, whole percentage collected (e.g., verifiable by hash functions)
Fit for Use	Data follow data compliancy for proper processing and review
Consistency and Completeness	Data are consistent and complete for the intended purpose
Relation	Data following a precise relation to their purpose

2.1.2 Processing and Analysis

The second stage of the data lifecycle includes the actual data processing by all data processors who in the case of URBANE are the project partners and who will be granted access to the datasets for distribution in accordance with the project's activities assigned to them. To meet the project's objectives, the appropriate partners should be able to process data needed quickly. This stage includes all steps toward data verification, organization, transformation, integration, and extraction for the intended application. Data analysis encompasses all procedures/actions performed on real data to characterize existing facts, recognize patterns, generate data explanations, and so on. This stage works closely with the previous one.

In the table below, specific guidelines have been developed to ensure compliance with the applicable rules.

Topic	Guideline -Means to ensure compliance
Data logic	Data can be and are processed following a concise logic and approach
Organization and Utility	Suitable content organization of data under processing
Validation	Ensuring that the data under processing are correct and relevant
Aggregation	Whenever multiple data need to be aggregated ensure that this is done in a concise approach
Transformation	Transformation of data to the proper format(s) for processing
Calibration	Calibration of data for their intended purpose

2.1.3 Publication and utilization

The data publication actions are primarily concerned with the ability to share datasets openly, whereas utilization includes the steps that the project must take internally in order to be able to do so. This implies that the data should be independent so that the transfer can be done either automatically or manually. To ensure the security of private data as well as the integrity of the data itself, it is critical to ensure that the data is shared with the necessary regulating mechanisms at every stage of the project.

Regarding the use of metadata, the Consortium needs to also ensure that they can be easily accessible, so the current stage as well as the next one (data storage and archiving) which are closely related (as another feature of the FAIR data treatment-see section 3 for more details).

In the table below, specific guidelines have been developed to ensure compliance with the applicable rules.

Topic	Guideline -Means to ensure compliance
Means-independent	Transferring of the data in a means-independent approach
Security (a)	Data stored in a secure server or locally in case of sensitive datasets

2.1.4 Storage, Archiving and Re-Use

The storage and archiving stages are also critical for data access, sharing, storage, archiving (including search capabilities), and re-use. The frequent state of the data update, which ensures that no newer versions is available, is an important consideration in this step. This will include safeguarding against unintentional data loss, corruption, and access. Data reusability, which is a component of FAIR data handling, is inextricably linked to data storage and archiving.

In the table below, specific guidelines have been developed to ensure compliance with the applicable rules.

Topic	Guideline -Means to ensure compliance
Up to date	Ensuring that the stored data are up to date for the specific purpose and no later version exists
Meta Data	Existence of meta data in stored files
Security (b)	Access control provided
Security (c)	Server is considered as safe enough (TLS connection protocol)
Bandwidth	Control of server bandwidth
Expiration	Properly setting expiration dates for all data after which the data will be deleted

2.2 Purpose of the Data Collection/Generation and its relation to project objectives

URBANE will support the transition path towards effective, resilient, safe and sustainable last mile transport, through four Lighthouse Living Labs in Helsinki, Bologna, Valladolid and Thessaloniki, that will demonstrate TRL8 efficient, replicable and socially acceptable innovative last mile delivery solutions [Wave 1 LLs], building on existing TRL>5 assets. Hands-on lesson learning at European level will be primarily facilitated by the URBANE Innovation Transferability Platform comprising Digital Twinning Tools, open models, smart contracts governed by blockchain technology and a data-driven Impact Assessment Radar that will enable the adaptation and replication of Wave 1 solutions in two Twinning LLs in Barcelona and Karlsruhe [Wave 2 LLs], demonstrating their own solutions within the course of the project. URBANE's commitment to upscaling is further strengthened by the engagement of six early adopters (Follower Cities) in innovations' adoption feasibility studies, thus stimulating the formulation of new LL communities across Europe.

A project key building block thus, will be the development of an open Digital Twin (DT) infrastructure for urban logistics, advancing the LEAD project DT platform, enabling city and industry actors to take decisions on the preferable delivery solutions to be implemented. The approach employs social simulation tools to experiment with possible strategies and business models, aiming at boosting end-user adoption and increase investors' confidence.

URBANE gathers a multidisciplinary team of 41 partners collectively working in the project LLs, endowed with the experience and outcomes of over 20 reference projects, to co-design innovative last mile delivery

solutions, implement interventions with significant impact and deliver tools for the quick adaptation and replication of successful models. The successful introduction of innovations such as robots in last mile delivery, requires restructuring the entire last mile ecosystem. Consensus building among private-sector and public-sector stakeholders from the regional level to the street level is critical to this transformation. The project is driven by the LLs logistic communities needs and the concept is structured around five innovation pillars (organised in respective WPs), integrated through continuous feedback loops and supported by technology enablers (blockchain, modelling and Digital twining technologies, AI-driven optimisation) (Figure 3).

The ambition is to enable replicability; therefore the project introduces a methodological approach that starts by defining target innovations, capturing knowledge in reusable models, refining the user stories and setting collaboration governance rules across local value chains, testing innovations in real-life environments following a co-creating approach with the support of digital twinning tools and, accelerating the adoption and scale-up of successfully demonstrated last mile delivery models.

URBANE will enable the establishment of collaborative communities, governed through safe and trustful white label collaboration schemes (blueprints, adaptable to local dynamically evolving last mile ecosystems), comprising a) Legal contracts and their digital blockchain-governed counterparts, b) Open collaboration governance principles with documented ecosystem onboarding processes, b) Neutral orchestration governance models to support the consolidation of assets/goods and smooth collaboration among stakeholders at different levels - shippers, last mile service providers, authorities and space management stakeholders, d) Connectivity and smart readiness assessment tools to ensure that digital infrastructure is in place and to guarantee that data is shared in a safe way.

2.3 Types and Formats of the collected/generated data

During the creation, the consortium identified the following data categories:

- qualitative and quantitative research type of data (experiment outcomes, sensor network and IoT data, existing LL last-mile logistics network & infrastructure data, city & municipality last mile logistics data, business relations etc)
- administrative type of data (participants details, communications, etc.);
- open-source type of data collected from publicly available sources (socioeconomic, literature, city authorities interests etc);
- publication and dissemination type of data included to open peer-reviewed publications, interviews, reports, proceedings.

In this scope, the general categories of the data that are going to be available into the scope of the URBANE project are the following.

- Administrative information about the consortium: Personal information about the consortium members, such as name, surname, email, phone number etc. will be handled and stored in the Microsoft Share Point repository accessed only by the members of the consortium. In this context, the said space can be characterized as private and secure.
- Project internal information: Information gathered from meetings, workshops, and any type of internal communication which will be protected according to each required level of confidentially. Fruitful and general outcomes of the project will be disseminated without restriction if no

sensitive data are disclosed. In case of confidential discussions or outcomes access will be granted only to partners that require such for the execution of the project activities assigned to them.

- Research activities: During research that necessitates the collecting of data, the relevant entity will retain and safeguard the data locally. To protect the rights and freedoms of the data subjects, appropriate organizational and technical measures, such as anonymization and/or encryption techniques, will be used. Moreover, open-source data will be collected that will be used as the basis to the project research activities.
- Testing: The Consortium partners will retain and manage data about the testing participants and the processed data. Such testing's results will be reported in an anonymous manner. It needs to be noted that the relevant entity responsible for the tests will retain and safeguard the data locally, and to protect rights and freedoms of the data subjects, ,appropriate organization and technical measures will be used.

The detailed datasets description to be generated/ processed on WP level is presented in Section 2.3. below. The expected size of the datasets to be generated/ used n the URBANE project will be below 1GB each.

Since the present is delivered in an early stage of the project activities, the second version (D7.3) of the Data Management Plan is foreseen to be delivered close to the project end in Month 42 in order to give a clearer and complete overview of the generated and used data and cover any gaps that exist in the current version.

Finally, INLECOM will ensure that the DMP will be updated by partners over the course of the project whenever significant changes arise and at least every 6 months in order to ensure that new datasets or changes in the relevant policies will be tackled.

2.4 Data handled by each WP

2.4.1 WP1

	Data/Metadata Description	Personal Data identification	Data Origin	Data Format	Purpose of data collection	Data sharing - Access	Procedures to safeguard data	Openess - Reusability	Storage	Retention Period
ID1.1	Contact details collected for internal communication purposes	Y	Public Sources	Spreadsheet, CSV, text	Execution of task activities for Work Package 1	Internal-Consortium partners with valid justification for processing this dataset	anonymization	Other studies in logistics domain	Servers at KLU, VLTN, SKEMA, Teams Collaborative space	at the latest until the end of the project
ID1.2	Research and Commercial data on Urban Logistics Innovations	N	Academic, EU, Commercial publications	Text in MS Word and Excel and/or PDF	Execution of task activities for Work Package 1	Analysis will be accessible to the public per project GA in D1.1	Data security rules of KLU, VLTN, SKEMA – Data is already public so no further access security envisioned	Reference for researchers	Servers at KLU, VLTN, SKEMA, Teams Collaborative space	at the latest until the end of the project
ID1.3	Personal contact details for dissemination activities	Y	Public sources, project interviews, project meetings	CSV, Excel and/or Outlook	Execution of task activities for Work Package 1	Internal-Consortium partners with valid justification for	authentication mechanism	Other studies in logistics domain	Servers at KLU, VLTN, SKEMA, Teams Collaborative spec	at the latest until the end of the project

						processing this dataset				
ID1.4	Information on prior successful and not successful collaboration schemes	N	Questionnaires	MS Word and Excel	Execution of task activities for Work Package 1	Internal-Consortium partners with valid justification for processing this dataset	authentication mechanism	Reference for researchers	Servers at KLU, VLTN, SKEMA, Teams Collaborative space	at the latest until the end of the project
ID1.5	Data about Logistic Service providers: fleets, types delivery vehicles, aggregated data of deliveries to be made in time, per city, type of parcel, type of delivery requirements	N	Logistic Service Providers, city authorities	CSV, Excel and/or MS Word	Derive basic business models for city authorities and logistic service providers as well as incentive schemes and city development plans.	Data to be shared with partners in T1.2 and with partners in T3.5 and T5.2, T5.3	anonymization	None: will not be used or published for other purposes than those authorized within the project.	Servers at KLU, VLTN, SKEMA, Teams Collaborative space	at the latest until the end of the project

TABLE 3 WP1 DATA

2.4.2 WP2 -3- 4

The datasets generated/ collected by the project LLs (Wave 1&2) as part of WP2 and 4, will be also processed by the WP3 participants for the implementation of their respective tasks and the development of the URBANE solutions. In this sense, a unique table describing the said datasets has been developed for the aforementioned WPs.

TABLE 4 WP2-3-4 DATA

ID	Data/Metadata Description	Personal Data identification	Data Origin	Data Format	Purpose of data collection	Data sharing - Access	Procedures to safeguard data	Openess - Reusability	Storage	Retention Period
ID_1	Business models, socioeconomic data	Y	LL partners	Documents format including pdf, docx, txt, xls,	Task2.1.	Internal; All partners	Encrytpion, anonymisation	For similar research	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_2	Delivery demand data: Parcel delivery demand dataset including delivery location, volume, weight, time of request, time of delivery requested, type of service (express, signed, specific time window), delivery mode/modal shift) and unsuccessful deliveries for each Logistics Service Provider (LSP) involved in the analysis of the LL.	y	LSP participating in each LL	.xls or .xlsx	Tasks 3.4, 3.5, 3.6: This type of data is essential to estimate parcel delivery demand in last-mile logistics networks. LSPs per LL could be able to provide some of their own dataset (anonymized) .	Internal; WP2/4 and WP3 participants	Anonymisation	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project

ID_3	Supply/service-related data : Service provider fleet specification for each LSP participating in the LL.	n	LSP participating in each LL	.xls or .xlsx	Tasks 3.4, 3.5: This type of data is essential to provide decision support regarding the necessary number of vehicles needed in order to cover the demand in an area under study.	Internal; WP2/4 and WP3 participants	Encryption	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_4	Supply/service-related data : Service provider's facilities locations (warehouses/consolidation centers/hubs/lockers/ pick-up points).	n	LSP participating in each LL	.xls or .xlsx	Tasks 3.4, 3.5, 3.6: This type of data is essential to provide decision support regarding the optimal set-up of facilities in an urban/sub-urban environment.	Internal; WP2/4 and WP3 participants	Encryption	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_5	Supply/service-related data : Charging stations network available to the LSP (if LL intends	n	LSP participating in each LL / Local Authorities	.xls or .xlsx	Tasks 3.6: These datasets can be useful if LLs are interested in	Internal; WP2/4 and WP3 participants	-	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project

	to examine EV usage).				exploring charging opportunities (supply/demand) and possibility of using electric vehicles in their delivery fleet.					
ID_6	Supply/service-related data about Cargo-bikes (services, fleets….)	n	LSP participating in each LL / Local Authorities	TBD	Tasks 3.6: Probably the current task is to identify what / how much data about cargo-bike activity is available to WP3	Internal; WP2/4 and WP3 participants	-	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_7	Urban environment geospatial and network data 1: Road network data, traffic data, distances data and/or travel time data (between locations).	n	Local Authorities / Local dedicated websites with open data	.xls or .xlsx	Tasks 3.4, 3.5, 3.6: This type of data is essential to provide decision support regarding most efficient/optimal assignment of vehicles to clients.	External	Anonymisation	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project

ID_8	Urban environment geospatial and network data 2: Cartography, city zones and map data.	n	Local Authorities / Local dedicated websites with open data	.xls or .xlsx	Tasks 3.4, 3.5, 3.6: This type of data is essential to provide decision support regarding efficient/optimal assignment of vehicles to clients.	External		n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_9	City-related data : Census and/or travel patterns data.	n	Local Authorities / Local dedicated websites with open data	.xls or .xlsx	Tasks 3.4, 3.6: These datasets can be used with models that focus on passenger mobility-related decision support, as well as for innovation adoption models.	External		n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_10	Blockchain related data	n	LSP participating in each LL	Text	Tasks 3.3: This data is required to understand how to design the blockchain/smart contract service	External		n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project

ID_11	IoT data: IoT data from sensors deployed at LLs to monitor processes.	n	Local Authorities / Local dedicated websites with open data	anything	Tasks 3.3: This data will inform the decisions of the smart contracts e.g. if temp measurement of a sensor is over a threshold then emit alarm	External		n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_12	EPCIS data: Transport events.	n	LSP participating in each LL	EPCIS server	Tasks 3.3: This data are events during the transport of a cargo from point A to point B such as delay, damaged, reach of POI, arrival, departure etc.	Internal	Encryption	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_13	Demand data: Relationship between the socio-demographic characteristics and demand patterns: % of the population ordering online, frequency, parcel size and weight, delivery	y	LSP participating in each LL / Local Authorities / Local dedicated websites with open data / dedicated studies	xls,csv	Tasks 3.4: Data is relevant to calibrate the ABM - hardcoding how often specific socio-demographic segments order	Internal	Anonymisation	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project

	location (pickup point, home delivery)				different types of parcels					
ID_14	Demand data: choosing a provider: Relationship between the socio-demographic characteristics and importance of delivery cost, delivery method, delivery time, perceived quality of the provider (provider reputation)	n	LSP participating in each LL / Local Authorities / Local dedicated websites with open data / dedicated studies	xls,csv	Tasks 3.4: Data is relevant to calibrate the ABM: Motives for the consumer decision about the service provider	External	Anonymisation	Scientific publications, EC websites	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_15	Demand data: choosing a provider: Relationship between the socio-demographic characteristics and the expected provider satisfaction related to delivery cost, delivery method, delivery time, perceived quality of the provider (provider reputation) - by provider	n	LSP participating in each LL / Local Authorities / Local dedicated websites with open data / dedicated studies	xls,csv	Tasks 3.4 : Data is relevant to calibrate the ABM: Satisfaction of motives for the consumer decision about the service provider	External	Anonymisation	Scientific publications, EC websites	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_16	Demand data: choosing a delivery location type: Relationship between	n	LSP participating in each LL / Local Authorities /	xls,csv	Tasks 3.4: Data is relevant to calibrate the	External	Anonymisation	Scientific publications, EC websites	MS TEAMS (INLECOM Share Point)	at the latest until the end of

	the socio-demographic characteristics and importance of delivery convenience (related to package size and weight), certainty of picking up from location type, last mile delivery method		Local dedicated websites with open data / dedicated studies		ABM: Motives for the consumer decision about the pick-up location					the project
ID_17	Demand data: choosing a delivery location type: Relationship between the socio-demographic characteristics and the expected location satisfaction related to delivery convenience (related to package size and weight), certainty of picking up from location type, last mile delivery method (for home vs pick-up point delivery)	n	LSP participating in each LL / Local Authorities / Local dedicated websites with open data / dedicated studies	xls,csv	Tasks 3.4: Data is relevant to calibrate the ABM: Satisfaction of motives for the consumer decision about the delivery location	External	Anonymisation	Scientific publications, EC websites	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_18	Qualitative data on decision processes: Defining the decisions customers can make, relevant motives (as proposed above) and relationships to the	n	interview/workshop with stakeholders of the LL	interview/workshop with stakeholders of the LL	Tasks 3.4: Data relevant for model definition	External	Anonymisation	Scientific publications, EC websites	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project

	innovative last mile delivery methods									
ID_19	Parcel Market share: Data on the market shares of the couriers.	n	LSP participating in each LL / dedicated studies	xls	Tasks 3.4: Data is to allocate demand to each courier	External	Anonymisation	Scientific publications, EC websites	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_20	Departure times (Cumulative Distribution Function): Data on the cumulative frequency of delivery.	n	LSP participating in each LL	xls	Tasks 3.4: Data is to generate parcel schedules	Internal	Encryption	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_21	Operator data: Van tracking data.	n	LSP participating in each LL	xls, csv, json or xml	Tasks 3.5: This data will simulate various operator needs	Internal	Encryption	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_22	Operator data: Bar code delivery scans data.	n	LSP participating in each LL	xls, csv, json or xml	Tasks 3.5: This data will simulate various operator needs	Internal	Encryption	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_23	City-related data: Parking management system info and/or curbside info.	n	Local Authorities / Local dedicated websites with open data	xls, csv, json or xml	Tasks 3.5: This data will help simulate city network and conditions	External	Anonymisation	n.a.	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project

ID_24	Project, cross-site and local KPIs	n	LL participants	xls	Evaluate the impact of the innovation tested in the project	External	Anonymisation	Scientific publications, EC websites	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_25	Data related to evaluation of the solutions' performance	N	Questionnaire, Impact Assessment Radar	Documents format including pdf, docx, txt, xls	Validation of the URBANE solutions	Task 4.3 participants	n.a	For further research	MS TEAMS (INLECOM Share Point)	at the latest until the end of the project
ID_26	Contact details collected for internal communication purposes	Y	Public Sources	Spreadsheet, CSV, text	Design & development of project solution.	Internal-Consortium partners with valid justification for processing this dataset	anonymization	Other studies in Urban Logistics domain	Partners infrastructure/ MS Teams	at the latest until the end of the project

2.4.3 WP5

TABLE 5 WP5 DATA

ID	Data/Metadata Description	Personal Data identification	Data Origin	Data Format	Purpose of data collection	Data sharing - Access	Procedures to safeguard data	Openess - Reusability	Storage	Retention Period
ID5.1	Information and data developed in past and on-going related projects	N	Data from EU projects such as ENTRANCE, SENATOR, CityLab, ULaaDS, LEED, BOOSTLOG and SENSE	different formats for tools, indicators, reports, etc (xls, csv, text, etc)	establishing the Market Observatory for Physical Internet that will help LLs benefiting from PI information and achieve a better understanding from the PI LMD	External	n.a.	Data collected will be publicly accessible	Data will be stored in the Market Observatory for Physical Internet	During the duration of the relevant task
ID5.2	Questionnaires and data collected from LLs to define the Business Models	N	LLs partners	text	Definition of the business models	Internal	n.a.	Data will be potentially used in the definition of the Business Plans and the commercialisation strategies	MS Teams Folder	At the latest until the end of the project

2.4.4 WP6

TABLE 6 WP6 DATA

ID	Data/Metadata Description	Personal Data identification	Data Origin	Data Format	Purpose of data collection	Data sharing - Access	Procedures to safeguard data	Openess - Reusability	Storage	Retention Period
ID6.1	Contact details of stakeholders	Y	Stakeholders themselves, D&C activities organised within the project	Documents format including pdf, docx, txt, xls	Maximise the outreach of the project/ City platform development and moderation	POLIS mainly & partners that need access	anonymisation	Several datasets may be reused for the project D&C activities	MS Teams Folder	At the latest until the end of the project
ID6.2	List of similar to URBANE initiatives	N	Public sources	Documents format including pdf, docx, txt, xls	Maximise the outreach of the project	All partners	N.A	N.A	MS Teams Folder	At the latest until the end of the project
ID6.3	City Data needed for the development of the feasibility studies	N	Follower Cities	Xls, xlsx, text , json or xml	Development of feasibility studies	Internal only to partners that need access to	Encryption	N.A	MS Teams Folder	At the latest until the end of the project
ID6.4	Capacity building material, white paper, contact list, leaflet,	N	Public sources	Documents format including pdf, docx, txt, xls	To support the adoption and use of URBANE both though Capacity Building and	All partners	N.A	PU, can be used for further research	MS Teams Folder	At the latest until the end of the project

	presentations, videos				Policy Recommendations					

2.4.5 WP7

TABLE 7 WP7 DATA

ID	Data/Metadata Description	Personal Data identification	Data Origin	Data Format	Purpose of data collection	Data sharing - Access	Procedures to safeguard data	Openess - Reusability	Storage	Retention Period *Each partner is responsible for the data and to enforce the retention period
ID7.1	Management (project internal templates, periodic report) and Financial Reports (internal and EC)	N	Project Partners and Coordinator	.doc, .docx, .pdf, .xls, .xlsx, .ppt, .pptx	To monitor the overall legal, contractual, financial, and administrative management of the project and to ensure a comprehensive risk management	Project Partners	N.A	CO	MS TEAMS (INLE Share Point) - EMDESK for financial reports	5 years after the end of the project
ID7.2	Datasets of the project	N	Project Partners and Coordinator	Text in documents (.doc, .docx, .pdf, .xls, .xlsx)	To monitor and manage the data generated and utilised within URBANE activities	Project Partners	N.A	CO	MS TEAMS (INLE Share Point)	5 years after the end of the project

ID7.3	Deliverable template and risk management file	N	Project Partners and Coordinator	Text in documents (.doc, .docx, .pdf, .xls, .xlsx)	To ensure that the project deliverables meet the defined quality standards, and perform quality risk management following the implementation of the project plan	Project Partners	N.A	CO	MS TEAMS (INLE Share Point)	5 years after the end of the project
ID7.4	Partners contact details	Y	Project Partners and Coordinator	Text in xls	For the project implementation	Project Partners	Authentication mechanism, password protected	CO	MS TEAMS (INLE Share Point)	5 years after the end of the project

3 URBANE Data Management Plan (DMP) - FAIR principles

The FAIR Principles are a domain-agnostic, high-level, and measurable set of guiding principles and practices that apply to a wide range of scientific data or metadata. They put "specific emphasis on enhancing the ability of machines to automatically find and use the data, in addition to supporting its reuse by individuals. The term "FAIR" refers to data or metadata that is Findable, Accessible, Interoperable, and Reusable. In practice, the FAIR principles' elements are related but independent and separable. Any combination of the principles can be implemented gradually. Thus, the principles' modularity, as well as their distinction between data and metadata, facilitates their application in a wide range of special circumstances.

The FAIR principles can also apply to a number of assets that must be identified, described, discovered, and reused in the same way that data is. These principles serve as a general guideline for the "FAIRness" of data inside a project. They are not, however, a standard or a specification in and of themselves. To be more specific, the FAIR principles need to be considered before the implementation decisions of the URBANE partners and do not always suggest specific solutions. Instead, they can be viewed as guidelines for data processors to evaluate whether their specific implementation choices are making their research results "FAIR". They serve as the foundation for the long-term preservation of valuable digital assets composed of research project data, with the goal of being discovered, accessed and re-used by other researchers.

It needs to be noted that there is a distinct difference between FAIR data and Open data, as the former does not always imply the latter. While the openness of data is encouraged by the Horizon Europe funding instrument, there are may be legitimate reasons to limit access to certain data/results. These can be related to IPRs, trade secrets or other exploitation related aspects. Nonetheless, the "FAIR" principles can also be applied to such kind of datasets or in general in an organization's internal procedures in order to make them more usable and valuable. In this regard, it is advisable to follow the principle of ”as open as possible, as closed as necessary", meaning that research data should be open by default, with a variable degree of openness. This is mainly because the greater the openness and "FAIRNESS" of data, the greater the benefits.

In this regard, research data produced under Horizon Europe, and in general under the paradigm of Open Science, recommended by the Unesco[i1], should be "FAIR". The guiding principles of each of the four concepts of "FAIR" are presented in more detail in the following sub-sections, where how URBANE will meet the requirements of the "FAIR" principles is also included.

[1] Unesco Recommendation on Open Science. 2021.
https://unesdoc.unesco.org/ark:/48223/pf0000379949.locale=en

3.1 Making data findable, including provisions for metadata

According to the URBANE Grant Agreement, open access to research data needs to be ensured. Thus, the FAIR principle refers to scientific publications, research results (i.e., from surveys etc.), dissemination material as well as digital research data.

In this regard, one of the goals of URBANE is to ensure data findability by ensuring that the generated data is identifiable and easily discoverable. In this context, the project partners will also ensure that non-confidential data gathered during the project will be compiled and deposited openly in institutional repositories, the project website and open repositories.

To that end, the datasets will be accompanied by rich metadata to improve their discoverability. Moreover, the project will ensure that a unique and persistent the Digital Object Identifier (DOI) will be assigned to the data.

The data will be identified with the naming convention included in Annex I. The suffix "_vx.y" will allow for the control of the versioning and document history. This naming convention used for the datasets is similar to the one used to identify the deliverables in the project. Keywords will be also used to enhance the discoverability of the data and associated metadata which will be explicitly include the identifier of the data they describe.

Last but not least, the Consortium will register all (meta)data in a searchable resource, like Zenodo as described in section 4 and will follow the OpenAIRE guidelines where applicable.

3.2 Making data accessible

According to the URBANE DMP policy, raw or processed data from the project, as well as related meta-data, must be preserved and archived and will be made openly available when applicable. The Raw data collected from partners in a predefined manner (file format, fields, etc.) is stored in a database facility and/or the cloud, which will provide the semantically enabled storage facility, and will be available the latest until the end of the project. It is important that the bibliographic metadata will use the the Dublin Core standard, as it is a flexible and commonly used. It will include all the following:

- the terms "European Union (EU)" and "Horizon Europe";
- the name of the action, acronym and grant number;
- the publication date, and length of embargo period if applicable, and
- a persistent identifier which will make them easily retrievable

The metadata will be openly and easily accessible through the Zenodo platform, even if the data are no longer available.

The consortium implements a GDPR-compliant procedure to protect information over time and to ensure high-quality long-term management and maintenance of the abovementioned datasets. These procedures enable a wide range of users to easily obtain, share, and interpret both active and archived information, and they will ensure that information is kept up to date in terms of content and format, ensuring that it remains easily accessible and reusable.

In case long term storage is needed, the responsible partner for these data sets will at minimum indicate how long the data will be preserved.

Data generated and collected within the project (and cannot be publicly available) will be stored and shared in the private channel in Teams, with authorized users having restricted access (only the

Coordinator can grant access to the said space). Only Consortium Partners will have access to the said storage where the datasets and metadata will be available. This is fully covering the day-to-day project needs in a secure and fully integrated manner for project coordination and operations monitoring.

Moreover, the storing processed data will be done into the Innovation Transferability Platform hosted in INLECOM server. Specific data related with IPRs or license restrictions, and/or confidentiality issues may also be uploaded to the platform, but access to those will be restricted via accessibility rules and made available to the partners needed in order to perform the activities assigned to them as described in the DoA. Another raw-data collection issue is the provision of data needed during trials in a real-world environment based on the defined use cases, such as sensor input data. This type of data is expected to be uploaded to the storage components of the URBANE platform demonstrator.

Apart from the above, the specific roles, access, policies, version numbers and naming conventions that have been defined are available in Annex I &III.

The URBANE project deliverables (including the project outcomes) will be accessible to the partners through the project common online collaborative tool (Teams). All the information related to these deliverables will be available by work package and task following a standardized format. Most of the data generated through the project (questionnaires, sensor data, software data, videos, images, audio files, part of the deliverables) will be confidential, only for members of the Consortium, due to privacy and security reasons. The public project deliverables along with the executive summaries of deliverables which are not public, will be available in the project's official website and the institutional repositories to make sure that the documentation is available long time afterwards the project finishes. As the project progresses the Consortium partners and especially the data owners (LL leaders) will be requested to identify the datasets that can be made publicly available through public repositories and other institutional repositories.

3.3 Making data interoperable

Data exchange formats are critical to improving interoperability. The concept of interoperability demands that both data and metadata must be machine-readable and that a consistent terminology is used. In this regards, standardization of data exchange formats within large research projects is thus critical, particularly when using disparate research tools and instruments.

The consortium will ensure the use of interoperable standard formats, such as XML-based standards like JSON Schema , Dublin Core or MARCXML, to allow data exchange and re-use between researchers, institutions, organizations, and countries. In terms of interdisciplinary interoperability, all datasets will adhere to the same data and metadata capture/creation standards. Data that can be made openly available (like the ones included in public deliverables, articles, conference papers, and so on) will be made available in commonly used formats in order to ensure that it can be used easily by other stakeholders. Other types of data will be registered following internal codifications, clearly specified within the file.

Moreover, the URBANE partners will observe OpenAIRE guidelines for online interoperability. These guidelines can be found at: https://guidelines.openaire.eu/en/latest/.

Data interoperability is a key project objective and applies mainly to data related to mainly WP2, 3, and 4. The overall concept of innovation transferability aims to achieve data transferability/interoperability among all logistics players in the context of a Living Lab. The URBANE set of tools will be established

through cloud services hosted in INLECOM server, which will connect data, applications, on-premises and cloud-based processes and services from multiple actors, enhancing collaboration and interoperability, potentially across the entire last mile delivery system of a city.

URBANE will ensure that the research data produced during the project activity meets the required interoperability standards by depositing the project datasets in a data repository (Zenodo, etc) compliant with the appropriate interoperability guidelines and providing a sufficient metadata description of such datasets as mentioned above. It is also worth noting that, as previously stated in the current chapter, metadata vocabularies, standards, and methodologies will be adjusted to promote interoperability.

3.4 Increase data re-use

Data re-use is becoming a distinguishing feature of modern scientific practice. Data re-usability refers to the ease with which one or more communities of research (consumer communities) can use data produced by other communities of research for legitimate scientific research (producer communities). Data re-usability enables the reanalysis of evidence, the reproduction and verification of results, the reduction of duplication of effort, and the building on the work of others.

The URBANE Data Sharing process entails describing how data is shared, including access procedures, technical mechanisms for dissemination, and required software and other tools to increase re-usability, as well as determining whether access is broadly open or restricted to specific groups.

When deposited to the repository, the datasets under their latest available version will be assigned the Creative Commons Attribution International Public License (CC BY) or Creative Commons Public Domain Dedication (CC 0) or a licence with equivalent rights, following the principle 'as open as possible as closed as necessary'. The data will be made available for re-use from the project website and will also be findable and reusable through the final depositing repository (the institutional one or Zenodo) and from OpenAire, the latest by the end of the project. The data will remain re-usable after the end of the project by anyone interested in it with no access or time restrictions for scientific and/or research purposes without prior notification.

In this context, for all shared data, and in accordance with the GDPR, an analysis will be performed to determine the need for anonymizing specific fields. The confidentiality and integrity of the shared URBANE data will be protected and guaranteed in every way using security encryption schemes that match and conform to the data governance requirements. An analysis will be performed on the shareable data sets that will be made publicly available to the EU research community to identify data appropriate for the ORDP. It is foreseen that data sharing for public use will be made available near the end of the project. Publicly accessible repositories, such as Zenodo, or institutional repositories will be considered for storing project results and providing access to the scientific community. All public deliverables will be made available to the project website as well as institutional repositories in easily accessible manner.

The reusability of data is determined by the nature and level of privacy involved, as well as the Intellectual Property Rights (IPR) involved in the data set or scientific publication. Each data owners will identify and impose, where applicable, specific restrictions when privacy, intellectual property, or other exploitations aspects are at stake.

In addition, the respective deliverables associated to the dataset will be licensed through an *All rights reserved license* as they are working papers not intended to be reused. Nevertheless, the database should be shared as a possible reusable datasets.

4 Other Research outputs

Beneficiaries should consider and plan for the management of other research outputs that may be generated or re-used throughout their projects, in addition to data management. Such outputs can be digital (for example, software, workflows, protocols, models, and so on) or physical. Beneficiaries should consider which of the FAIR data-related questions raised above can be applied to the management of other research outputs, and they should strive to provide sufficient detail on how their research outputs will be managed, shared, or made available for re-use in accordance with the FAIR principles.

As one of the European Commission's top priorities, URBANE will strongly support the Open Science policy by providing easy access to information for other relevant public authorities, city associations, and the general public concerning the last mile delivery optimization concept.

All of the project's research outputs—publications, data, software, models, and algorithms—will be made open access. The data and articles will be hosted on the European Open Science Cloud under the license ensuring the principle 'as open as possible as closed as necessary and the Zenodo repository as described below. It should be noted that some of the data generated and collected during the project may be restricted if there is a valid reason to protect the legitimate interests of a partner or an individual. These types of datasets will not be made public.

In addition, the project will contribute to forums and repositories for SULPs, and it will give other parties access to the monitoring data through an Open API infrastructure through its cloud services. After receiving EC approval, the project will also deposit its public deliverables (including the open-source software components and datasets) on its website and in designated data repositories, and it will take steps to make it easier for third parties to access, mine, exploit, reproduce, and distribute the materials without charging any users.

4.1 Open Access to Scientific Publications

It is each beneficiary's responsibility to ensure open access to all peer-reviewed scientific publications relating to project results. In the context of an EU-funded project, open access to scientific publications primarily refers to free online access for anyone who is interested. Thus, open access will be achieved by implementing the following steps:

1. Any article outlining the project's findings must include the following statement accompanied by the EU emblem: "The research leading to these results has received funding by the European Union's Horizon Europe research and innovation programme under grant agreement No 101069782 -URBANE."

2. Any article or paper, presenting the Action results will be deposited at least by the time of publication to a formal repository for scientific papers. Nevertheless, the paper can be uploaded in the European sponsored repository for scientific papers: http://zenodo.org/. It needs to be noted that each case will be examined separately in order to decide whether the self-archiving or paying option will be followed for open access publishing.

3. Authors will make sure that the following will be included in their papers:
    a. The terms "European Union (EU)" and "Horizon Europe";
    b. "UPSCALING INNOVATIVE GREEN URBAN LOGISTICS SOLUTIONS THROUGH MULTI-ACTOR COLLABORATION AND PI-INSPIRED LAST MILE DELIVERIES", Grant agreement number 101069782;
    c. Publication data, length of embargo period if applicable; and
    d. A persistent identifier.

4.2 Public repository in ZENODO

In continuation to the information provided in the previous section and to assure adherence to FAIR principles, the consortium will also create a repository in ZENODO for the project.

The repository will consider the following terms, guidelines, and regulations:

- The applicable Task Leader is responsible for gathering the data in the best format possible, store them in the ZENODO repository, and make them searchable.
- All partners must ensure that data sets and research outputs are cross-referencing one another (e.g., publications and the data behind them).
- The description of how to find the data should be included; for example, provide metadata (author, date of publication, etc.)
- Each partner is accountable for their records and documentation related to data generated, which must be in accordance with this DMP and monitored by Task leaders.
- Data will be made accessible within one month of their publication unless the responsible partner has specified justifiable reasons to keep the data confidential.
- Task Leaders should notify the Responsible partner (INLECOM) after uploading data in ZENODO.

5 Allocation of resources

The costs connected to the FAIR data management have been foreseen and covered by the partners themselves, since they are part of their internal procedures. In case there are any additional related costs, these will be covered by the respective partner. At the point of submission of the current document, no extra-costs are foreseen.

TABLE 8 DATA MANAGEMENT COSTS

Cost Type	Cost Allocation according to DoA
Cost for dataset collection, storage, backup, archiving and sharing that is realized mainly through the Microsoft Teams for project coordination and management	WP7

Costs of storage for data that will be managed locally or on cloud during the solution development, integration and testing (sensor data, DT platform, sensor data etc.)	Included to WP2 , WP3 and WP4, and more specifically to each partner that is responsible for the system component development and testing. Included under the activities of WP2 and 3 and allocated to each partner that is responsible for the respective component to be deployed on the DT platform.
Costs of storage for data that will be managed during the real-life testing (sensors, questionnaire input etc.)	Appointed to WP2 and 4, each partner is responsible for the component to be deployed in real life.
Data management cost for the dissemination and communication activities	WP7
Costs related to the data curation and publication after the end of the project	Covered by the internal processes and own resources of each responsible partner

Furthermore, the following human resources have been identified and are covered within the URBANE budgeted costs:

- **Data Protection Officer**: According to GDRP each partner will allocate a Data Protection Officer for the collection and any action needed for the handling of personal data.
- **System Administrators:** That will ensure the uptime, performance, resources and security of the project computers platforms needed for data storage and processing.

It should be noted that INLECOM will be the accountable partner for providing guidance on data management policies. Each URBANE consortium partner, however, will be solely responsible for ensuring that the guidelines outlined in the current document are followed.

The dissemination material (e.g., scientific publications) will be made freely available via the project website and the institutional repositories as well as open access repositories when applicable.

5.1 Roles and Responsibilities

WP7 Project Management is the work package in which the process for data management has been created and will be monitored to ensure compliance with data management decisions as they relate to the DMP. The following summarizes the DMP roles and responsibilities in URBANE.

TABLE 9 DATA MANAGEMENT ROLES AND RESPONSIBILITIES

Tittle	Role	Organisation
WP7 leader	Responsible for preparing the Data Management Plan and policies and providing guidance as necessary.	INLE
Data Controller	Responsible for reviewing the Data Management Plan (DMP) and policies and should be aware of their responsibilities to comply with the GDPR and other applicable regulations.	Each Partner within URBANE that is responsible for processing Personal data in accordance with the GDPR.

6 Data Security

To meet the project's main requirement for protected digital data storage, URBANE partners will adhere the below set of guidelines:

- Data availability must be guaranteed.
- Confidential data must be stored using access protection.
- Strictly confidential information must only be stored in an encrypted mode.
- Confidential data must not be stored in online services that are not approved by the URBANE Consortium.
- Any exception from this measure must explicitly be approved.
- Modifications to data with high integrity requirements must be documented and approved by the partners.

The URBANE consortium partners prioritise the security of the data generated or used during the lifetime of the project. In this context, state-of-the-art technologies will be used for secure storage, delivery and access of information, as well as managing the rights of the users for the data generated or collected. In this way, it will be guaranteed that the accessed, delivered, stored and transmitted content is managed by authorised persons.

Securing stored digital data entails preventing the unauthorized access to it as well as accidental or intentional data destruction, infection, or corruption. While data encryption is a well-known mechanism, it is only one of many techniques and technologies available for implementing a tiered data-security strategy. In this regard, the URBANE Consortium adopted specific security measures as a set of technological, procedural, and organizational requirements with the goal of implementing an adequate level of security in data processing, to ensure their privacy, availability, and integrity as well as the systems' resilience.

In this regard, the participants' contact details will be stored in a password protected excel file. The stored data in project's Teams collaborative space will not include any personally identifiable information. However, their proper management will be ensured by complying with GDPR and legislation. The project will not collect sensitive personal information, such as ethnic origin, political, religious or philosophical

beliefs. Where needed, partners will encrypt and anonymize the data to protect personal identities. It needs to be noted that data collected from sensors or historic datasets will be privacy protected by using one-way hashing encryption and cleaning techniques at the source before uploading them to the cloud or the platform, thus eliminating accessible information.

Specifically, for cloud storage, all the information in transit will be performed over secure channels. The use of Transport Layer Security (TLS) with strong ciphers is the established best practice for securing network communication. Additionally, TLS provides integrity and authenticity of the interacting peers. Moreover, the TLS-secured network communication channels and HTTPS will be used both internally (among the platform's components) and externally (when the system is accessed by its users or other systems). The identification and authenticity of the interacting other components will be verified with digital certificates signed by either using well known and trusted Certificate Authorities (CA) or an internal CA of the platform in order to simplify deployment. The latter can facilitate the testing of the components and it's certainly easier, at the cost of supporting only the internal communication. Of use of strong private keys (2018-bit RSA or 256-bit ECDSA), recent versions of TLS (TLS 1.2 and 1.3), and a short list of strong ciphers that offer at least 128-bit encryption will be utilized.

The outcome of each responsible partner's analysis, evaluation, and risk management process collected led to the selection of the required security measures.

6.1 Teams Platform

For the internal collaboration among project partners, INLECOM is offering a Teams collaborative space. Below we describe the server capabilities and services as far as physical, network and content security are concerned.

Below, the server capabilities and services are described as far as the physical, network and content security are concerned.

The TEAMS server is a cloud hosted facility, providing an environment that operates using two-point verification security and world class data exchange, storage, and collaboration services. It is a cloud-based facility utilising Microsoft data servers, web/application servers, file servers and databases. TEAMS is used to store and distribute internally all project related documents, also integrating meetings and calendar services. Physical security is guaranteed by the service level agreement.

Network security is transparent in TEAMS. Internally a secure socket layer (SSL) with the AES algorithm and 2048-bit key length are used to guarantee on a both server authentication and data encryption levels.

As for the content security, access control is managed, and fully configurable, all users and participants of the shared documents facility are provided with roles, and access rights. User authentication is used to provide access to the server data based on unique accounts, password protected. There is a possibility to configure and define different user and thematic/topic interest groups. Hence, the project administrator is also capable of providing or restricting access to particular folders/data by setting rights and permissions.

6.2 Access control mechanism

The URBANE project seeks to create a trustworthy environment for all project participants, particularly the LLs stakeholders. Because of the sensitivity of certain datasets, data security is critical, and thus data

access control mechanisms must be implemented. For all restricted datasets, a control access mechanism will be established using the following steps:

- For all sensitive data sets, groups having access should be defined.
- Procedures to define access rights as well as to manage access requests need to be developed.
- Authentication mechanism development.
- Sharing of sensitive data sets, will be done after defining the conditions for accessing and using such data.
- Sensitive and confidential data can only be accessed by the predefined authorized groups and if needed non-disclosure agreements need to be signed.

6.3 Data confidentiality

Personal data and information are not considered confidential because they are protected under basic data protection legislation, as discussed in the following section. In the current section, it is particularly technical and commercial information that is protected. This information may be protected by intellectual property rights, but it is also possible that it is unprotected raw data with business value for the disclosing party. This category also includes information related to datasets provided by LL stakeholders for the implementation of the LL activities as well as the development of the models and tools in the scope of URBANE project.

In this regard, for protecting the said datasets the project will examine to use encryption or anonymization techniques. In addition to the above and if deemed necessary, the project partners may also use NDAs as the preferred method for protecting confidential information exchanged during project execution.

7 Ethical Aspects – GDPR compliance

The confidentiality of personal data is a top priority throughout the project and beyond. As a result, the URBANE project is eager to preserve any personal data handled throughout the project's lifespan and will implement the necessary GDPR and European Code of Conduct for Research Integrity compliance measures. All information gathered from project participants will be handled securely, in accordance with applicable data protection and privacy laws, as well as national ethical standards and requirements. The current document, as well as the one that will follow it, will describe how sensitive data will be handled.

In this regard, URBANE will fully comply with GDPR legislation (see Annex III for more details). Every project partner is fully aware of their GDPR responsibilities, and the project takes concrete steps to prevent, to the greatest extent possible, any unauthorized access and misuse of personal information. The Data Protection Officer (DPO) of each of URBANE partners are key figures in ensuring the GDPR compliance.

With respect to all data processing activities, guidance will be provided by the INLECOM that is the leading partner of the associated WP/Task and the Data Protection Officer of each partner. For partners not having the obligation of appointing a DPO, a GDPR policy has been set in place which is also included in Annex III. Data Protection definitions and data processing principles can be also found at Art. 4 GDPR.

Since the project is related with the last mile delivery, it does not in principle need the collection of any personal type of information. Generally, personal data processing might fall under the following cases:

(a) process personal data by way of collection,

(b) process personal data by way of data transfer,

(c) do not undertake any personal data processing under the Project.

Personal data shall not be transmitted to non-EU countries and consequently cloud computing infrastructure will be based in an EU country.

At the time of the drafting of the current document, the personal information that are foreseen to be collected and stored throughout the project duration (as extracted from the answers to the DMP questionnaire and included in Table : Data and Personal Information of day-to-day activities) are related to:

- Coordination and management purposes (WP7);
- Research activities that involve participants on a voluntary basis, i.e. experiments, questionnaires, interviews, workshops, demonstrations and other testing activities (e.g. as part of WP2, WP3, WP4);
- Dissemination, communication and exploitation purposes (WP5, WP6).

7.1 Coordination and Management

In the context of WP7, the Coordinator and Task Leaders will process personal data originating from Consortium partners' personnel for the purposes of project coordination and management. Names, email addresses, signatures, voice (during online meetings), and images will be collected (if necessary, during online meetings as well). The information mentioned above is obtained directly from the data subjects (researchers). The personal details of the members of the URBANE consortium are already covered by the CA, which includes non-disclosure clauses, as well as the Grant Agreement signed with the EC, which includes Special Clause on data treatment.

The purpose of this processing is needed for the performance of the obligations that derive from the URBANE Grant Agreement as well as the URBANE Consortium Agreement.

According to the Data Sheet of the Grant Agreement, the storage period is 5 years after the end of the project for reasons of accountability to the EC. The image/voice will be kept for the time period specified in the Consortium Agreement for the purpose of drafting minutes.

Only Consortium members will receive information shared via the project's online repository. Only members with permission can access the repository, which is controlled and secured by INLECOM. If the project is transferred to non-EU partners, the rules of Chapter V of the GDPR will be followed.

Data subjects have certain rights that can be exercised by contacting the DPO or the data controller directly, related to the ability to access information, request the rectification or erasure of inaccurate data, request a restriction on the use of their personal information, request data portability, and file a complaint with a supervisory authority. These rights can be exercised by contacting the controller's DPO or, in the absence of a DPO, the controller directly.

7.2 Research activities that involve personal data obtained by the data subjects (volunteers)

Based on the input provided by the WP leaders (as included in section 3) within the project context, any collection of personal data might take place via the following means:

a) interaction with individuals during interviews, questionnaires, experiments, workshops or other dissemination and demonstration events.
b) collection of data from piloting activities
c) whenever evidently personal information is recorded.

In this context, it is recommended that the URBANE partners to take the appropriate data protection measures in the aforementioned cases. All partners who collect personal data must notify the organisation's DPO before collecting any data. It is assumed that parties already comply with the relevant legal and data protection rules if they collect or receive such information as part of their existing business operations.

In this regard, the researcher collecting personal data through volunteers must provide them with a detailed Information Sheet outlining the procedures to be followed for the processing of their personal data in advance, in accordance with GDPR rules.

This request for consent must be made in an understandable, easily accessible, and plain language. In addition, the researcher should make himself available to answer questions and provide clarifications, when needed.

A copy of the Information Sheet will be given to each participant to ensure that the volunteers can read the material at any time and that they will exercise their rights whenever they feel the need to do so. Participants may withdraw their consent at any time without consequence.

The personal information included in the Informed Consent Form will be treated and stored securely in accordance with the General Data Protection Regulation for the duration specified in the URBANE Grant Agreement (5 years after the project's completion).

In the case of Personal identification data (name, date of birth, phone number, department ID and study IDs), these will be stored separately and will not be used for analysis in accordance with the "personal data definition" as defined by GCP. They will be saved in locked Excel format on the data controller's computer and/or on the coordinator's computer.

Data governance in URBANE will ensure proper Data Management of important and sensitive data, including information for customers and products, to be appropriately managed, anonymized, encrypted, and sanitized, managing risks that may arise from their access by third parties.

7.3 Dissemination, communication and exploitation of project's results

The project's website will always be the primary source of information. It will be used to communicate about the consortium, upcoming events and workshops. The website will also support dissemination and communication initiatives by including press releases, articles, papers, and conference presentations. URBANE will create electronic newsletters that will be published on the project's website to highlight ongoing activities and future planning of the project's activities. The social media accounts for the project serve the same purpose.

Personal information of attendees at a meeting or event will be collected for registration and participation purposes, provided they have consented to the collection and processing. The registration process will include a data Information Sheet for this purpose.

In order to maximize the exploitability and the outreach of the project results, the Consortium intends to also publish the respective datasets/ information in institutional repositories and/or in Zenodo and EOSC whenever applicable.

The storage period for the aforementioned information is for 5 years after the end of the project according to Data Sheet of the Grant Agreement for accountability reasons towards the EC.

7.4 AI in URBANE

In terms of Artificial Intelligence, the algorithms and models will adhere to the ethical guidelines outlined in the Ethics Guidelines for Trustworthy AI (published by the EC in April 2019) as well as the current EU guidelines outlined in the AI HLEG reports. The AI system will not interact with humans and will pose no risks in terms of privacy, ethics, human rights, freedoms, or biased AI. The system's goal is to investigate synergistic phenomena and identify causal links in order to improve the last mile delivery concepts. Furthermore, the system will be designed to produce explainable results by sharing the training datasets in the project's public repository and documentation about the system's architecture.

7.4.1 Personal data under AI

The GDPR legislation includes terms referring to the internet (websites, links, and social networks), but it does not include the term "artificial intelligence". However, there are many provisions that are relevant to AI and need to be considered throughout the relevant technical development activities:

1. Article 4(1): Personal Data (identification, identifiability, re-identification)

   In connection with the GDPR definition for personal data, AI is raising two key issues: i) the 're-personalisation' of anonymous data, namely the re-identification of the individuals to which such data are related; (ii) and the inference of further personal information from personal data that are already available.

2. Article 4(2): Profiling

   Although explicit reference to AI is not made, GDPR does address the processing as it is performed using the AI technology, consisting of the usage of the data connected with an individual.

3. Article 4(11): GDPR consent

   Consent is critical in the traditional understanding of data protection, which is based on the 'notice and consent model,' which states that data protection is aimed at protecting the right to 'informational self-determination.'

4. Article 5(1)(b): GDPR Purpose limitation

   The concept of a purpose limitation connects the purpose of processing to the relevant legal foundation. There is a conflict between the use of AI and the requirement for purpose limitation. The technology enables the useful reuse of data for new purposes' other than those for which it was originally collected. To establish the legitimacy of data repurposing, one must first determine whether the new purpose is 'compatible' or 'not incompatible' with the original purpose of data collection.

5. Article 5(1)(d): GDPR Accuracy

   GDPR mandates that data be "accurate and, where necessary, kept up to date," and that steps be taken to correct inaccuracies. This principle also applies when personal data is used as an output to an AI system, particularly when personal data is used to draw conclusions about the data subject.

7.5 Gender issues

Adopting the EU's Gender Equality Strategy 2020-2025, URBANE consortium is committed to the gender equality principles: 1) producing equal opportunities for women and men in research; 2) performing of the sex and gender analysis in the project; and 3) referring of the biological characteristics and social/cultural factors respectively. The target is to integrate gender dimensions into research and innovation content according to the guidelines produced by the H2020 expert group (H2020-GI-2) on "Gendered Innovations" and to using of the recemented methodological tools (e.g. IGAR tool) for sex, gender and intersectional analysis.

The overall aim is to avoid gender-biased analysis and conclusions; thus, the integration of gender and sex dimensions into the research design process at all its stages will be ensured in the extraction of user needs and scenarios in last mile context (WP2), the technology development phases being committed to frame the technological approach in a SoEL manner (WP3), the piloting activities (WP2&4), and the dissemination, communication and exploitation activities and including the recommendations for stakeholders (WP5&6).

Finally, there could always be the chance of eventual presence of yet unrecognized or difficult to detect sex/gender biases in the envisaged research and innovation. The widespread method of fighting against this phenomenon is to ensure gender equality in research and pilot implementation, which will be one of the consortium's top priorities.

8 Conclusions

This Data Management Plan Version 1 provides an initial overview of the data collected, generated, and eventually processed in URBANE and describes the data categories within the project's scope, providing information on their management and FAIR principles implementation.

URBANE is committed to adhering to the principles of the Open Research Data Pilot, and thus the open access guidelines have been described, with the goal of ensuring that the project's outputs are openly available to the research community.

The current deliverable's content will be updated on a regular basis, and its final version will be officially submitted in month 42. The current document is the first version of the Data Management Plan; in the final version (D7.3 Data Management Plan), more details will be provided, particularly regarding the description of shared datasets and the corresponding standards and methodologies.

Special attention will be paid to datasets that will be shared within the scope of the Living Labs (WP2&4) but for which we do not yet have enough information at this stage of the project. These various types of data necessitate distinct treatments and the development of an appropriate methodology by the project (the need for anonymisation techniques for different datasets , for example personal traveller data). Similarly, the data from our reference group of stakeholders will be detailed and their unique characteristics will be described.

Annex I

The naming guidelines are presented in 10 below. Some of these use meeting identifiers (meetingID):

- **KOM:** The Kick-Off Meeting of the project.
- **PM:** Project Meeting (The General Assembly).
- **SC:** Steering Committee meeting.
- **WPX:** Work Package X meeting.
- **LL:** Living Lab meeting (for other LL meetings, not for the regular WP4 meeting).
- **TM:** Technical Meeting.
- **RM:** Review Meeting.

and location identifiers (locationID):

- **ONL:** Online Meeting.
- **cityName:** If it is a physical meeting, use the city name as the locationID e.g. Madrid

TABLE 10 THE NAMING CONVENTIONS FOR DOCUMENTS IN URBANE.

Document Type	Template
Deliverables	'URBANE_Dx.x_DeliverableTitle_versionX.X_Date_partner'
Agendas	'URBANE_meetingID_locationID _meetingDate_Agenda'
Minutes & Agenda	'URBANE_meetingID_locationID_meetingDate_Minutes/Agenda_versionX.X
Presentations	'URBANE_meetingID_shortTitle_meetingDate_partner'
Peer Review Score Sheets	'URBANE_PR_Dx.x_submissionDate_partner'
Peer Review Response (Completed by LB)	'URBANE_PR_RESP_Dx.x_submissionDate_partner(reviewer)_LB'

Data and Personal Information of day-to-day activities

TABLE 11 DATA AND PERSONAL INFORMATION FROM DAY-TO-DAY ACTIVITIES

Personal Data Description[2]	Access[3]	Storage[4]	Purpose[5]	Duration[6]
XLS list of URBANE AB contacts	Internal to URBANE (project partners only)	Inlecom Secure Server	URBANE mass-dissemination, list of potential users, exploitation	5 years after the end of the project for reporting purposes
Meeting related material (agendas, presentations, signature lists, minutes)	Internal to URBANE (project partners only)	MS TEAMS (folder: *meetings*)	URBANE meetings' related	
Workshops/Conferences and Training sessions	Internal and external to URBANE	MS TEAMS (folder: *meetings*), URBANE website	Large event dissemination	
Deliverables, internal documents and other URBANE reports	Depending on deliverable type could be public or consortium restricted	MS TEAMS (folder: *Deliverables*)	URBANE documents and deliverables	
Publications	Internal and external to URBANE	MS TEAMS (folder: *Publications*)	Dissemination and publication of research results	
List of stakeholders (external to URBANE)	Internal and external to URBANE	MS TEAMS (folder: *contacts*)	URBANE mass-dissemination, list of potential users, exploitation	

[2] Overall data description.
[3] Determines who has access to the particular data (internal, external to consortium).
[4] Storage places of actual data.
[5] Intended purpose of data and reasons for keeping.
[6] Duration of stored data (until when they will be kept).

Annex II-DMP questionnaire

ID	Data/Metadata Description	Personal Data identification	Data Origin	Data Format	Purpose of data collection	Data sharing - Access	Procedures to safeguard data	Openess - Reusability	Storage	Retention Period
Guidelines	*Describe the data/metadata that you foresee to be collected in the project activities your organisation participates.*	*[Y/N]*	*Describe the source from which the data/metadata come from.*	*Describe the format of the data*	*Analyse the purpose of data collection and relation to project activities -if applicable name the respective task /WP and project objectives*	*[Internal/External] to the consortium Should access be limited to a specific consortium subgroup? Will any entity (including any service provider) outside of the E.U. have access to these data? If so, who?*	*Describe any measures/ preconditions for data access and sharing*	*Potential reuse of data in other domains, work and efforts, studies beyond the project scope -Will you provide open access (publicly available) ? Elaborate how the data can be reused*	*Please describe where the data will be stored*	*Please mention the time period for the data retention*

Please provide the contact details of your organization's DPO.	

Annex III - Global Data Protection Policies

This Global Data Protection Policies in the context of URBANE should be applied individually by all Partners so to:

- Comply with the policy and legal requirements of the EU General Data Protection Regulation (Regulation EU 2016/679, the "**GDPR**"), as in effect since 25 May 2018;
- Comply with all other applicable national and EU regulations and guidelines on personal data processing;
- Comply with applicable regulations and best practices with regard to research projects within the EU H2020 Research Programme;
- Raise awareness and improve knowledge among the Project Coordinator, the Project Partners, as well as their employees and/or agents and/or contractors (collectively, the "**Policy Recipients**").

Because the field of data protection is a dynamic legal field of constant change, new developments, in the form of new regulations, official reports and/or guidelines, are issued by EU and national legislators, as well as competent national authorities at a constant pace. In this context, Policies may need to be periodically updated to remain relevant to legislative change. Accordingly, Policy Recipients will be duly informed, and will be asked to provide their renewed consent upon any such updates.

Definitions

The GDPR definitions, as set in the GDPR Article 4[7], apply.

List of Definitions	
Datasets	A structured collection of data generally associated with a unique body of work.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Information can fall under the category of personal data for example if it can be linked to an identifiable person through accessing a register.
Sensitive Data	Classified information that must be protected and is inaccessible to outside parties unless specifically granted permission. Sensitive data is regarded as private information or data for the protection of interests in business, individual rights, organizations, R&D, political, economics, security of the EU or member states, etc. Sensitive data, or special category data, according to GDPR is any data that reveals a subject's information.
Anonymisation	The process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. An individual may be directly

[7] http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm

	identified from their name, address, postcode, telephone number, photograph or image, or some other unique personal characteristic. An individual may be indirectly identifiable when certain information is linked together with other sources of information, including, their place of work, job title, salary, their postcode or even the fact that they have a particular diagnosis or condition. Once data is truly anonymised and individuals are no longer identifiable, the data will not fall within the scope of the GDPR and it becomes easier to use.
Pseudonymization	A data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. The use of pseudonymization in personal data may reduce the risk associated with data management and help controllers and processors to comply with their data protection obligations. Pseudonymization does not imply a complete anonymization or complete dissociation of the data or the impossibility of reversion of the same. This is because there is always the possibility of identifying the party concerned through additional information. Unlike anonymization, it is considered as personal data by GDPR
Metadata	Information about datasets stored in a repository/database template. For example, an image may require metadata that describe how large the picture is, the colour depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Primary Data	Primary data is a type of data that is collected by researchers directly from main sources through interviews, surveys, experiments, etc.
Controller	means the owner of the data (usually the creator of the data itself), unless otherwise expressly clarified in e.g., Project deliverables and reports. Further information for the use of the term "Controller" complying to GDPR is provided in this Annex.
Processor	means each Project Partner, referring mainly to the technical partners participating into the URBANE consortium, unless otherwise expressly clarified in this Policy or elsewhere in Project deliverables and reports.
Consent	of the data subject means any freely given, specific, informed, unambiguous and **in writing** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Supervisory authority	means the competent Data Protection Authorities within the Project Partners' jurisdictions.

Policy scope

URBANE leaves the GDPR compliance to the Controllers and Processors consortium members. The Controller determines in advance what is the law applicable to the processing of personal data in a particular case, considering that according to EU law such determination comes from legal principles and cannot be derogated by the parties.

Establishment

Each Project Partner is established on the territory of EU Member States. In the event of any change in establishment, the respective Project Partner shall notify the Project Coordinator duly and in writing. Unless otherwise expressly specified, each Project Partner is considered the controller in that Member State.

Processor outside the EU

In the event of any subcontracting to an organization not established on EU territory (such as subsidiaries pertaining to the same corporate group) that processes personal data of people staying on EU territory, on behalf of a Project Partner, that organization qualifies as Processor and ensures the fulfilment of the obligations imposed by the GDPR for that specific part of processing.

Personal data processing

Personal data

Personal data means any information relating to natural persons, that is or can be identified, even indirectly, by reference to any other information including a personal identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of data

Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation as well as the processing of genetic data and biometric data for the purpose of uniquely identifying an individual. In the event of such processing the Controller and/or Processor respectively comply with specific rules related to the processing of such data of special categories, as collecting specific informed consent from data subject and applying stricter safeguards. When the Controller and/or Processor relies on data subject's consent as a legal ground for processing special categories of data, it will meet all legal consent requirements; otherwise, they are only processed if and to the extent it is based on one of the legal grounds listed in the GDPR for the processing of such data.

Newsletters, social media and other dissemination material

Unless otherwise expressly specified in Project contract, Controller shall be responsible for the personal data processing carried out for Project dissemination purposes. To this end, Controller shall:

- Collect and keep all relevant personal data (including lists of contact details), or copies thereof.
- Monitor relevant communications;
- Address to Project Partners instructions and guidelines on Project dissemination activities (including any EU or other state guidelines, whenever available);
- Inform Project Partners of any policy or legal requirements reviews and changes.

Data processing

Data processing means any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organization, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data whether the latter are contained or not in data bank. European Union data protection law set forth the following specific principles for legitimate data processing.

Pertinence and necessity - The Controller should implement management practices to fulfil the obligation to collect only relevant and necessary data for a specified purpose.

Purpose limitation - Personal data is collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The Controller has a clear overview of all purposes for which personal data is processed. Personal data is not processed for purposes besides the original purposes, unless the (secondary) use is compatible.

Data minimization - Personal data collected by the Controller must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected and further processed; if the same purposes can be realized in a less data intensive way a preference is given to that method.

Data update - Personal data is accurate, and where necessary, kept up to date. Every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

Data retention - Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The Controller and/or Processing concerned should have processes and policies in place to:

a) determine what the applicable (minimum and maximum) retention periods are for the personal data that is being processed;

b) ensure that relevant retention periods are monitored.

Data anonymisation

Whenever possible, including non-detrimental to Project execution purposes, Controller and Project Partners shall undertake efforts to keep personal data processed by them for Project purposes anonymous or pseudonymous. According to the GDPR, "anonymous information" is information which does not relate to an identified or identifiable natural person, or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In this context, the GDPR does not apply to the processing of such anonymous information, including for statistical or research purposes. Similarly, "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Data protection legal roles

Controller

By determining the purposes and means of the processing of personal data, unless otherwise expressly specified in this Policy, the Controller is considered by law as the "Controller" and it is the primary target of the provisions of the law.

Identification

The data controller previously identifies itself as such and ensures an effective implementation of data protection measures in order to comply with the principle that personal data are processed fairly and lawfully. The legal role of controller implies specific responsibilities because provisions setting conditions for lawful processing are essentially addressed to the controller.

i. Accountability

The GDPR provides full accountability of the company/controller regarding the compliance of its processing of personal data with the law. To ensure the effectiveness of that obligation, it prompts the Controller to follow an overall approach, achieving a genuine system of control and management of its pertinent information. So, accountability and compliance system are elements of the framework for the protection of personal data, in the cause/effect relationship: to be compliant and able to prove it (accountability), the Controller needs to put in place a comprehensive compliance system.

ii. Data protection by design

The Controller considers data protection issues from the outset and from the design of the Project, within the whole lifecycle of processing, to manage the issues in a proactive way, to reduce costs and improve efficiency.

iii. Data protection by default

The Controller standardizes data protection principles in personal data processing, products and services. The measures adopted ensure that

- personal data is processed for purposes not different from the original purposes,
- only data necessary for these purposes are collected, and
- data are not disclosed without human intervention.

Joint controller

If at any time during Project execution the Controller processes personal data in conjunction with a third party, by jointly determining the purposes and means of the processing, they both act as joint controller. Both joint controllers determine the mutual responsibilities with a specific arrangement.

Processor

Unless otherwise specified expressly in this Policy, all Project Partners act as Processors during Project execution. A processor processes personal data on behalf of the Controller – that is, the Controller delegates all or part of the processing activities to them. In such event the Project contract assumes the role of the relevant required written agreement as per GDPR requirements.

The processor warrants that it shall provide sufficient guarantees to ensure compliance with the GDPR, has implemented appropriate controls to meet data protection requirements defined by the agreement, instructions and/or legal requirements and ensures the protection of the rights of data subjects.

Auditing

The Controller ensures the commitment of the Processor(s) to enable and contribute to any review activities, including inspections, carried out by the Controller or other (EU authorities') auditors and/or reviewers, as appropriate.

Security

Each Project Partner undertakes that it adopts appropriate security measures to ensure the security, integrity and confidentiality of personal information and electronic communications at an adequate level with regard to Project purposes, and at any event at no lower lever than processing of similar data within its own organisation.

Data Protection Officer (DPO)

Whenever required, following applicable GDPR and Member State respective legal requirements, the Controller and each Processor, may designate a data protection officer ("DPO") for assistance in monitoring internal compliance with GDPR.

i. Identification

Each Processor appoints a DPO in accordance with the criteria and the requirements set forth in the GDPR, as applicable to it. In such event, it shall notify the Controller in writing accordingly.

ii. Designation compulsory vs. voluntary

Each Processor documents the reasons supporting the designation of the DPO or, rather, the reasons why such designation is deemed not necessary. This documentation forms part of the data protection documentation system of that Processor.

iii. Professional requirements

The DPO has sufficient authority, professional qualities, and independence to ensure success in his role, according to the GDPR provisions.

Tasks, Notification to Supervisory Authority

The organization assigns to the DPO at least the tasks listed in the GDPR. Whenever a DPO is appointed, the organization notifies the Supervisory Authority of such designation and publishes DPO's contact details.

i. People in charge of processing

Individuals who process personal data under the authority of the Controllers or Processor(s) must receive specific formal instructions. Hence, the Controller gives specific instructions, relating also to the implementation of security measures and safeguards, to all its personnel in charge of processing personal data.

ii. Training and awareness

All Project Partners' employees should be well informed and aware of data protection implications and be able to carry out their obligations in their work. A data protection education and communication program should be in place and supported by a monitoring system that confirms all employees and/or contractors are appropriately trained on their data protection responsibilities.

iii. Policies and procedures

Data protection policies and procedures exist, are documented in writing, are formally approved by management, implemented, reviewed, updated, and approved when there are changes to applicable laws and regulations.

All Project Partners understand, and the Controller may ask them to overview all their personal data processing, the data protection risks and the applicable rules and procedures. In such event, they shall provide it with all requested information to the best of their ability without undue delay.

Notice and consent

Notice

Each Controller and/or Processor, as appropriate, provides the information required by law to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, for any information addressed specifically to a child.

The data protection notice informs data subjects about the processing of personal data relating to them, even when the personal data is not collected from them as well as of their rights, to let them verify the accuracy of the data and the lawfulness of the processing.

Free and informed consent

Personal data is processed if and to the extent that the data subject has given valid consent to the processing for one or more specific purposes, or another legal basis for processing exists.

Systems or applications can document the explicit consent of the data subject so that it can be evidenced at any time.

Other legal grounds for a legitimate personal data processing are the following:

1. performance of a contract,
2. legal obligation,
3. vital interest of data subject,
4. public interest,
5. legitimate interest of the controller or third party.

If "legitimate interest" is used as a basis, the interests that have preceded to the decision, need to be documented as well as any possible mitigating measures which will be taken to be able to proceed with personal data processing based on the defined interests.

Withdrawal of consent

Data subject's consent can be withdrawn at any time; even though it will not affect the lawfulness of processing based on consent before its withdrawal.

Rights of data subjects

The individual whom the data refers to (data subject) is entitled with specific rights set forth by the law. The GDPR requires that each Controller and/or Processor, as appropriate, must facilitate the exercise of the data subject's rights, act on the request within a specific time frame and must communicate the information requested in an intelligible and easy to access form.

Right of access

Any individual must be able to exercise the right of access to data relating to him which are being processed.

Right to rectification

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request rectification of their personal data. The procedure specifies in which cases rectification is legitimate.

If a data subject's request for rectification is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

Right to erasure

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request erasure of their personal data. The procedure specifies in which cases erasure is legitimate.

If a data subject's request for erasure is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

Right to restriction of processing

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request restriction of processing of their personal data. The procedure specifies in which cases restriction is legitimate.

If a data subject's request for restriction of processing is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

Right to data portability

Each Controller and/or Processor, as appropriate, determines which processes are subject to the right of data portability as well as when the requirements for such right are met.

Data subject can request the organization to receive a machine-readable copy of the personal data the organization holds about them and where possible, enable the transfer of this data to another data controller.

Portability right can be exercised when:

1. processing operations are based on data subject's consent or on contract
2. personal data concerns the data subject and are the same that the latter has provided to the organization
3. the right does not adversely affect rights and freedoms of others
4. the processing is carried out by automated means.

Each Controller and/or Processor, as appropriate, implements appropriate measures and procedures to provide data subject, who is entitled to, with a structured, commonly used, and machine-readable copy of the personal data it holds about him and where possible, to enable the transfer of this data to another data controller indicated by data subject.

Right to object

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subjects have the right to object on grounds relating to their situation (unless the processing is necessary for the performance of a task carried out for reasons of public interest). The right to object is explicitly brought to the attention of the data subject at the latest at the time of the first communication with the data subject, presented clearly and separately from any other information. Measures should be in place to assess such objections and to ensure that such processing ceases when the request is legitimate and needs to be respected.

Data subjects have right to object, on request and free of charge, to the processing of personal data relating to them for purposes of direct marketing.

Automated decision making

Data subject has the right to object to any automatic decision-making (including profiling).

Each Controller and/or Processor, as appropriate, will have determined which processes entail automated decision-making (including profiling) and will have established measures to allow data subjects to object to such automated decision making and profiling. Suitable measures are in place to safeguard the data subject's rights and freedoms and legitimate interest, at least the right to obtain human intervention on the part of the Company/controller, to express his or her point of view and to contest the decision.

Timely response to exercise of rights

Each Controller and/or Processor, as appropriate, must confirm to data subjects without delay whether data relating to them are processed and communicate the data to them in an intelligible form. Each Controller and/or Processor, as appropriate, should implement internal procedures to be able to provide a timely response to the requests of data subject for the exercise of his rights.

Measures must be implemented in a way that effectively allows an individual to exercise his or her right to personal data, and that enables Each Controller and/or Processor, as appropriate, to respond to such request appropriately within the required timeframes.

Notification to recipients

In case of a legitimate exercise of rights to rectification, erasure, or restriction of processing recipients of the personal data should be informed of the rectification, erasure of that data or of the restriction of processing.

Each Controller and/or Processor, as appropriate, should have a procedure in place for communicating any rectification or erasure of personal data or restriction of processing to the recipients to whom the personal data has been disclosed and for disclosing these recipients to the data subject, if so requested.

Data protection documentation system

Register of processing

Each Controller and/or Processor, as appropriate, about their processing activities must set up a relevant record, maintained in writing (including in electronic form) and made available easily and swiftly to the supervisory authority on request, as per applicable legal requirements within their respective Member States. The record of processing activities shall contain all the information required by GDPR.

Consequently, the Controller shall have an up-to-date overview of all personal data processing activities and shall maintain records within the Project, that meet the legal requirements posed by the GDPR. By so doing, the Controller will be able to demonstrate compliance to any Supervisory Authority or other state or EU authority concerned.

For the avoidance of doubt, each Project Partner carries the same responsibility above within its own respective organisation.

Register of data breaches

A specific register where the breaches must be recorded together with other information specified by the law, must be maintained by the Controller and shown to the Supervisory Authority upon request. This register is an important element of the data protection documentation system.

Project Partners need to notify immediately and in writing the Controller of any personal data breach within their respective organisations that affects execution of the Project in any way, and to cooperate with the Controller while applying relevant GDPR legal requirements.

Data protection assessment

Assessment

If a Data Protection Impact Assessment ("**DPIA**") is carried out under the Project, the Controller shall ensure that personal data receives the appropriate level of protection in accordance with the assessed data protection risk.

The decision whether to carry out a DPIA under the Project, unless undertaken in respective Project contract, will be made by the Controller upon prior written consultation with the Project Partners.

i. Adequacy of protection

The Controller, assisted by Project Partners, should have a process in place in order to assess for all processing the risks of varying likelihood and severity for the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of personal data processing.

ii. Impact assessment in case of high risk (DPIA)

When the preliminary assessment highlights that processing represents high risks, a formal and documented DPIA is carried out by ascertaining possible impact on data subject.

DPIA is conducted in such a way to meet all the requirements set forth by the GDPR (art. 35) in order to confirm the quality and validity of the findings.

iii. Prior consultation to Supervisory Authority

The Controller has a process in place and roles are assigned in order to ensure that when a DPIA determines that the processing represents high risks, the competent Supervisory Authority is consulted prior to the processing.

Technical and organizational measures

The Controller and each Project Partner, as appropriate, adopts appropriate technical and organisational measures about Project execution (the "**Measures**"), and reviews and updates them where necessary, to ensure and to be able to demonstrate that processing is in compliance with GDPR.

Each Project Partner shall notify relevant Measures to the Controller in writing. In the event of any queries or further requests by the Controller, each Project Partner undertakes to address them duly and in writing.

If any Project Partner has notified the Measures to its competent Supervisory Authority, it shall inform the Controller thereof, and shall provide respective copies thereof.

Data breach

According to GDPR, the Controller and/or Processor, as appropriate, has to implement adequate Measures in order to prevent personal data breaches.

In addition, the Measures should be able to minimize the adverse effects in case a security breach to personal data relating in any manner to the Project occurs anyhow.

Should a data breach occur, GDPR sets forth that the Controller and/or Processor, as appropriate, has to notify it to the Supervisory Authority providing specific information, without undue delay and in any case no later than 72 hours from the time of knowledge.

When the breach leads to significant risk of serious adverse effects on the data subject(s) or serious adverse consequences for the protection of personal data, also the latter must be informed without undue delay.

Data transfers to third countries

No international transfers of personal data are expected to take place under the Project.

If any Project Partner wishes to carry out such personal data processing, it shall notify the Controller in writing and in advance. Unless otherwise expressly specified, any international data transfers carried out by any Project Partner for any reason during Project execution take place at its own exclusive liability and responsibility; same Project Partner shall hold all other Project Partners (including the Controller) harmless from any legal or other claims arising for such personal data processing.

Sanctions and damages

In case of violation of data protection principles and rules, each Project Partner (including the Controller) is responsible for damages and is subject to sanctions. Possible violations may involve civil liability and sanctions to ensure that any relevant damage is compensated.

The Project Partner (including the Controller) that is liable for said damages and/or sanctions shall hold all other Project Partners harmless from any claims, costs, and expenses arising from relevant GDPR infringement.

Deliverable Scoring Sheet

	URBANE Deliverable Scoring Sheet	
URBANE	Deliverable No:	D7.1
	Deliverable Title:	Data management and ethics
	Lead Beneficiary	UOC
	Reviewer Name	Maria Aurora Quijada Castillo
	Review Date	[17/02/2023]

Grading Scheme: Please paint the 'Score' box with the appropriate colour.		Good quality. Perhaps some minor comments.
		Reasonable quality, but some revision is necessary.
		Substantial revision and / or additional work is necessary.

Please note that a red score in the 'Overall' section in the end means the deliverable must undergo peer review again to approve the revised version.

Criterion	Description	Grade	Reviewer Comments	Author Response
Language	The deliverable is easy to understand, with good use of English, and suitable terminology.		The language is clear and easy to understand, even there is some "decorative" information that would not be necessary to include	
Visuals	Fonts, figures, tables etc. are easy to read and referenced in the text.			
Glossary	The glossary of the deliverable is complete (acronyms, unusual terms).			
Clarity	Vision, contributions & state of the art improvements are discussed explicitly and are clear.		We consider it is not clear, because it doesn't follow the template of the Call, so when a reviewer reads the document, it is not easy to be sure that everything that is needed is included.	Updated based on the DMP HE template
Symbols	Mathematical symbols and nomenclature are well-defined and understood.			

Template Application	The template is successfully applied.		We are not sure to which template you refer. If you refer to the Template of the DMP, then the template of the Call is not applied.	The DMP of the URBANE deliverable has been applied as well as the DMP HE template
References	The deliverable uses a consistent style to cite all external work referenced in the document.			
Objectives	The deliverable clearly addresses the objectives of the involved tasks.		Not all the definitions and decisions that have to be taken into account in a DMP are fulfilled in this document, for this reason we consider that the deliverable does not address all the objectives.	Updated based on comments received.
DoA Compliance	The content clearly contributes to the project plan and is consistent with the DoA.			
Task Mapping	It is clear which WP Tasks inform all parts of the deliverable's main content.			
Methodology	The methodological framework is explained clearly and the approach is scientifically sound.		In the writing of a DMP the methodology should be related to the template used. As not Horizon Europe template has been used, then we consider that the methodological framework is not explained clearly.	Updated based on the DMP HE template
Contributions	Challenges are clearly addressed and the document stimulates further research.		The document should stimulate the updating of the DMP during the project (and not only at the end) more than further research.	In Chapter 8, a biannually revision is now foreseen.
Conclusions	All key contributions and challenges are discussed clearly and are reflected in the deliverable.		We have included some comments about questions not addressed in the DMP or addressed with mistakes, that should be reviewed.	Updated based on comments received.
Overall	The deliverable is of good quality and can be finalised in time.		We would recommend taking into account the comments included in the text.	Updated based on comments received.
Suggestions and Comments (Reviewer)				