D7.2 - Initial Data Management Plan

Deliverable Number	D7.2
Deliverable Type	DMP - Data Management Plan
Dissemination Level	PU (Public)
Deliverable Responsible	Rafael Afonso (UniLU)
Document Version & Status	v1.0 | Final version

Project Acronym	NEXTLOGIC
Project Title	Next-Gen urban freight logistics for net zero emissions through innovative solutions
Grant Agreement Number	101238585
Project Coordinator	University of Luxembourg
Project Website	www.nextlogic-project.eu

Co-funded by the European Union

NEXTLOGIC has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101238585

NEXTLOGIC is a project under the CIVITAS Initiative. Read more – civitas.eu

Funded by the European Union. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them

Author(s)

Name	Organisation
Rafael Afonso	Universite du Luxembourg (UniLU)
Jiří Moc	Skoda Auto Vysoka Skola ZU (SAU)
Radim Lenort	Skoda Auto Vysoka Skola ZU (SAU)

Reviewers

Name	Organisation	Date
Simone Bosetti	LuxM	2026-06-02
Gabriel Tilg	Trans	2026-06-02
Artur Jop	WCG	2026-06-15

Change History

Version	Date	Name/Organisation	Description
0.1	2026-04-14	Rafael Afonso (UniLU)	Table of Contents
0.2	2026-04-30	Rafael Afonso (UniLU)	Initial draft
0.3	2026-05-08	Jiří Moc (SAU)	First additions from co-authors
0.4	2026-05-29	Radim Lenort and Jiří Moc (SAU)	Final additions from co-authors
0.5	2026-06-01	Rafael Afonso (UniLU)	Draft for internal review
0.6	2026-06-22	Rafael Afonso (UniLU)	Integration of reviewers' comments
1.0	2026-06-29	Rafael Afonso (UniLU)	Final version for submission

Table of Contents

List of Figures

List of Tables

1. Executive summary

The present deliverable presents the first Data Management Plan (DMP). It aims to provide an overview of the datasets expected to be collected or generated throughout the project and to define the consortium's data management policy with regards to these datasets. Moreover, the DMP aims to ensure that appropriate procedures and mechanisms for data management - from data collection to processing and sharing - are established and consistently followed.

This DMP will be reviewed and updated at least three times during the project duration, as the activities become further specified.

- First revision: M18
- Second revision: M36
- Final revision: M48

Keywords: Data Management Plan, GDPR, FAIR principles, Digital Twin, Mobility Data Space, anonymisation

2. Introduction

NEXTLOGIC is a four-year Horizon Europe project supporting cities in their transition towards climate neutrality by rethinking how urban space, mobility, and logistics are planned and managed. To achieve this objective, a combination of digital and physical solutions and tools will be deployed across eight European Mission Cities, with a digitally enabled platform at the core of the project.

Given NEXTLOGIC's strong focus on digital tools and their inherent reliance on data, effective data management constitutes a critical component of the project. Ensuring that collected, processed, and shared data are findable, accessible, interoperable, and reusable (FAIR) is essential for supporting the project objectives and enabling the development of interoperable Digital Twin and urban logistics solutions.

The structure of the deliverable is as follows:

- **Section 2** introduces the scope of the deliverable, outlining both its objectives and the general approach to data management.
- **Section 3** presents an overview of the data types and sources considered, which will be further updated in future revisions of the deliverable.
- **Section 4** describes the approaches adopted to ensure that research data adhere to the FAIR principles.
- **Section 5** outlines the conditions related to data security and privacy.
- **Section 6** addresses the ethical dimensions, guidelines, and implications of the project.
- Finally, **Section 7** provides a description of the resources allocated to data management.

2.1 Scope and objectives

The objective of this Data Management Plan (DMP) is to describe the data management processes within the NEXTLOGIC project, ensuring compliance with applicable regulatory frameworks, including the European General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) [1], and alignment with the FAIR (Findable, Accessible, Interoperable, Reusable) principles.

In addition, the DMP defines the procedures and mechanisms for the collection, processing, sharing, preservation, reuse, and further exploitation of data generated and used throughout the project. It also outlines the data-sharing standards to be implemented over the course of NEXTLOGIC, with particular attention to primary data generated through project activities.

Specifically, the DMP provides information on:

- The types of data to be collected, processed, and generated.
- The handling of research data during and after the completion of the project.
- The frameworks and standards to be applied.
- The conditions under which data will be made publicly available.
- The procedures for data storage, management, and preservation throughout the project lifecycle and beyond.

The NEXTLOGIC DMP is a living document and will be updated throughout the project to ensure continued alignment with the above-mentioned objectives. Three revisions are planned, as outlined in Table 1.

Table 1. List of Data Management Plan deliverables of NEXTLOGIC

Deliverable No	Deliverable Name	Type	Due Date (Month)
D7.2	Initial Data Management Plan	DMP - Data Management Plan	M6
D7.3	First updated Data Management Plan	DMP - Data Management Plan	M18
D7.4	Second updated Data Management Plan	DMP - Data Management Plan	M36
D7.5	Final Data Management Plan	DMP - Data Management Plan	M48

2.2 General Approach

At the core of data management in NEXTLOGIC is the definition of processes and technical approaches for data acquisition, storage, validation, interoperability, and controlled data sharing. These activities are being addressed within Task 1.2, led by SAU, in collaboration with project partners involved in data-related activities.

To identify and structure the project's data sources, Task 1.2 has been established, involving all partners working with data. As outlined in the Section 2.3, SAU will lead the mapping of datasets to be used within the project. An initial collection of datasets from project partners is currently underway, with the existing compilation presented in Section 3.1.

To develop an updated and comprehensive view of the datasets, partners will be requested to revise the provided information based on the most recent and relevant information. As the project progresses, partners may further refine and extend the dataset descriptions based on evolving project requirements, technical developments, and pilot needs. This deliverable also provides an initial overview of datasets that may be generated during the project activities.

2.3 Data architecture

The NEXTLOGIC project will adopt a layered data architecture designed to ensure data sovereignty, interoperability, and controlled access across all participating partners. The architecture will be structured into four main layers: **Raw Data**, **Processing**, **Governance**, and **Data Sharing**. Figure 1 provides a visual overview of the NEXTLOGIC Data Architecture and outlines the interconnections between its layers.

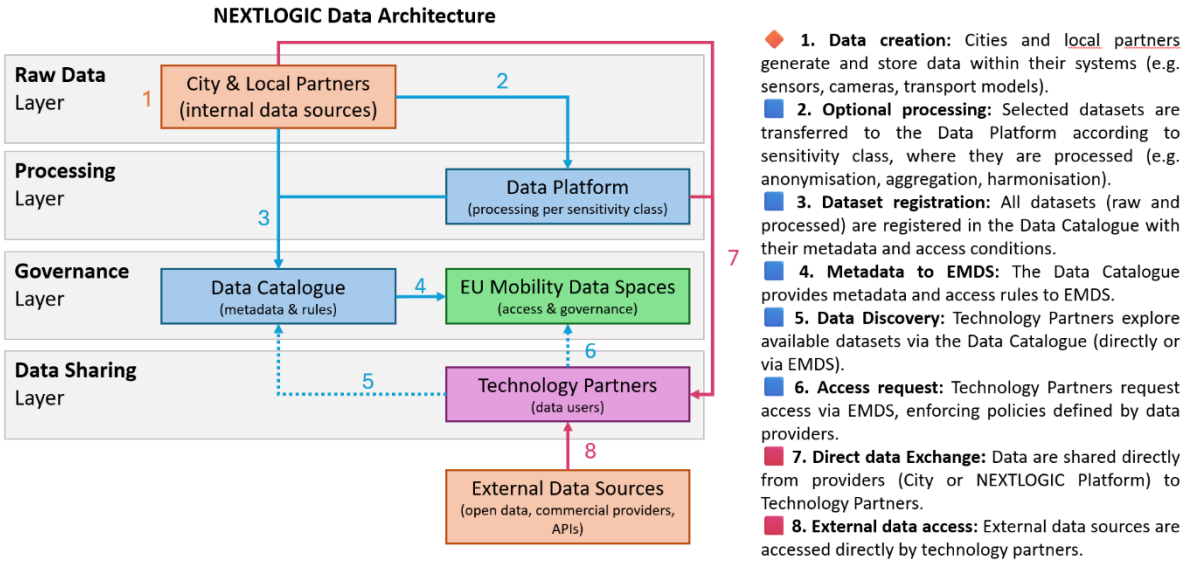

Figure 1. Overview of the NEXTLOGIC Data Architecture

At the **Raw Data Layer**, city and local partners will generate and store data within their own systems, including sources such as sensors, cameras, and transport models. This approach is intended to support that data ownership remains with the original providers, in line with the principle of data sovereignty.

Within the **Processing Layer**, datasets may be transferred to the Data Platform for processing according to their assigned sensitivity class. Three data classes are distinguished: Class A (open data), Class B (controlled data), and Class C (sensitive data). To clarify responsibilities for anonymisation and compliance verification, processing requirements are differentiated as follows:

Table 2. Description of sensitivity classes

Class	Description	Examples	SAU processing
A (open)	Publicly available data, no personal information	Road network geometry, curb boundaries, General Transit Feed Specification schedules	Optional: can be served directly without transformation
B (controlled)	Data containing potentially identifiable patterns; access restricted to authorised partners	FCD trajectories, SLZ session logs, Microhub booking events	**Mandatory**: must be pseudonymised/aggregated before API exposure
C (sensitive)	Data with direct personal identifiers or high re-identification risk	Raw GPS from cargo-bikes, camera feeds, VR behavioural signals	**Mandatory**: requires full anonymisation and DPIA clearance

For Class A datasets, transfer to and processing within the Data Platform remains optional, allowing partners to retain full control over whether their data are processed centrally. Classes B and C datasets, however, must undergo mandatory processing before any API exposure or sharing within the platform ecosystem. Where anonymisation or pseudonymisation is performed locally by partners, evidence of

such procedures will be required prior to integration into the shared data environment. While Task 1.2 will define the compliance verification procedures and associated requirements, the implementation and execution of anonymisation and pseudonymisation measures remain the responsibility of the respective data owner. Consequently, each data provider is responsible for ensuring compliance with GDPR and other applicable data protection requirements before data are shared within the project ecosystem.

Class B datasets include data containing potentially identifiable patterns, for which access is restricted to authorised project partners.

Class C datasets include data containing direct personal identifiers or presenting a high risk of re-identification, requiring full anonymisation and Data Protection Impact Assessment (DPIA) clearance prior to processing or sharing.

Additional refinements will be carried out in the coming months to ensure that all datasets, regardless of whether they are transferred to the Processing Layer, are standardised, interoperable, and aligned with the project's common semantic framework.

The **Governance Layer** is planned around a shared Data Catalogue and a phased integration with the Mobility Data Space (MDS) [2]. Datasets will be registered with metadata descriptions, access conditions, and applicable rules. The shared Catalogue will serve as the primary mechanism for data findability and transparency, while metadata and access policies may be shared with MDS for policy-based and governed data access.

In the **Data Sharing Layer**, technology partners will discover available datasets through the Data Catalogue, either directly or via the MDS. Access to data will be requested through MDS, which enforces the conditions defined by data providers. Once access is granted, data can be shared either directly from the providers (e.g. city partners or the Data Platform) or accessed through external data sources such as open data portals, commercial providers, or APIs.

The overall data flow will follow a structured process: data are created and stored by providers, optionally processed, registered with metadata, discovered by users, and accessed under controlled conditions. In parallel, external data sources can be integrated directly by technology partners where relevant.

This architecture is intended to support a balanced approach between data sharing and control, underpinned by the following key principles:

- **Data sovereignty**, ensuring that data remain under the control of their owners.
- **Trust and security**, through controlled and policy-driven access mechanisms.
- **Scalability**, supporting integration across multiple cities and partners.
- **Flexibility**, accommodating both raw and processed data.
- **Interoperability**, aligned with European data space standards.
- **Reusability**, enabling long-term value beyond the project.
- **Exploitation**, supporting open and innovation-friendly data use where possible.

3. Data summary

The NEXTLOGIC project will collect, process, and generate a diverse range of datasets to support transport modelling, Digital Twin development, behavioural analysis, and urban logistics optimisation. These datasets originate from multiple sources, including existing data provided by the eight pilot cities: Dublin, The Hague, Aarhus, Wrocław, Differdange, Heidelberg, Frankfurt, and Bergamo. Open geospatial data, road network information, and public transport schedules in GTFS and NeTEx formats will be sourced from publicly available repositories and platforms [2], [4]. For datasets that are neither publicly available nor accessible within the consortium, NEXTLOGIC will rely on external data providers.

3.1 Features of the collected data

Shared data catalogues specific to each pilot site will be gathered progressively as the project progresses. The shared data catalogue will include the following fields, aligned with the technical requirements B-01 collaboratively defined by Task 2.1 and Work Package 2 (WP2):

- Dataset identifier
- CRS (coordinate reference system) in EPSG (European Petroleum Survey Group) code
- Data format
- Sensitivity class.
- Data provider/origin.
- Update frequency.

Table 3 summarises the main categories of data to be collected and processed within the project, together with the associated formats, standards, and intended use.

Table 3. Summary of the data to be collected and processed by NEXTLOGIC, subject to iterative updates throughout the project

Data Category	Data Type/Standard	Description
Geospatial vector data	GeoJSON [5]	Exchange format for web APIs and small-to-medium datasets
	GeoParquet [6]	Columnar storage for large geospatial datasets and data lake analytics
	OGC WFS, OGC API - Features [7], [8]	Standardised access service to geospatial vector features
Raster and 3D city models	GeoTIFF/Cloud-Optimised GeoTIFF (COG) [9], [10]	Satellite and aerial imagery

Data Category	Data Type/Standard	Description
	CityGML 3.0/CityJSON [11], [12]	3D models for Digital Twin visualisation and spatial simulation
	STAC [13]	Spatiotemporal asset catalogue for raster and point cloud collections
Transport and traffic data	DATEX II [14]	Road traffic conditions and SLZ occupancy
	GTFS/NeTEx [2], [4]	Public transport schedules and real-time feeds
Derived and model outputs	Aggregated KPI datasets	Journey times, transfer durations, parking search times, congestion hotspot maps, carbon footprint estimates, parcel distribution maps
	Digital Twin simulation outputs	Traffic flows, curbside occupancy, Microhub user metrics
Sensor and behavioural data	Behavioural and physiological signals	Data retrieved from VR experiments through sensors, heart monitors, and headset placed on users; data anonymised at point of collection
	GPS, accelerometer, and gyroscope streams	Data collected from the NEXTLOGIC mobile application with explicit GDPR consent, anonymised before storage
	EV charging session records	Duration, energy delivered, location, occupancy, dwell time
Expert input and interviews	Minutes, notes, and documents	Within the consortium or outside of the consortium; gathered via interviews, workshops, meetings, etc.
Surveys, consultations and participation in events	Survey answers, minutes, notes, and documents	Surveys with external parties, public workshops, consultations, webinars and events, with outputs and results for the project will be treated with data protection and privacy regulations.

3.1.1 Software development

The NEXTLOGIC Platform, consisting of a DT, ADAV and XR, is an iterative implementation by combining, validating and testing several different tools. The platform will be simultaneously general to ensure post-project uptake and site-specific to guarantee local implementation within the project pilots.

Software developed is subject to IPR provisions, governance and ownership will be defined during the activities and duly identified and included. Development of NEXTLOGIC tools and software doesn't imply the publication of algorithms or software previously developed by the project partners and indicated as background and provided data as per Grant Agreement [15] and Consortium Agreement [16].

3.2 Anonymisation

Specific processing procedures will be applied depending on the data type and sensitivity level.

In accordance with Article 5 of Regulation (EU) 2016/679 (GDPR) [1], and the project's data governance framework, all datasets classified as Class B (Controlled) or C (Sensitive) will undergo mandatory anonymisation or pseudonymisation prior to any cross-partner sharing or API exposure.

Table 4 presents examples of the data types collected, together with their corresponding processing procedures and privacy measures.

Table 4. Processing and privacy safeguards per data type

Class	Date Type	Processing and Privacy Measures
A (open)	Road network geometry and OSM data	Publicly available open datasets requiring no anonymisation or pseudonymisation procedures.
A (open)	GTFS and public transport schedule data	Open transport scheduling data used for routing and multimodal analysis. No personal data processing involved.
B (controlled)	AR parking occupancy application data	The AR application will access only aggregated parking occupancy information and will not process or expose raw camera feeds.
B (controlled)	Anonymised MUV trip datasets	Mobility trip data will be anonymised and aggregated before integration into the shared data environment.
B (controlled)	Aggregated SLZ occupancy datasets	Only aggregated occupancy metrics will be shared. No raw identifiers or session-level personal data will be exposed.
B (controlled)	FCD vehicle trajectories	Vehicle trajectories will be pseudonymised and aggregated prior to cross-partner sharing or API exposure. Personally identifiable information will not be exposed to downstream consumers.

Class	Date Type	Processing and Privacy Measures
B/C (controlled/ sensitive)	SLZ session data	Phone numbers, partial licence plates, and related identifiers will be anonymised or pseudonymised prior to storage or external access. Aggregated occupancy indicators may be generated for operational analysis.
C (sensitive)	Camera-derived occupancy data (EXE/PKUN systems)	AI-based processing will be conducted directly on-device to generate occupancy counts and traffic indicators. Raw video streams and identifiable footage will not be transferred or stored within the platform infrastructure. A DPIA will be completed in accordance with GDPR Article 35.
C (sensitive)	Behavioural and physiological signals from VR experiments	Personal data will be anonymised at point-of-collection.

Compliance with anonymisation and pseudonymisation requirements will be verified through the platform governance framework before datasets become accessible. Processed datasets will include verification metadata (e.g._complete status flags), while policy enforcement mechanisms implemented through the governance layer and Open Policy Agent (OPA)-based controls will ensure that datasets not meeting the required privacy and processing conditions cannot be exposed through APIs or shared services.

As stated in Section 2.3, data owners are responsible for implementing and executing anonymisation and/or pseudonymisation measures in accordance with the requirements and procedures defined under Task 1.2.

4. FAIR data

Ensuring that collected, processed, and shared data are findable, accessible, interoperable, and reusable (FAIR) is essential for supporting the project objectives and enabling the development of interoperable Digital Twin and urban logistics solutions.

4.1 Making data findable

At the outset of the project, efforts concentrate on identifying existing datasets that can be reused. The findability of these datasets depends largely on the nature and characteristics of their original sources. In the domain of logistics, traffic and transport, data are generally accessible either through commercial providers (e.g. sector-specific companies) or via public authorities responsible for transport systems and land use.

In addition, the project will explore further data sources through open data portals managed by public administrations, as well as European-level platforms such as the European Data Portal. These platforms provide structured search functionalities, including keyword-based classification systems, which support the efficient discovery of datasets across thematic domains.

All data used for, and resulting from, research activities and the production of scientific publications will be made available through a general-purpose repository (e.g. Zenodo [17]).

To ensure that project data are findable, a Digital Object Identifier (DOI) will be assigned to each relevant research publication. All datasets made openly available will be accompanied by comprehensive metadata to facilitate discovery by third parties. Each metadata record will include a set of keywords to support efficient search and retrieval.

Through the metadata provided and the assignment of DOIs to publications and research outputs, project results and, where possible, the respective datasets will be made findable. However, where the project relies on data that cannot be shared due to restrictions (e.g. confidentiality, intellectual property rights, personal data protection, or inability to ensure adequate anonymisation), such data will not be made openly available by the consortium.

4.2 Making data accessible

The Mobility Data Space (MDS) , based on the Dataspace Protocol (DSP 2025-1), was identified as the target governance architecture for NEXTLOGIC. However, full integration is not expected to be fully operational by M12, when the first release of the NEXTLOGIC Platform is planned. Hence, the project will initially implement tiered access model, which will progressively transition towards MDS-based governance.

A description of each phase is provided below, while an overview of the implementation timeline is presented in Table 5.

Table 5. Timeline of data governance model

Timeline	Access governance model
M1-M12	Tiered access model
M12-M18	Progressive migration from the tiered access model to Mobility Data Spaces

Timeline	Access governance model
M18+	Mobility Data Spaces governance model

4.2.1 Tiered access model

During the initial project phase, **controlled data access** will be implemented through OGC API endpoints combined with Identity-driven (Identity and Access Management tool) Role-Based Access Control (RBAC). This interim solution provides authenticated and authorised access management equivalent to the intended MDS governance model without requiring full dataspace infrastructure deployment. A migration pathway toward MDS-governed access control will be maintained for later project phases (M18+), once the Dataspace Protocol ecosystem and partner connector availability have matured.

Table 6 illustrates the tiered access under which the NEXTLOGIC platform operates, explicitly aligned with the sensitivity class defined in Table 2 (Classes A, B, C).

Table 6. Access mechanism per sensitivity class

Class	Access Tier	Access Mechanism
A (open)	Open access	Direct OGC API access; no authentication required
B (controlled)	Restricted access	OGC API + Keycloak RBAC authentication and authorisation
C (sensitive)	Highly restricted access	OGC API + Keycloak RBAC authentication and authorisation, anonymisation requirements, and DPIA clearance

Class A (Open) datasets, containing publicly available and non-personal data, may be accessed openly through standard APIs or published repositories.

Class B (Controlled) datasets, containing potentially identifiable patterns, will be accessible only to authorised project partners through authenticated access mechanisms.

Class C (Sensitive) datasets, containing direct personal identifiers or presenting a high re-identification risk, will remain strictly restricted and accessible only through secure and controlled environments following anonymisation and, where applicable, DPIA clearance.

Datasets from both Class B and C will remain within the T1.2 platform infrastructure and are accessible only to authorised project partners and pilot city representatives through authenticated endpoints and role-based permissions.

4.2.2 European Mobility Data Spaces

Following recommendations from key project partners and in alignment with the objectives of the Mobility Data Space (MDS), the MDS was selected as the target governance architecture for later phases of the project (M18+).

Within MDS, data providers will register datasets through connector catalogues associated with usage policies, while consumers will discover datasets via DSP catalogue endpoints and initiate contract negotiation procedures. Access to data will be governed through Policy Enforcement Points (PEPs), ensuring that only parties with valid contractual permissions can access datasets. Data exchanges within the MDS ecosystem will occur peer-to-peer, without centralised storage on the MDS platform itself.

4.3 Making data interoperable

Data exchange within NEXTLOGIC is based on open standards developed by organisations such as OGC, IETF, W3C, CEN, and the EU SEMIC framework, ensuring alignment with the objectives of the MDS. The adopted approach addresses three layers: data encoding formats, API and service protocols, and semantic vocabularies.

Table 7. Data encoding formats

Format	Standard	Data type	Primary use in NEXTLOGIC
GeoJSON [5]	IETF RFC 7946	Vector features	API responses, SLZ and road network feature exchange
GeoParquet [6]	GeoParquet 1.1.0	Large-scale vector	Analytics-ready batch datasets, FCD trajectories
GeoTIFF/COG [9], [10]	OGC GeoTIFF	Raster/imagery	Environmental and emissions raster layers
CityGML [11]	OGC CityGML 3.0	3D city models	Canonical exchange format for 3D urban models from pilot cities
CityJSON [12]	OGC Community Standard 2.0.0	3D city models	Lighter processing format; ETL pipelines, DT model ingestion
3D Tiles [18]	OGC Community Standard	Streaming 3D	Web-based 3D visualisation (CesiumJS / OpenLayers)
GTFS [3]	MobilityData GTFS	Transit schedules	Public transport schedule data from pilot cities
GTFS Realtime [19]	MobilityData GTFS-RT	Real-time transit	Real-time vehicle positions and service alerts
NeTEx [4]	CEN EN 12896 (Transmodel)	Transit exchange	European standard for public transport data; where cities supply NeTEx
SIRI [20]	CEN EN 15531 (Transmodel)	Real-time transit	Real-time service information, alternative to GTFS-RT

DATEX II [14]	CEN 16157	Road traffic	SLZ status, traffic events, ITS data
GBFS [21]	MobilityData GBFS	Shared micromobility	Cargo-bike and micro-mobility vehicle feeds

Platform-internal data will be published through open standards based on the OGC API family. Existing WFS and WMS services already operated by pilot cities will be consumed as external input sources without modification. Newly developed platform interfaces will implement OGC API standards wherever applicable.

- **OGC API - Features**: primary REST/JSON endpoint for vector features
- **OGC SensorThings API**: observation and event streams for SLZ occupancy, cargo-bike telemetry, environmental sensors, and traffic detections; deployed via FROST-Server; supports HTTP pull and MQTT push.
- **OGC API Coverages**: raster and grid data access.
- **OGC API Tiles**: tile-based map serving.
- **OGC API Processes**: triggering and managing analytical workflows.
- **OGC API Records**: metadata catalogue endpoint.
- **OpenAPI**: interface specification for co-designed city APIs.

4.4 Make data reusable

Every dataset deposited in a repository or shared through the platform will be accompanied by documentation describing:

- The data collection or generation methodology (e.g. sensor type, sampling rate, aggregation method, and pilot city).
- Attribute definitions and measurement units based on the Task 1.2 canonical naming scheme.
- Any cleaning, anonymisation, pseudonymisation, or transformation procedures applied prior to storage or sharing.
- Versioning and changelog information.
- References to the payload standards with which the dataset complies.

Data will be published through open and royalty-free standards, including OGC API Features, OGC API Records, and SensorThings API, all of which support multiple independent implementations. Hence, no NEXTLOGIC-specific software will be required on the consumer side to access or process the data. Restricted datasets will be made accessible only after appropriate authorisation and contract negotiation procedures through DSP-compatible connectors, including Eclipse EDC-compatible implementations.

Quality assurance procedures will be applied at three stages of the data lifecycle: source identification, metadata onboarding, and payload ingestion.

Prior to onboarding a new data source, the consortium will evaluate it against four main criteria:

- Technical accessibility (e.g. API availability, supported formats, update frequency).

- Data quality dimensions (e.g. accuracy, completeness, consistency, and timeliness).
- Interoperability readiness (e.g. compliance with recognised standards and schema documentation availability).
- Legal and ethical constraints (e.g. licence clarity, GDPR risk level, and access restrictions).

Data sources that do not meet the minimum requirements in any of these categories will not be integrated into the project platform or shared data environment.

The operational responsibilities, automation procedures, and technical enforcement mechanisms associated with these quality assurance checkpoints will be further refined and specified in subsequent revisions of the DMP.

5. Data security

NEXTLOGIC addresses three security domains: data in transit, data at rest, and access control.

All data transfers shall use **TLS 1.2 or higher**. Unencrypted transport shall not be permitted for any project dataset, regardless of access classification.

Datasets classified as Class B (Controlled) or C (Sensitive) shall not be published to any federated or public catalogue. They shall remain within the NEXTLOGIC infrastructure and shall be accessible only to authorised project partners and pilot city representatives via authenticated endpoints.

Backup and recovery procedures for the platform will be specified in a future deliverable, including backup frequency, retention period, Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

6. Ethics

The NEXTLOGIC consortium shall ensure that no privacy or data protection rights are violated and that all data management procedures comply with applicable national and European legislation. In particular, the consortium will ensure full compliance with European GDPR, as well as any additional national requirements applicable within the partners' countries.

6.1 Protection and management of Personal Data

The consortium will implement the necessary technical and organisational measures to ensure the confidentiality, integrity, availability, and security of personal data, including protection against unauthorised access, accidental loss, destruction, alteration, or disclosure.

The design of surveys, interviews, questionnaires, and other data collection activities will follow the principle of data minimisation, ensuring that only personal data strictly necessary for the purposes of the project are collected and processed. Where personal data processing is required, the legal basis will be identified in accordance with GDPR provisions, including consent, scientific research purposes, or tasks carried out in the public interest, depending on the nature of the activity and the applicable national framework.

Participant Information Sheets, Privacy Notices, and informed consent procedures will be developed during the subsequent stages of the project and included in future revisions of the DMP. Consent to participate in project activities will be collected using methods that avoid the unnecessary collection of personal data (e.g. consent checkboxes in online questionnaires or registration forms).

Datasets classified as Class B (Controlled) or Class C (Sensitive) under the project's data governance framework will undergo mandatory anonymisation or pseudonymisation before any cross-partner sharing or API exposure. Raw personally identifiable information will not be exposed through the project platform or shared services.

6.2 Storage and protection

Personal data, including names, organisation, nationality, email addresses, and telephone numbers, may be collected when contacting external experts, stakeholders, and pilot participants for the purpose of obtaining information, feedback, or participation in project activities.

Such data may be collected at different stages of the project, including:

- The establishment of the Outreach Group.
- Participation in workshops, interviews, surveys, demonstrations, and pilot activities.
- Communication, dissemination and stakeholder engagement activities.

Personal data collected within NEXTLOGIC will be used exclusively for project-related purposes and will not be disclosed to unauthorised third parties. Processing activities will be limited to communication, coordination, participation management, dissemination, and feedback provision related to project activities and outputs.

Personal data will be stored within the NEXTLOGIC's shared environment on SharePoint and, where applicable, with features subject to access controls and role-based permissions. Access to personal data will be restricted to authorised project personnel directly involved in the relevant activity or task.

For datasets involving higher sensitivity levels, additional safeguards may be applied, including encryption, pseudonymisation, access logging, and restricted-access environments. Camera-derived occupancy data and other high-risk processing activities will be subject to DPIAs, where required under GDPR Article 35, prior to data ingestion or processing within the platform environment.

6.3 Retention and destruction

Personal data collected during the project, including contact information, survey responses, and stakeholder feedback, will be retained for a period of five years after the end of the project for audit, reporting, and verification purposes. During the retention period, personal data will continue to be protected using the same technical and organisational safeguards applied throughout the project lifetime.

At the end of the retention period, personal data and related records will be securely deleted or anonymised in a manner that preserves the confidentiality of the data subjects. The consortium will maintain appropriate records documenting the deletion or anonymisation procedures performed, including the categories of data removed and the date of destruction, where applicable.

7. Allocation of resources

To support the objectives of NEXTLOGIC, dedicated resources for data management have been allocated across multiple work packages, including personnel, equipment, infrastructure, and operational costs. While data management activities are primarily addressed within Task 1.2, WP2, and Task 7.4, **all project partners are responsible** for ensuring compliance with ethical, legal, and GDPR requirements, as well as with the data management procedures and guidelines established in this deliverable and its subsequent revisions.

The project includes the following data-related activities:

- **WP1:** Task 1.2 will identify relevant datasets, support the development of a secure data-sharing platform, and define project data requirements. Tasks 1.1, 1.3, and 1.4 will generate primary data through surveys, interviews, and consultations involving cities and project partners.
- **WP2**: WP2 will identify, process, and integrate multiple data streams into the DT platform and will generate additional datasets through XR and ADAV activities.
- **WP3**: WP3 will identify datasets and external data sources required for the definition and refinement of project solutions.
- **WP4**: WP4 will use data generated in WP1, WP2, and WP3, while also generating additional datasets derived from pilot preparation, implementation, monitoring, and post-implementation activities. These outputs will support the communication, dissemination and exploitation activities in WP6, as well as the impact assessment and the development of business and governance models in WP5.
- **WP7**: Task 7.4 is specifically dedicated to the development and continuous update of the DMP. Led by UniLU, in collaboration with all project partners, the task will support the governance and management of data associated with the project.

Dedicated budget lines have been allocated for data acquisition, maintenance of the central repository for urban freight and mobility data, cloud storage services, and physical data collection infrastructure across the consortium.

The project website will be maintained by LuxMobility for a minimum period of three years following the completion of the project to support the long-term dissemination of project results.

Finally, **data management is a shared responsibility across the consortium**. Each partner shall allocate the necessary resources to ensure that all data-related activities comply with the project's Data Management Plan, as well as applicable European and national legislation.

8. Abbreviations

Term	Definition
ADAV	Advanced Data Analytics and Visualisation
API	Application Programming Interface
AR	Augmented Reality
CEN	European Committee for Standardisation
CRS	Coordinate Reference System
DAPS	Dynamic Attribute Provisioning Service
DATEX II	Data Exchange II
DMP	Data Management Plan
DOI	Digital Object Identifier
DPIA	Data Protection Impact Assessment
DSP	Dataspace Protocol
DT	Digital Twin
EDC	Eclipse Dataspace Connector
EN	European Standard
EPGS	European Petroleum Survey Group
ETL	Extract, Transform, Load
EXE	EXE, A.S.
FAIR	Findable, Accessible, Interoperable, Reusable
FCD	Floating Car Data
GBFS	General Bikeshare Feed Specification
GDPR	European General Data Protection Regulation
GTFS	General Transit Feed Specification
IETF	Internet Engineering Task Force
ITS	Intelligent Transport Systems
MDS	Mobility Data Space
MQTT	Message Queuing Telemetry Transport
NeTEx	Network Timetable Exchange

Term	Definition
OGC	Open Geospatial Consortium
OPA	Open Policy Agent
OSM	OpenStreetMap
PKUN	Parkunload
PU	Public
RBAC	Role-Based Access Control
RFC	Requests for Comments
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIRI	Service Interface for Real-time Information
SLZ	Smart Loading Zone
TLS	Transport Layer Security
WFS	Web Feature Service
WP	Work Package

9. References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[2] Mobility Data Space. Available: https://mobility-dataspace.eu

[3] General Transit Feed Specification (GTFS). Available: https://gtfs.org

[4] Network Timetable Exchange (NeTEx). Available: https://transmodel-cen.eu

[5] GeoJSON. Available: https://geojson.org/ and https://geojson.io

[6] GeoParquet. Available: https://geoparquet.org/

[7] Open Geospatial Consortium Web Feature Service (OGC WFS). Available: https://www.ogc.org/standards/wfs

[8] Open Geospatial Consortium API - Features (OCG API - Features). Available: https://www.ogc.org/standards/ogcapi-features

[9] GeoTIFF. Available: https://www.ogc.org/standards/geotiff/

[10] Cloud Optimised GeoTIFF (COG). Available: https://www.ogc.org/standards/ogc-cloud-optimized-geotiff/

[11] CityGML. Available: https://www.ogc.org/standards/citygml/

[12] CityJSON. Available: https://www.ogc.org/standards/cityjson/

[13] SpatioTemporal Asset Catalog (STAC). Available: https://www.ogc.org/standards/stac/

[14] DATEX II. Available: https://datex2.eu

[15] "NEXTLOGIC Grant Agreement Number 101238585”, 2025

[16] "NEXTLOGIC Consortium Agreement v1.0”, 2026-04-22

[17] Zenodo. Available: https://zenodo.org

[18] 3D Tiles. Available: https://www.ogc.org/standards/3dtiles

[19] General Transit Feed Specification Realtime (GTFS Realtime). Available: https://gtfs.org/documentation/realtime/reference/

[20] Service Interface for Real-time Information (SIRI). Available: https://transmodel-cen.eu/index.php/siri/

[21] General Bikeshare Feed Specification (GBFS). Available: https://www.gbfs.org