Co-funded by
the European Union

Ref. Ares(2024)4685054 - 28/06/2024

Project Acronym:	GREEN-LOG
Project Number:	101069892 (HORIZON-CL5-2021-D6-01 - Innovation action)
Project Full Title:	Cooperative and Interconnected Green delivery solutions towards an era of optimized zero emission last-mile Logistics

DELIVERABLE

D5.6 – Data Management Plan-Second version

Dissemination level	PU – Public
Type of Document	Report
Contractual date of delivery	30/06/2024
Deliverable Leader	EUT
Status - version, date	Final – v1.0, 28-06-2024
WP / Task responsible	WP5 / EUT
Keywords	WP5, DMP

Executive Summary

The GREEN-LOG consortium shares the vision that unrestricted access to knowledge is a fundamental human value of scientific knowledge progress and dissemination and is essential for generating growth. In this regard, GREEN-LOG ambition is to share ideas and knowledge that permit to advance sustainable transport and logistics services. Thus, GREEN-LOG embraces Open Science and Open Data as a mechanism to bring society a return of investment from our research.

The FAIR[1] Data Management guidelines are adhered to, as are the Guidelines on the Open Access to Scientific Publications and Open Data Access to Research Data. The current Data Management Plan (DMP) is the 2nd version of the GREEN-LOG's DMP and describes: (i) the handling of research data during and after the end of the project; (ii) what data will be collected, processed, and generated; (iii) which methodology and standards will be applied; (iv) whether data will be publicly shared/made open access, and (v) how data will be curated and preserved (including after the end of the project). In terms of accessibility and exploitation, most datasets generated within GREEN-LOG, and as part of the demonstrations, will be available for research purposes to all partners, after being subjected to appropriate anonymisation and securitisation measures to guarantee privacy protection in accordance with General Data Protection Regulation (GDPR) and guaranteeing industrial properties rights from data providers. Some datasets might remain private due to privacy, intellectual right protection or commercial interests. The next (third) version of the GREEN-LOG DMP (D5.7), due in M36, will provide a comprehensive list of the data sets accessible for the scientific community.

The description of the type of data and procedures to facilitate open science is updated in this version of the DMP with respect to the previous version as the project has evolved and more details on the type of data available is known.

The data to be collected and generated during the lifetime of the project includes network, hubs, supply/demand data (orders and parcels), routing data, traffic data, weather data, qualitative and quantitative questionnaire and interview data, images as well as assessment and evaluation outcomes.

The partners also contribute to novel research work and transfer the generated knowledge to the general public and wider logistics community through the publication of the deliverables, webinars, scientific publications and other communication and dissemination materials.

A repository with restricted access is available for members of GREEN-LOG consortium in the framework of the project to store the material and information related to different Work Packages and project management (e.g. contacts, meeting minutes, presentations, work plans, etc.) and other project's material produced during the project such as project deliverables, reports, or scientific publications. This repository is based in Microsoft Teams SharePoint™ application.

The data sets to be used or to be generated during the project will be stored in the GREEN-LOG Data Space which is developed within WP2. This Data Space is based on CKAN, it enables different accessibility levels and allows storage of data in multiple forms such as databases or files. An API to store and retrieve data is provided facilitating interoperability to GREEN-LOG components.

[1] F.A.I.R: Findable, Accessible, Interoperable and Re-usable

For the sharing of sensitive data, bilateral Non-disclosure Agreements (NDAs) have been signed between some logistics operators and technical partners within the consortium, beyond the Consortium Agreement. In addition, a template for NDA between third parties and the Consortium has been prepared in case any external data provider requires it.

For the data selected to be public, after the anonymisation of any sensitive information, the datasets will be made open to the general public in Zenodo, under HE GREEN-LOG community and OpenAIRE community.

Open access publications will be made available in Zenodo, GREEN-LOG webpage and, also, in Open Research Europe.

Finally, for software components envisioned to be open source, the source code will be made available on GitHub.

Deliverable Leader (organisation)	EURECAT (EUT)
Contributors (names & organisations)	NETCOMPANY - INTRASOFT SA (INTRA), HOGSKOLAN I HALMSTAD (HALM)
Reviewers (name & organisations)	MOSAIC FACTOR SL (MOSAIC), NETCOMPANY - INTRASOFT SA (INTRA)
Approved by (organisation)	NETCOMPANY - INTRASOFT SA (INTRA)

Document History			
Version	**Date**	**Contributor(s)**	**Description**
0.1	13-12-2023	EUT	Initial version. TOC
0.2	26-03-2024	EUT	First draft
0.3	18-06-2024	EUT	Peer review version
0.4	27-06-2024	EUT	Comments from peer review addressed
1.0	28-06-2024	INTRA	Final QA'ed version

Table of Contents

Table of Figures

List of Tables

Definitions, Acronyms and Abbreviations

Acronym/Abbreviation	Title
API	Application Programming Interface
CA	Consortium Agreement
CERIF	Common European Research Information Format
DMP	Data Management Plan
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
DOI	Digital Object Identifier
EU	European Union
EC	European Commission
FAIR	Findable, Accessible, Interoperable, Re-usable
GA	Grant Agreement
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
JSON	Java Script Object Notation
M2M	Machine-to-Machine
NDA	Non-disclosure Agreement
REST	Representational State Transfer
RTD	Research and Technology Development

1 Introduction

1.1 Document scope

The GREEN-LOG project aims at developing cooperative and interconnected green delivery solutions towards an era of optimized zero emission last-mile logistics.

It will establish city platforms made up of inclusive stakeholder Urban Living Labs to foster social innovation, and design and implement cutting-edge delivery solutions to accelerate systemic changes to create last-mile delivery ecosystems that are economically, ecologically, and socially sustainable. The cutting-edge simulation environment for scenario building combining different solutions to enable the integration of last-mile delivery interventions is envisioned to achieve the highest possible impact on environmental sustainability and traffic reduction, also considering their financial viability.

GREEN-LOG offers Logistics-as-a-Service platforms for interconnected city logistics, automated delivery concepts using autonomous vehicles and delivery droids, cargo-bike-based innovations for sustainable micro-consolidation, and multimodal parcel deliveries integrating public transportation. The solutions are supported by city logistics data space that supply dynamic services for proactive ecosystem optimisation while respecting the interests of stakeholders including consumers, businesses, and the city.

The approach is deployed and validated in five Urban Living Labs: Athens, Barcelona, Flanders (Ghent, Leuven and Mechelen), Oxfordshire and Ispra. Three follower cities – Arad, Helsingborg, and Valga – will be involved in testing the transferability of the proposed innovations.

GREEN-LOG will support knowledge sharing and research and innovation results uptake by society as part of the European Commission's plans Horizon Europe research projects. It is mandatory for the beneficiaries to manage the digital research data responsibly, in line with the FAIR principles. Data, either gathered or generated, is one of the valuable assets that will enable the scientific community to go beyond the results achieved by GREEN-LOG.

The starting point is to elaborate a Data Management Plan (DMP) and keep it updated throughout the course of the project. This is the second version of the GREEN-LOG DMP. After approval of the EC, it will be made public in GREEN-LOG website and in a public repository to be decided (most likely Zenodo). The DMP is considered to be a living document and it will be updated during the course of the project as the development of the data collection, curation and publication progress. It is envisioned to issue updated versions of this DMP in M36 (D5.7) and M42 of the project (D5.8). The first version was released in M6 (D5.2). For the more advanced versions, GREEN-LOG will consider publishing the DMP in specialized journals like RIO[2].

The DMP ensures that data collected, processed, and analysed during the project lifecycle are handled efficiently, ethically, and in compliance with relevant regulations. This plan also addresses data sharing, preservation, and long-term access to facilitate reproducibility and maximize the impact of the research outcomes.

[2] https://riojournal.com/

The content of this DMP has been prepared considering the template of the "Guidelines on Data Management in Horizon Europe"[3]. For future versions of the DMP, it is envisioned to use an open access web tool such as ARGOS[4] or DMPOnline[5].

1.2 Document structure

After the introduction in section 1 describing the scope of the document and its structure, a summary of the updates of this version of the DMP with respect to the first version is presented in section 2 to facilitate the reader to identify the changes.

Section 3 presents a summary of the data to be handled by GREEN-LOG project that describes the purpose of using such data, the path that data follows within GREEN-LOG according to the nature of information, the legal framework applicable, an enumeration of data types and formats as well as an estimation of the size of the data sets. This section also includes a description of the origin of data and the means to be used to handle and store the data during and after the project.

Section 4 describes the FAIR principles in general and how they are applied to GREEN-LOG.

Section 5 provides an overview of the main partners in charge of providing the infrastructure for the realization of the data management plan.

Data security both for the private and public repositories is presented in section 6, while a description of the ethical aspects involved in GREEN-LOG data management is presented in section 7.

A final conclusion section closes this deliverable.

Appendix A contains the template for the Non-disclosure Agreement (NDA) between the GREEN-LOG consortium and third parties.

[3] https://www.openaire.eu/images/Guides/HORIZON_EUROPE_Data-Management-Plan-Template.pdf
[4] https://argos.openaire.eu/splash/
[5] https://dmponline.dcc.ac.uk/

2 Data Management Plan updates

This section aims at summarising the most relevant updates with respect to the initial DMP issued in M6 [REF-01]

As the project evolves and the first round of demonstration activities is approaching (M21), more details on the nature of data and the technological implementations to support data sharing within GREEN-LOG ecosystem are available.

The most significant changes in this version are:

- Bilateral NDA's between the Greek logistics operators and the technical partner responsible for handling the raw data in the first place.
- NDA template to be signed between Project Coordinator on behalf of GREEN-LOG consortium and third parties outside the consortium providing data, if requested.
- Description of the first version of GREEN-LOG data model (entities and properties) and estimation of size of the data sets for each type.
- Description of the GREEN-LOG Data Space technological solution to handle data during the project lifetime.

3 Data Summary

3.1 Purpose and motivation

The overall motivation for data collection in GREEN-LOG is to assess the impact of the measures applied in the Living Labs and learn and provide insights that can be later used to accelerate the transition to greener and more sustainable logistics solutions.

Technology providers participating in the project require data to design and develop the technology applications included in GREEN-LOG solution as well as create the models or run simulations. Likewise, the design of business models and policies also requires data to assess their feasibility and sustainability. Finally, once the measures are applied in the Living Labs, data will be gathered to analyse the impact of GREEN-LOG solution in terms of economic, ecologic and social impact.

Beyond the scope of the project, the scientific community and technology providers can re-use the data gathered during the project as starting point for further research. Yet, the three follower cities involved in the project and any other that may be outreached during the course of the project can use the lessons learned generated by the project and applied or adapt GREEN-LOG solution or policies starting from the transferability guidelines outcomes.

Only data that is needed to perform project activities will be collected. The collection of sensitive data will be performed only if strictly necessary and with informed consent. Sensitive data will not be made public.

3.2 Dataflow

GREEN-LOG gathers data from 5 demonstration areas (Living Labs) which are used to evaluate last mile interventions and provide qualitative and quantitative information on the results of the local solutions that are implemented. A relevant amount of data is provided by the logistics operators participating in the Living Labs. Yet other data sources are also used to complement logistics operation information such as network information (road and railway), weather information and traffic data. The collected data from GREEN-LOG pilots will be available to partners who need it for their research activities, provided that appropriate anonymization and protection measures have been applied. Some restrictions apply to specific data due commercialisation potential or Intellectual Property Rights (IPR) that will be handled either through Consortium Agreement (CA) or bilateral Non-Disclosure Agreements (NDAs) as discussed in section 3.3.3. Data collected goes beyond purely data sets and includes information gathered in the co-design activities for the definition of the Living Labs and measures to be applied and the evaluation phase to gather feedback from participants. Likewise, GREEN-LOG produces more than data sets generated by GREEN-LOG components after the processing of input data and includes scientific publications, deliverables, training materials, technology assets, business models, policies and guidelines. GREEN-LOG considers Open Access publication both as a prime method for increasing its scientific impact and visibility, and an ethically sound treatment and dissemination of the results.

Figure 1 shows an overview of the data flow defined as part of the data process handling established in the DMP that covers the path from collection to publication. Data can be collected either manually or automatically via Machine-to-Machine (M2M) communications using different mechanisms that will be briefly described in following sections.

The data collected from the Living Labs will be referred as Research Data and will serve to produce scientific publications, deliverables, technology assets, business models and policies as well as data sets to support future research.

It has been established to first store the data in a restricted data repository, only accessible by project partners according to access rights (different types of restrictions may applied). It is among the aims of the Consortium to make public as much data as possible in a public repository in a second step. However, in some cases it will not be possible. Protection mechanisms for exploitable results will be analysed according to partners interests and market opportunities to decide which assets are meant to remain protected. Likewise, some data will be qualified as sensitive and will remain protected if it is not possible to convert it into non-sensitive after anonymisation processes to prevent the disclosure of personal or industrial protected data and references to use-cases and user profiles.

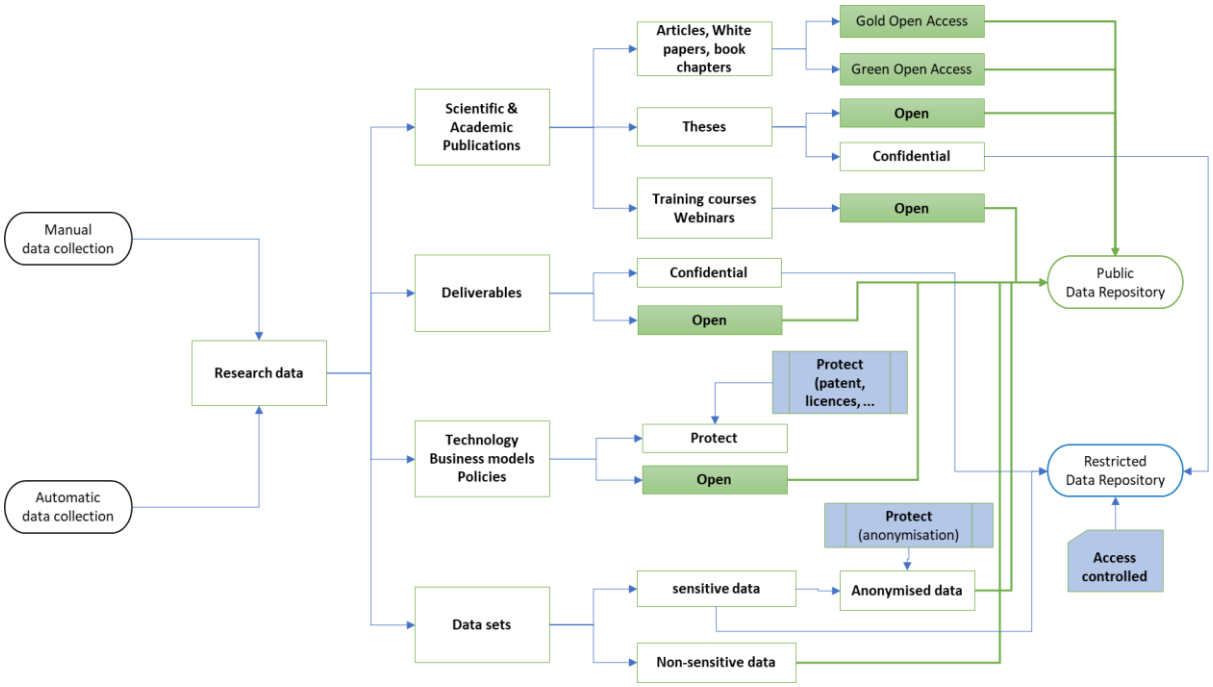

Figure 1: Data flow in GREEN-LOG

3.3 Legal framework

3.3.1 General Data Protection Regulation (GDRP)

As of May 2018, the General Data Protection Regulation (GDPR)[6] is applicable in all Member States in the European Union, as well as in the countries in the European Economic Area (EEA). GDPR updates and modernises existing laws on data protection to strengthen citizens' fundamental rights and guarantee their privacy in the digital age.

GDPR regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU[7]. It does not apply to the processing of personal data of deceased persons or of legal entities. It sets down one set of data protection rules for all

[6] 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[7] https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

companies and organisations operating anywhere in the EU and European Economic Area (EEA), for two main reasons: 1) to give people more control over their personal data, 2) level the playing field for businesses and organisations operating in the EU and EEA. GDPR grant individuals a set of rights that must be protected by any actor who processes personal data. The individual rights include the right to:

- information about the processing of your personal data;
- obtain access to the personal data held about you;
- ask for incorrect, inaccurate or incomplete personal data to be corrected;
- request that personal data be erased when it's no longer needed or if processing it is unlawful;
- object to the processing of your personal data for marketing purposes or on grounds relating to your particular situation;
- request the restriction of the processing of your personal data in specific cases;
- receive your personal data in a machine-readable format and send it to another controller ("data portability"); and
- request that decisions based on automated processing concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers. You can also have the right in this case to express your point of view and to contest the decision.

Concerning the UK, which is a non-EU country, it has a security of information agreement with the EU in place. The EU published two Adequacy Decisions on 28th June 2021, thereby establishing UK-EU agreements on the transfer of personal data under the EU's General Data Protection Regulations (EU) 2016/679 and the EU Law Enforcement Directive (EU) 2016/680. Both Adequacy Decisions can be found via the official EU website. In addition, the UK has published the UK/EU: Agreement concerning Security Procedures for Exchanging and Protecting Classified Information on the UK Government's official website.

As far as the Consortium is concerned, the CA and the Grant Agreement (GA) establish obligations and restrictions to partners. In particular, the members of the consortium must ensure personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subjects;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed; and
- processed in a manner that ensures appropriate security of the data[8].

If materials or documents are subject to moral rights or third-party rights (including IPRs or rights of natural persons on their image and voice), the beneficiaries must ensure that they comply with their obligations under the Agreement (in particular, by obtaining the necessary licences and authorisations from the rights holders concerned).

At the moment of signing the CA, each partner in the Consortium has enabled the mechanisms and resources to comply to protection of personal data, that typically is part of the data privacy and protection organisation policy. The person in charge is the Data Protection Officer who is in charge of monitoring the data handling in their organisations comply with the established

[8] https://gdpr.eu/article-5-how-to-process-personal-data/

obligations. Beyond personal data, there is a need to exchange data among partners for technical and research purposes. In this case, for each data provider, it has been established a main contact point to address data requests. . Once the GREEN-LOG data space is set up, EUT will assist partners in finding the mechanisms to upload and retrieve data, either in an automatic or manual way, depending on the possibilities of each partner. In case issues arise concerning privacy, they will be addressed with the support of EUT legal department and contacting the national Data Protection Agencies, if needed. As described in Section 6, personal data collection will always be done under informed consent. Partners will explain how all the personal data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle). The project involves human participants as researchers and logistic stakeholders. Although limited, it is envisioned to collect a certain amount of personal data concerning the following topics:

- Addresses of senders and receivers of parcels: Due to the need to calculate delivery routes, the origin and destination of parcels need to be specified. In general, GREEN-LOG components do not need to link addresses with individuals. However, the Logistics-as-a-Service platform includes a nudging engine that will persuade customers to take more sustainable delivery options according to public authorities policies and rewards schemes. In this particular case, a record of historical rewards achieved need to be stored and linked to the corresponding customer. However, the platform does not need the real name of the customer or any personal data, since to access the service only a user account (email address) is needed.
- Image recordings for evaluation: HALM envisions to use image footage to analyse user acceptance during the implementation of the Living Labs to assess GREEN-LOG solution. The analysis of the images will be performed by humans and will not be uploaded to any image processing platform. Participants will be informed about the scope of the research and the treatment of the images.
- Dissemination purposes: During dissemination task partners will reach end users with dissemination materials so contact data of end-users will be collected. Furthermore, events for promoting public acceptance, market uptake and others will be conducted. Databases of personal data will be created and feedback collected through workshops and other events Images may be recorded during workshops, events or Living Lab implementation activities to serve communication and dissemination purposes. Informed consent will be requested to use these images, and special care will be taken in not using any image that may affect personal integrity.

3.3.2 Consortium Agreement

The Consortium Agreement includes a section (section 10 Non-disclosure information) for information disclosed by a Party to any other Party in connection with the Project during its implementation and which has been explicitly marked as "confidential" at the time of disclosure, or when disclosed orally has been identified as confidential that establishes the obligations for Recipient party. In particular, article 10.2 states that:

The Recipient hereby undertakes in addition and without prejudice to any commitment on non-disclosure under the Grant Agreement, for a period of 5 years after the final payment of the Granting Authority (the Coordinator notifies the Associated Partner(s) about the date of the final payment):

- *not to use Confidential Information otherwise than for the purpose for which it was disclosed;*

- *not to disclose Confidential Information without the prior written consent by the Disclosing Party;*
- *to ensure that internal distribution of Confidential Information by a Recipient shall take place on a strict need-to-know basis; and*
- *to return to the Disclosing Party, or destroy, on request all Confidential Information that has been disclosed to the Recipients including all copies thereof and to delete all information stored in a machine-readable form to the extent practically possible. The Recipients may keep a copy to the extent it is required to keep, archive or store such Confidential Information because of compliance with applicable laws and regulations or for the proof of on-going obligations provided that the Recipient complies with the confidentiality obligations herein contained with respect to such copy.*

Despite the framework established by the Consortium Agreement, some Parties have deemed necessary to set a specific bilateral non-disclosure agreement for the sharing of sensitive information relating to logistics operation. This is the case of the NDA signed between ACS SMSA and AUEB. A similar agreement will be signed between FedEx and ACS SMSA. In this case, AUEB is responsible for the processing of the raw data sets shared by the mentioned logistics provided. Once this information is processed, meaning that information relevant to GREEN-LOG is extracted, the resulting data can be stored in the GREEN-LOG repository for other component developers to be used.

3.3.3 Non-Disclosure Agreements

The terms established by the Consortium Agreement between the parties does not apply to the exchange of information between the consortium members and third parties not participating in the consortium. At the moment of writing this deliverable (M18), this is the case of logistics operators in Flanders Living Lab, a second logistics operator in Barcelona Living Lab and the canteen tender in Ispra. In such cases, respective NDA have been prepared to be signed between the Coordinator of GREEN-LOG on behalf of the consortium and the data provider, if requested.

The NDA template can be found in the Appendix A: Non-Disclosure Agreement Template.

3.4 Data types, formats and size

GREEN-LOG will collect, process, and generate vast amounts of data of several types and formats. Table 1 summarises the information to be generated or used during the GREEN-LOG project.

Table 1: Overview of data generated or used during GREEN-LOG project

Created/ Collected/ Re-used	Type of data	Format	Dissemination level
Created	Dissemination material (roll-ups, leaflets, posters, presentations)	PDF, PNG, JPG	Public
Created	Image recordings (evaluation research)	Waw, mp4	Confidential
Created	Project website	Webdata	Public
Created	Activity on Social media and the Website	htlm, xml, text, jpg	Public (only aggregated)

Created	Deliverables	Docx, PDF	Confidential Public
Created	Public reports, scientific publications, articles	Docx, PDF	Public
Created	Registration to events organised by the consortium	Docs, Excel	Confidential
Created	Subscriptions to the GREEN-LOG newsletter	Moosend[9] platform	Confidential
Collected/ Re-used	Survey data	Forms, Docx, PDF, Excel	Confidential Public
Created	Workshop reports	Docx, PDF, Miro	Confidential Public
Created	Webinars	Webdata, wav, mp4	Public
Created/ Re-used	Academic outcomes (Master and PhD theses)	Docx, PDF	Public
Re-used	Operational data from logistics operators (e.g. networks, traffic flows, etc)	CSV, GFTS, GIS	Confidential Public
Collected	Operational data	Docx, CSV, DatexII	Confidential[10], Public
Collected	Feedback from users	Docx, mp4, forms	Public (aggregated)

3.4.1 Data types

The types of data envisioned to be gathered during the project include the following categories:

- Operational data: Real-time logistics data collected from logistics platforms, sensors, Internet of Things (IoT) devices, and tracking systems[11].
- Planning data: Logistics demand data, logistics services data (i.e., fleet compositions, locations for micro-hubs, etc.), simulation models.
- Geospatial data: Maps, routes, and geographical information related to last mile logistics.
- Statistical data: Aggregate data on delivery times, costs, distances, and other relevant metrics.
- Image recordings: footage taken during Living Lab implementation, workshops, webinars and other dissemination events.
- Qualitative data: Interviews, surveys, and other qualitative data collected from stakeholders and end-users.

At this stage (M18) an initial data model for the implementation of the first version of the GREEN-LOG solutions has been defined. The definition of the model has taken into account other standard existing models for logistics, the type of data to be provided by logistics operators participating in the Living Labs and the inputs and outputs generated by GREEN-LOG components.

The data model is organized into entities or objects. The main entities are:

- Order
- Parcel

[9] Moosend: Email Marketing Software for Thriving Businesses

[10] For some operators, some restrictions apply.

[11] Restrictions apply; only when it do not link to individuals.

- Events (Track&Trace, Disruption)
- Vehicle
- Hub
- Tour
- Network
- User

Table 2 provides an overview of the properties of each entity.

Table 2: Overview of data to be collected in GREEN-LOG project.

Category	Properties
Order	Order ID Order date Due date Time window Type of service CustomerID Status
Parcel	ID ParcelOperatorID OrderID Release time Number of attempts Status Pickup location Delivery location Weight Volume Width Height Length Nature of the items Sender Type of service Delivery constraints Bulkiness Associated round Round sequence
Track&Trace Event	RecordID Track Event ID Parcel ID Coordinates Timestamp Status
Vehicle	Id Type of vehicle Fuel Type Average speed Capacity Maximum travel time Maximum distance per daily shift Average CO2 emissions

	Life cycle Cost_per_km Operator Num drivers Dedicated location/Served area Mileage GPS coordinates Speed State of Charge Status LidStatus Box Type/Current capacity Capacity used Driver Id Route Id
Hubs/MCC	ID Type of hub Owner Operator Location Address Surface Logistics services Pickup service area Dropoff service area Operation hours Max vehicles Capacity Type of service Eligible products
Network infrastructure	Name Type Boundaries Format Link
Tour/Route	Senders Departure hub Number of tasks Total distance Number of items Total weight/volume Duration Round date Departure time (round) End time (round) Departure time (shift) End time (shift)
User	ID Type Role Registered since Profile (i.e. rewards, preferences)

3.4.2 Data format

A dataset can include different types of formats. For instance, qualitative data collected from stakeholders and end-users can consist of both written interview notes, audio files from interviews, pictures from pilot sites, and survey responses. Only parts of these datasets will be made openly available, for instance in an aggregated manner, since they include personal information.

GREEN-LOG will only use widely accepted formats for data generation, such as:

- Documents/Reports/Publications: .PDF/A, txt, doc/docx
- Spreadsheets: .xls/.xslx, .csv
- Databases: .sql
- Audio files. .mp3, .mp4, .wav, .wma, .ra
- Pictures: jpg, png
- Video: avi, flv, mov, mp4, wmv

3.4.3 Data sizes

Among the different types of data, the most demanding in terms of storage space requirements are video recordings and the databases to store the records of GREEN-LOG data model presented previously.

In terms of video recordings, the size depends on the quality of image (resolution, frames per second). For instance, an hour of recording from videoconferences held with Teams at 402 Kbps stores in mp4 format requires approximately 180 MB/hour. That would be equivalent to webinar recordings. The recording of demonstrations activities may last hours and will probably recording with higher quality, thus these will be by far the most demanding in terms of data space.

Regarding the datasets to be stored in the GREEN-LOG Data Space, a rough estimation of the size can be done taking into account the sample sets provided by logistics operators participating in the project.

Table 3 Estimation of data record size

Category	Records	Record size
Orders	PEDAL: 10.000 orders/month iCargo (external, third-party logistic provider in Leuven site): 536 orders/month VANAPED: new service (expected 10-20 orders/day) Ispra: new service (expected 10-15 orders/day)	123 bytes
Parcel	Similar to orders	270 bytes
Track&Trace Event	4-10 events per parcel	
Vehicle	ACS SMSA +FedEx[12]: 1 vehicle (for white brand GREEN-LOG) Ispra: 2 robots, 1 bike Barcelona: 1 robot, 1 bike, 1 e-van (potentially)	282 bytes
Hubs/MCC	2-4 per site	700 bytes
Network infrastructure	1 per site	Varies very much >100 MB

[12] In this document FedEx refers to FedEx Express Greece

Tour/Route	At least one per vehicle; potentially 2 shifts/day	400 bytes (varies)

3.5 Origin of data

GREEN-LOG data has different origins:

- Data provided by project partners, sourced from their activities;
- Data provided by stakeholders engaged in project activities;
- Data collected during the execution of the Living Labs in the corresponding 5 demonstration areas;
- Data generated by the partners after analysis of literature and processing of collected data.

The channels in which data will be collected include:

- Interviews with groups and individual participants in the Living Labs;
- Video recording of activities in the Living Labas
- Feedback from participants at stakeholder workshops;
- Survey responses;
- Market survey;
- Literature study/review and open data (re-use of existing data);
- Automated data collection by sensors and other systems in place.

3.6 Data repository

There have been some changes with respect to the data repository, in particular for the repository to implement the GREEN-LOG Data Space. Following there is a description of the repositories envisioned to store data produced during and after the project.

3.6.1 GREEN-LOG Data Space

The GREEN-LOG city logistics data space (which is under development in T2.1) will be the main repository for storage of data sets. These data sets are coming from logistics operators and uploaded either automatically or using batch processes and data generated within GREEN-LOG platform and its components. The framework chosen to implement the city logistics data space is CKAN[13]. CKAN (Comprehensive Knowledge Archive Network) is an open-source data management system designed to facilitate the storage, management, and distribution of data sets. It is widely used by governments, organizations, and communities to publish open data. Some key features and functionalities of CKAN:

- Data Repository: CKAN provides a robust platform for storing and managing large volumes of data sets, making it easy to organize and retrieve information.
- Metadata Management: It allows users to describe their data sets with rich metadata, improving discoverability and usability.
- Data Publishing: CKAN offers tools for publishing data sets in various formats, enabling easy access and sharing of data with the public or specific user groups.
- Search and Discovery: It includes powerful search capabilities, helping users find relevant data sets through keywords, tags, and other metadata attributes.
- API Access: CKAN provides a comprehensive API that allows developers to interact with the data, build applications, and integrate with other systems.

[13] https://www.ckan.org/features

- Customization and Extensibility: It supports extensions and customization, allowing users to tailor the platform to meet specific needs and integrate additional functionalities.
- Community and Support: As an open-source project, CKAN has a vibrant community of developers and users who contribute to its development and provide support.

Overall, CKAN is a versatile and scalable solution for managing and sharing data, promoting transparency, and fostering data-driven decision-making.

The details for the implementation can be found in deliverable D2.1 - Services for orchestrated deployment of new delivery methods V1. A schema with the data path follows by data until it is stored in the database is shown Figure 2. For data collected automatically, a series of processes will be applied to translate original format into GREEN-LOG data model, ensure data consistency and contextualize it before persisting it in the repository. Access to CKAN is granted through an authorization layer. Credentials have been provided to project developers that either uses data coming from external sources or generate data from their components. CKAN allows the definition of organisations. Users are assigned to organisations, thus, access to restricted information can be handled through the storage to different organisations. At the moment of writing this deliverable, no datasets are available for public access. The main database to be used is based on posgresql technology.

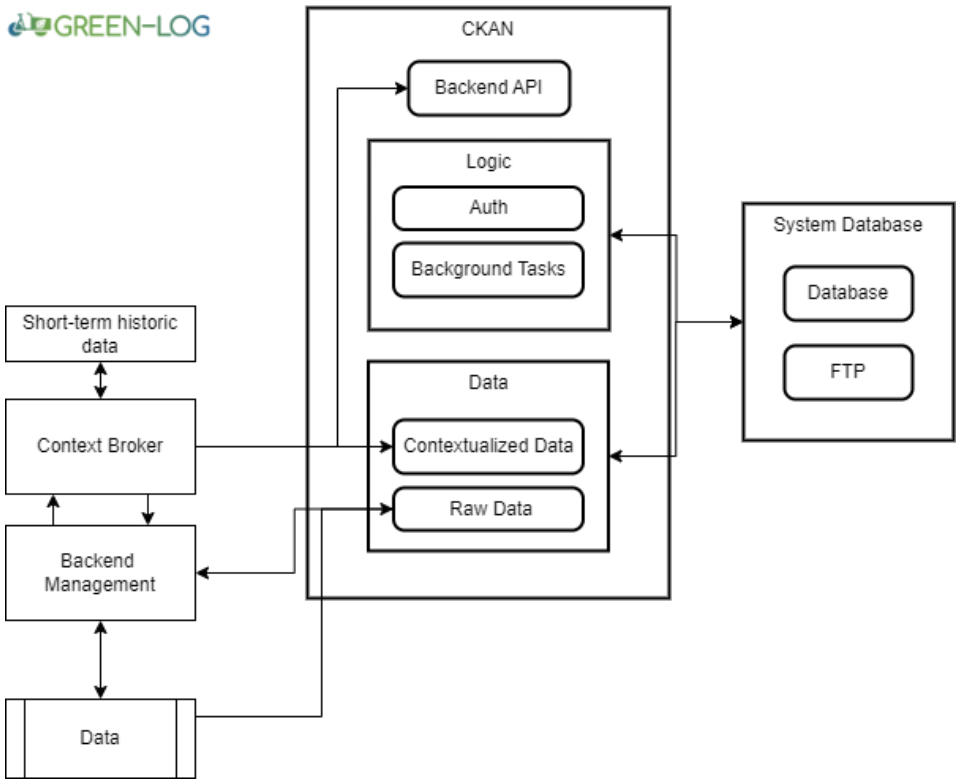

Figure 2 Schema for city logistics data space

The final version of the data management plan will include the lifecycle of the data stored in the city logistics data space. During the project execution, no cleaning policy will be applied due to obsolescence. Furthermore, data generated during the project lifetime need to be persisted at least 2 years after the project finalisation.

Sample datasets provided by data providers at developing phase have been uploaded and tagged manually to CKAN by EUT and can be retrieved by technical partners of the consortium.

3.6.2 SharePoint

A Microsoft SharePoint™ repository has been setup by INTRA to be used by the Consortium partners. This is an access restricted space for collaboration where data will be stored prior to make them publicly available.

This repository is meant to store the material and information related to different Work Packages and the project management (e.g. contacts, meeting minutes, presentations, work plans, etc.) and other project's material and data available for sharing amongst authorised consortium members in the framework of the project. It is not envisioned to be used to store bulk datasets. Data with specific restrictions will be handled by the authorised parties under the directives of the DPO. The documents stored in the SharePoint will follow the naming convention established in the GREEN-LOG Project Handbook [REF-02]. Besides, the SharePoint provides a historical register of changes and editors of the document.

Besides, written and audio-visual material from Interviews, workshops, participants observations for the sociodemographic analysis to be performed by HALM will be stored in HALM Microsoft OneDrive. This material will be stored as research data, providing the confidential needed according to research material data management plans at HALM. In user engagement activities in the Urban Living Labs we will ask for permission from the participants either according to HALM consent forms regarding public publication in university outlets or according to research project consent forms depending on activity, according to the principles and guidelines provided by Research Councils. This means that we will do all measurements needed for mitigating risk for harm of the research participants and providing confidentiality and a right to withdraw from participating in the project whenever asked for. We will also follow "The European Code of Conduct for Research Integrity" guiding principles.

3.6.3 Zenodo

GREEN-LOG will use the open research data repository *Zenodo* to comply with the Horizon Europe mandate. All scientific publications, including public deliverables and public parts of underlying datasets will be uploaded to the *HE GREEN-LOG Community*[14] in addition to the *European Commission Funded Research (OpenAIRE) Community*[15] in Zenodo. In the case of deliverables, the process will take place after the deliverables have been accepted by the Project Officer after the reviewing process.

Zenodo is a "catch-all" open research data repository which gathers research data across all disciplinary fields. It is for non-military purposes only, and the repository is hosted and managed by CERN. All data deposited to Zenodo is stored securely in the CERN Data Centre's cloud infrastructure[16] .

3.6.4 GitHub

After an initial survey, some software components have been identified as potentially being of interest for publication as open source. A deeper analysis will be performed as development progresses bearing in mind the mandate making publicly available as many project outcomes

[14] https://zenodo.org/communities/hegreen-log/?page=1&size=20
[15] https://zenodo.org/communities/ecfunded/?page=1&size=20
[16] https://zenodo.org/

as possible. However, it will be at the discretion of individual consortium members (and any Consortium Agreements regarding IPR on supplied data) to decide whether the source code of their developed software is openly accessible.

In the case the source code can be published, it will be done through GitHub[17]. Since the DMP is expected to mature during the project, the next release of the deliverable will specify which and how this data can be accessed by the wider research community.

[17] https://github.com/

4 FAIR Data Management

GREEN-LOG will manage data in accordance with the principles of FAIR data management as requested by the European Commission, according to OpenAire principles[18] to make data:

- Findable
- Accessible
- Interoperable
- Re-usable data

The project aims to maximise access to, and re-use of research data generated by the project. However, the project will also consider the legit right of partners not to publish all the datasets and assets produced during the project for the sake of data privacy of Living Lab participants and Intellectual Property Rights.

4.1 Findability

Best practices to make data findable are to:

- assign (Meta)data a globally unique and persistent identifier;
- describe data with rich metadata;
- include in the metadata the identifier of the data they describe;
- register and index (Meta)data in a searchable resource.

The application of this principles within GREEN-LOG will be as follows:

- Use of the Digital Object Identifier (DOI) System to assign unique identifiers to the GREEN-LOG datasets.
- A set of data, mainly generated by the project, will be published in OpenAIRE and Zenodo repositories. Zenodo provides version control and assigns DOIs to all uploaded elements.
- Creation of HE GREEN-LOG community in Zenodo.
- Deliverables produced by GREEN-LOG will follow the naming conventions described in [REF-02].
- Metadata will be easy to find for both humans and computers. Machine-readable metadata are essential for automatic discovery of datasets and services, so this is an essential component of the FAIRification process.

Metadata associated with each published data set in Zenodo will by default be as follows:

- Digital Object Identifiers
- Version numbers
- Bibliographic information
- Keywords
- Abstract/description
- Associated project and community
- Associated publications and reports
- Grant information
- Access and licensing info
- Language

[18] https://www.openaire.eu/openaire-guidelines-paving-the-way-to-interoperability-fairness-and-eosc

By the time to make data open, the CERIF model[19], specifically the part that is relevant for OpenAIRE[20], will be taken into account to enhance standardisation of metadata.

Besides, a dataset catalogue will be built containing the following descriptors:

- Type of data set: Type of data according to categories and origin (imported or generated).
- Period covered: Initial and final dates of the data contained in the data set.
- Data origin: System and organisation providing the data.
- Responsible partner: Describes who is responsible for the data generation and quality.
- Dataset name: brief description of the properties of the dataset.
- Data format description: description of the format of the data.
- (Expected) Amount: description of the amount of data.
- Confidentiality level:
  - Public: fully open, they can be shared with the general public.
  - Sensitive: data is limited under the conditions of the GA and CA.
- Additional classification: these classifiers will be revised and extended during the project and additional information will be provided as it is required during the project implementation.

4.2 Accessibility

All public datasets, scientific publications and deliverables will be uploaded to Zenodo and made openly available, free of charge, after each reporting period, once they have been approved by the EC through the Project Officer.

Publications and underlaying data sets will be linked through use of persistent identifiers (DOI versioning). Data sets with dissemination level "confidential" (non-anonymous datasets) will not be shared due to privacy concerns. Some datasets are restricted due to protection for commercial exploitation. The final version of the DMP will list public and restricted datasets.

As described in section 3.2, before making it publicly available in the public repository (Zenodo), data will be anonymised to avoid recognizable patterns or personal information that could identify individual.

Master theses and PhD theses derived from the project will be made available at repositories provided by the corresponding academic partners participating in the GREEN-LOG consortium (i.e., UoA[21], UAEGEAN[22]).

In the cases where private data is processed and aggregated (e.g., as part of a model, or functionality of a component) permission will be needed from the provider prior to making the altered data publicly available.

Reports, deliverables, and other information for public distribution will be available on Zenodo and the GREEN-LOG website. Raw data (recordings, notes, user data, etc.) will not be available for third parties.

[19] https://eurocris.org/services/main-features-cerif

[20] CRIS information elements relevant for OpenAIRE — OpenAIRE Guidelines for CRIS Managers 1.1.1 documentation (openaire-guidelines-for-cris-managers.readthedocs.io)

[21] https://www.uantwerpen.be/en/library/

[22] https://www.ekt.gr/en/library/phdtheses

Metadata including licences for individual data records as well as record collections will be harvestable using the OAI-PHM[23] protocol by the record identifier and the collection name. Metadata is also retrievable through the public REST API. The data will be available through Zenodo website[24], and hence accessible using any web browsing application.

4.3 Interoperability

Data produced by GREEN-LOG will follow widely accepted standards, including DATEX-II[25] or real-time traffic information, the GML Schema[26] standards related to public transport information systems (Transmodel, NaPTAN, NPTDR, Google Transit Feed Specification), standards related to Multi-Modal Journey Planners (JourneyWeb[27]), framework architectures for the transport sector[28], and NGSI v2 as the foundational framework.

As an ongoing activity, the project follows advances in GAIA-X initiative, which is aligned with the European Data Strategy, focusing on the data economy and cloud services, particularly leveraging the cloud as-a-service model for flexibility and ease. Besides, recurrent meetings with the sister projects (URBANE and DECARBOMILE) are organized to identify synergies in terms of data space definition and data models standardisation.

Zenodo uses JSON schema as the internal representation of metadata and offers export to other formats such as Dublin Core, MARCXML, BibTeX, CSL, DataCite and export to Mendeley. The data record metadata will utilise the vocabularies applied by Zenodo. For certain terms, these refer to open, external vocabularies, e.g.: license (Open Definition), funders (FundRef) and grants (OpenAIRE). Reference to any external metadata is done with a resolvable URL.

4.4 Reusable data

The GREEN-LOG project will enable third parties to access, mine, exploit, reproduce and disseminate (free of charge for any user) for all *public* data sets, and regulate this by using Creative Commons Licences and corresponding data will be Open Data. The final version of the DMP (D5.7) will contain a description of the material made publicly available. At this moment, the data collected from logistics operators is restricted to partners.

[23] https://www.openarchives.org/pmh/
[24] https://zenodo.org/
[25] http://www.datex2.eu/
[26] http://www.opengeospatial.org/standards/gml
[27] http://www.dft.gov.uk/journeyweb/
[28] http://www.arktrans.no/

5 Allocation of resources

EUT, with the support of FI, is responsible for ensuring the implementation of the DMP. The Data Manager is Mrs. Regina Enrich Sard. On the other hand, each partner is called to nominate a Data Protection Officer (DPO) who will handle each activity involving collection and process of data. Specific budget has been allocated for the DMP and Open Science activities (T5.2) as well as some budget to cover the cost of Green/Golden access scientific publications.

The city logistics data space is hosted in EUT data centre. The data space is based on CKAN that is free of charge for the purpose of the project. The hardware infrastructure for hosting the data space is covered by the indirect costs allocated to EUT budget.

INTRA, as project coordinator has set up the internal data repository on SharePoint using its corporate Office365 license.

INTRA leading communication and dissemination activities has allocated resources for the production of communication material. POLIS is managing the project website and has allocated corresponding resources for the hosting.

HALM, as responsible for socio-demographic research during the evaluation phase, will store material from the workshops, dissemination and user engagement activities, including interviews and specially image recordings, in their corporate Microsoft OneDrive repository. No project specific budget is allocated to that purpose beyond the indirect costs granted to HALM as part of their participation in the project.

Long-term preservation of the public data is ensured through Zenodo, Github and the Open Research Europe (or equivalent repositories) at no cost. Other resources needed to support reuse of data after the project ends will be solved on a case-by-case basis.

6 Data security

This section describes the security features of the research data infrastructure used to store and handle data.

6.1 Data security as specified for restricted repository

INTRA SharePoint is the online collaboration platform used in the GREEN-LOG project. A dedicated MS Teams environment has been established on this platform, accessible only by the partner representatives in the consortium. Data with specific restrictions will be handled by the authorised parties under the directives of the DPO setting up specific repositories under agreement of involved parties.

The GREEN-LOG SharePoint site is hosted by INTRA. INTRA applies all appropriate technical and organizational measures to ensure the safe processing of personal data and to prevent the accidental loss or destruction and unauthorized and / or illegal access to, use, modification or disclosure thereof (for more information please follow the link).

The GREEN-LOG data space is hosted by EUT. EUT all appropriate technical and organization measures to avoid inappropriate access to their servers. Access to the Dta Space is controlled through the CKAN authentication layer. Credentials have been handled individually to each organisation. Partners are responsible for protect corresponding passwords.

The following figure illustrates the sequence diagram implemented for the authorization process in the data space.

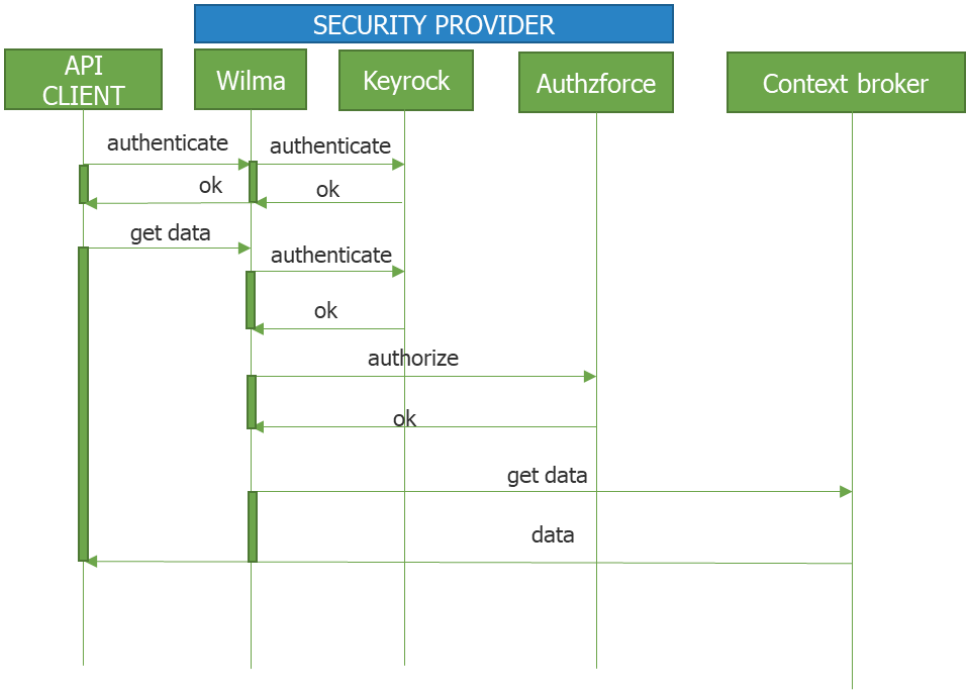

Figure 3 Authorisation process in the data space

6.2 Data security as specified for public repository

The following list describes the security settings for Zenodo:

- Versions: Data files are versioned. Records are not versioned. The uploaded data is archived as a Submission Information Package. Derivatives of data files are generated, but original content is never modified. Records can be retracted from public view; however, the data files and records are preserved.
- Replicas: All data files are stored in the CERN Data Centres, primarily Geneva, with replicas in Budapest. Data files are kept in multiple replicas in a distributed file system, which is backed up to tape on a nightly basis.
- Retention period: Items will be retained for the lifetime of the repository. The host laboratory of Zenodo CERN, has defined a lifetime for the repository of the next 20 years minimum.
- Functional preservation: Zenodo makes no promises of usability and understandability of deposited objects over time.
- File preservation: Data files and metadata are backed up nightly and replicated into multiple copies in the online system.
- Fixity and authenticity: All data files are stored along with an MD5 checksum of the file content.
- Files are regularly checked against their checksums to assure that file content remains constant.
- Succession plans: In case of closure of the repository, a guarantee has been made from Zenodo to migrate all content to suitable alternative institutional and/or subject based repositories.

In the case of Github, platform for hosting and collaborating on code repositories, prioritizes security to protect users' data and ensure the integrity of their projects. Here is a summary of the security measures implemented by GitHub:

- Encryption: GitHub uses industry-standard encryption protocols (TLS/SSL) to protect data transmission between users and the platform, ensuring that sensitive information remains secure during transit.
- Access Control: GitHub provides granular access controls, allowing repository owners to manage permissions for collaborators, defining who can view, clone, modify, or merge changes into the codebase. Access can be granted at the repository, organization, or individual file level.
- Two-Factor Authentication (2FA): GitHub offers 2FA as an additional security layer for user accounts. By enabling 2FA, users are required to provide a second verification factor, such as a time-based one-time password (TOTP) generated by an authenticator app, in addition to their password.
- Vulnerability Detection: GitHub employs a security scanning feature called "Code scanning" that automatically analyses code repositories for potential vulnerabilities, including common security issues and coding errors. It helps identify and address security weaknesses early in the development process.
- Security Advisories and Alerts: GitHub provides security advisories and alerts for known vulnerabilities in dependencies used in projects hosted on the platform. Users receive notifications about vulnerabilities and recommended actions to address them.
- Security Bug Bounty Program: GitHub maintains a bug bounty program, encouraging security researchers to responsibly disclose any discovered security vulnerabilities. This initiative helps identify and address potential security flaws in the platform.
- Audit Logs: GitHub logs and tracks various activities, providing an audit trail of actions performed within repositories. This feature helps users monitor changes, identify unauthorized access attempts, and investigate any security incidents.
- Protected Branches: GitHub allows users to designate branches as "protected," enabling additional safeguards to prevent accidental or unauthorized changes. Protected branches can enforce code reviews, require status checks, and restrict direct pushes, reducing the risk of unauthorized modifications.

- Dependency Management: GitHub supports dependency management tools like Dependabot, which automatically scans repositories for outdated or insecure dependencies and creates pull requests to update them to the latest secure versions.
- Security Best Practices: GitHub provides guidance and best practices for secure coding, repository management, and collaboration workflows. This includes recommendations for secure development practices, secure password management, and safe handling of sensitive data.

Github uses Microsoft Azure data centres. These data centres are located in different countries and regions across the globe, spanning multiple continents. In principle, the data centre chosen is the one that is geographically closer. Microsoft Azure has data centres in EU regions.

7 Ethical aspects

The GREEN-LOG project consortium has long and extensive experience in the conduct of ethically sound research in compliance with national legislation, EU legislation, respect for international conventions and declarations, and their own institutional requirements. The overall responsibility for ethical governance of the project will rest within the Project Coordinator and concerning data management to the appointed Data Manager (EUT).

The research will be carried out in accordance with the ethics and data protection legislation of the participating countries, European legislation, and international conventions, as well as international declarations and codes of conduct relevant to research activities which include:

- Committee of Ministers Council of Europe (1990). Recommendation (No. R(90)3).
- Conventions of the Council of Europe (Convention for the Protection of Human Rights and Dignity of the Human Being)
- Universal Declaration of UNESCO (Universal Declaration on the and Human Rights, 11 November 1997).
- Charter of Fundamental Rights of the EU (signed in Nice, December 7, 2000, 2000/C364/01). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR).

7.1 Collecting personal data from the Living Labs

Data collection activities (interviews, surveys, etc.) will be designed to maintain privacy and applying the principle of minimum harm. Personal data will not be requested unless this is absolutely necessary. Vulnerable groups like minors and individuals unable to freely provide an informed consent will be excluded. Participation is voluntary. Volunteers will be given important information, including possible risks and benefits, about their participation in the study. Participants will be given the possibility to decline and withdraw their participation at any time.

GREEN-LOG will collect pictures and video for use in communication activities (website, newsletter, social media, etc) and evaluation research. Pictures and video can contain personal data if an individual is the focus of the image or video. Examples include: 1) pictures/video of individuals stored together with personal details (e.g. identity cards); 2) pictures/video of individuals posted on the project website along with biographical details; 3) individual images published in a newsletter. Examples of pictures and video that is unlikely to contain personal data are: 1) pictures/video where people are incidentally included in an image or are not the focus (e.g. at a big conference/workshop); 2) images of people who are no longer alive (the GDPR only applies to living people).

When collecting pictures and video GREEN-LOG will follow established guidance and best practice on collecting and processing such data to ensure that we adhere to the legal requirements (e.g. guidance established by the University of Reading[29], UK). Under no circumstances will pictures containing personal information be publicly shared without the subject's explicit consent.

[29] https://www.reading.ac.uk/internal/imps/DataProtection/DataProtectionRequirements/imps-d-p-photographic.aspx

Personal data will be handled in accordance with European legislation on privacy (GDPR). Under no circumstance will the deliverables or processes compromise the individual right to privacy and satisfactory handling of personal data.

All personal data will be stored on secure servers with access control managed by the Data Protection Officers. Personal data will be handled by authorised personnel, and no one will have access to the data unless this is necessary to carry out the project work.

7.2 Information and consent form

The participants will be given an information letter and a consent form (on paper or electronically). The information letter will provide information about:

- The type of data that will be collected during the study.
- How the data will be collected (interview, automatic data collection, etc.).
- What the data will be used for. The information letter will explain the purpose of the project and the expected results. It will also be explained that published information always will be anonymous, and that no personally identifiable information will be published in any way.
- How the data collected will be handled. The information letter will explain that personal data will be treated in full confidentiality and will be registered and stored in a secure manner. The data will be de-identified before it is processed (name or other characteristics serving to identify person will be replaced by a number and the list of identifiers will be kept separate from the data).
- Who will have access to the data. The information letter will state that data will be handled by a very limited number of authorised personnel and that confidentiality will be regulated by legal agreements. The data will be de-identified before it is discussed and processed within the project.
- The rights of the participants. The information letter will state that participation is voluntary and that participants have the right to see the data collected about them and that they can withdraw from the study at any time without any obligation to explain their reasons for doing so (contact information for such requests will be provided).

8 Conclusions

The second version of the Data Management Plan has been generated taking as starting point the initial version elaborated in M6. The DMP establishes as a formal commitment by GREEN-LOG partners to adhere to the data management strategy and the procedures it defines. All project partners are aware of the regulations and recommendations provided by the European Commission and Funding authorities. Project partners will also comply with the principles and practices described in the GA and CA.

As Data Manager, EUT will ensure that any data management issues which may arise during the project will be handled appropriately and in a transparent and fair manner. Data Protection Officers designated by each consortium partner will be responsible for assuring data quality and protection for confidential data.

As the project has evolved, after 18 months of projects, more detailed information is available about the type of data to be collected and generated by the project and the restrictions applicable that lead to a refinement of the data management plan, in particular, linked to the GREEN-LOG data space.

The data space under implementation to support GREEN-LOG platform is based on CKAN framework. This framework provides appropriates mechanisms to facilitate data accessibility control and interoperability. The GREEN-LOG data space will include data with different dissemination levels and will be operational during the project lifetime.

The public repositories envisioned to share data are Zenodo and GitHub and will store publicly accessible data beyond the project lifetime.

Microsoft SharePoint will be used as protected repository only for Consortium members to store project documents.

Likewise, Microsoft OneDrive will be used to store sensitive data collected during the evaluation phase.

The DMP is a living document that will be updated during the project lifetime. The next of this deliverable will be published by M36 as a new milestone in the project will be reached. In the meantime, it will be updated as the project evolves and new information on data collection, generation and handling arise.

References

Reference	Name of document
[REF-01]	D5.2 Data Management Plan 1st version, GREEN-LOG deliverable, Eurecat, 28-02-2023
[REF-02]	D6.1 Project Handbook, Quality Plan & Risk Management, GREEN-LOG deliverable, Netcompany-Intrasoft, 28-02-2023

Appendix A: Non-Disclosure Agreement Template

The present non-disclosure agreement (the "Agreement") is entered into on the Effective Date (as this term is further defined) between Netcompany ("Netcompany") on behalf of GREEN-LOG Consortium (see Appendix I) and the "Participant" which is defined below.

Hereinafter, Netcompany and the Participant will be individually referred as the "Party", and collectively as the "Parties". The Parties are interested in exchanging Confidential Information, as this term is further defined, for the purpose this information for developing a Logistics-as-a service platform for interconnected city logistics, sustainable micro-consolidation, and multimodal parcel deliveries in the scope of the European funded GREEN-LOG project, according to the project's needs (the "Purpose"). The Parties agree to protect the confidentiality of the Confidential Information, as it is defined hereafter, in accordance with the following terms:

1. The following definitions shall apply to the present Agreement:

"Confidential Information" means every information provided by the Disclosing Party to the Receiving Party, as these terms are further defined, regardless of its form or content and the medium through which the information is released, including but not limited to all tangible, intangible, written, oral, visual, electronic, present or future information, acquired in any form or at any time, including but not limited to postal mail, fax, e-mail, text message (SMS) or visual inspection during any visit to the facilities and establishments of the Disclosing Party.

Such information will include, without limitation:

1.1. commercial secrets (regardless they are protected or not by copyright, patent or trademark (registered or not));

1.2. financial information, including but not limited to pricing information;

1.3. technical information, including but not limited to investigation, development, processes, data, designs and know-how;

1.4. commercial information, including but not limited to operations, planning, marketing, interests and products; and

1.5. the terms of any other agreement entered into between the Parties and the exchange of opinions, negotiations and proposals in this regard.

(Detailed list of data exchange in an annex, if required)

"Disclosing Party" means the Party which discloses Confidential Information;

"Effective Date" means the last of the dates stated below, in this Agreement, in both signatures of Netcompany and the Participant;

"Process" means by operation of law, by order or determination of a Court, Tribunal or any other competent judicial authority, or the rules, requirements, order or petition of any competent administrative and regulatory authority.

"Receiving Party" means the party which receives the Confidential Information.

"Staff" means employees, managers, professional advisors of any of the Parties or of those companies controlled by the Parties (as this term is defined in article 42 of the Spanish Commercial Code), provided that they are not direct competitors of the Disclosing Party.

2. Both Parties acknowledge that the disclosure of any Confidential Information shall be subject to the terms of this Agreement.

3. The Receiving Party will use Confidential Information (a) with the strictest confidentiality; (b) only to achieve the Purpose; (c) with not less diligence than the Receiving Party would use to protect its own information of a similar nature; and (d) to prevent any use of Confidential Information that might violate this Agreement and/or the communication of Confidential Information to a non-authorised third party.

4. Confidential Information cannot be provided, delivered or disclosed to any third party different from the Staff which needs to know such information in relation to the Purpose to be achieved. In this respect, the Receiving Party undertakes, before disclosing Confidential Information, to (i) inform the Staff of the confidentiality obligations under the present Agreement, and to (ii) obtain the signature of a binding agreement to be entered into by the Staff which will contain confidentiality provisions that will be substantially identical to those stablished under the present Agreement.

5. Notwithstanding clause 4 above, the Receiving Party shall be responsible for any infringement of this Agreement, regardless of whether those infringements are made by the Staff (with or without Receiving Party's knowledge).

In this sense, the Receiving Party acknowledges that any infringement of this Agreement, of its terms and conditions, by the Receiving Party itself or its Staff, could irreparably harm the Disclosing Party. For this reason, the Receiving Party agrees that in the event of infringement, the Disclosing Party will have the right to claim for the damages caused, without prejudice of any other appropriate legal actions. In this sense, the Receiving Party undertakes to hold harmless the Disclosing Party of any losses, responsibilities, costs, charges and expenses that may arise as a consequence of the infringement of the obligations derived from the present Agreement.

6. Both Parties agree that, without prior written consent of the other Party, any article, advertisement or publicity in relation to this Agreement will be published (including the fact that a meeting or discussion has taken place between the Parties) or mentioning or involving the other Party's name, and will not communicate, indicate or suggest in any way to a third party the existence of any negotiation between the Parties in relation to the Purpose.

7. The Receiving Party will have the duty to protect the Confidential Information disclosed by the Disclosing Party.

With respect to personal details, apart from being subject to the confidentiality obligations set out in this Agreement, either Party will comply with the applicable regulation in terms of data

protection and will adopt any technical and or organisational measures that might be necessary to protect such data.

8. This Agreement does not impose to the Receiving Party any obligation regarding the Confidential Information when:

8.1. the Receiving Party is able to prove that such information was already in its possession or knowledge before the signature of this Agreement and that it was legally obtained from the Disclosing Party or a third party without confidentiality obligation.
8.2. is made available to the public, provided that such publicity does not result from any fault, action, omission or intervention of the Receiving Party;
8.3. it is received by the Receiving Party through a third party who is not subject to the confidentiality duty concerning the Disclosing Party;
8.4. it is independently developed by the Receiving Party, without being based, directly or indirectly, in the Confidential Information and without any infringement of the present Agreement;
8.5. it is disclosed by the Receiving Party with the prior written consent of the Disclosing Party; or
8.6. its disclosure is required in the framework of any Process, taking into account that the Receiving Party must, immediately after becoming aware of the Process and before disclosing any Confidential Information, provided that this is permitted according to law, notify the Disclosing Party of the existence of such Process, providing copy of the documents and information required. In any case, the Receiving Party shall only provide the corresponding authority with the strictly necessary information to comply with such requirement. Likewise, when the Confidential Information is disclosed in such case, the Receiving Party must require confidentiality protection to the legal or governmental authorities which have initiated the Process.

9. Both Parties, in their condition of Receiving Parties, acknowledge that neither the Disclosing Party nor its Staff have any responsibility (nor give any statement, declaration, expression of opinion or warranty in this respect) regarding the accuracy or completeness of the Confidential Information.

10. This Agreement might be terminated by any of the Parties, at any moment, by means of a written notice. From the moment in which the corresponding Party has received the referred written notice, the provisions of the present Agreement will cease to be binding between the Parties in relation to any information disclosed from one Party to the other Party after such date. In any case, and according to Clause 11, this Agreement will still be binding between the Parties in relation to the Confidential Information which had been disclosed before the termination of the Agreement.

11. Unless otherwise agreed by the Parties in writing, the Receiving Party's duty to protect Confidential Information will expire in five (5) years to be counted from the termination date of this Agreement.

12. Immediately after receiving the writing notice from the Disclosing Party and, in any event, in the case described under clause 10 above, the Receiving Party will return to the Disclosing Party all documents or any material which contains and includes Confidential Information. Likewise, the Disclosing Party may order the destruction of all copies in charge of the Receiving Party and may require to certify in writing that the Confidential Information and the corresponding copies have been destroyed. Regardless of whether the Confidential Information has been returned or destroyed, the Receiving Party might retain, in accordance with a legal or regulatory provision, some documents which constitute Confidential Information, in which case the obligations assumed under this Agreement will continue to apply to such Confidential Information.

13. This Agreement does not impose to any Party the obligation to exchange Confidential Information, move forward with the Purpose or any other business opportunity, or to buy, sell, license, transfer or otherwise make use of technology, services or products.

14. Neither Party will acquire under this Agreement any intellectual property right (including, in a non-exhaustive way, patent rights, copyrights or trademarks) and, for the avoidance of any doubt, none of the rights or licenses in the Confidential Information are granted to the other Party, except for, in any case, those limited rights necessary to carry out the Purpose, as it is foreseen in the present Agreement. The Confidential Information of one Party, including any right, title or interest, will remain of the sole and exclusive property of such Party.

15. The present Agreement does not constitute any agency, *joint venture* or corporate relationship.

16. The present Agreement cannot be assigned nor transferred by any of the Parties without the prior written consent of the other Party.

17. No-one different from the Disclosing Party and the Receiving Party will have any right under the present Agreement.

18. The present Agreement might be documented in two or more identical copies and each of them will be considered as original, understanding that all of such copies are part of the Agreement, provided that a representative duly authorised by each Party has signed such copies.

19. The present Agreement represents the complete understanding between the Parties regarding the issues discussed herein and replaces any previous agreement, either oral or written, as well as any previous oral communications. Any additions or amendments to the present Agreement must be agreed in writing and signed by both Parties. Any fault or delay in complying any provisions under the present Agreement will not imply a waiver to such provisions or to any other provision under this Agreement.

20. In the event that some or most of the provisions in this Agreement, might be considered, for any reason, void, illegal or unenforceable, such invalidity, illegality and unenforceability will not affect other provisions of this Agreement, and it will be interpreted as if such void, illegal or unenforceable provision was never included in this Agreement and its provisions will have force and effect according to its original terms.

21. The Parties designate the following domiciles, phone numbers and e-mails for issuing and receiving notices:

By Netcompany:

(i) To the attention of: […]
(ii) Phone number: […]
(iii) E-mail: […]
(iv) Postal Address: […]

(i) By the Participant: To the attention of: […]
(ii) Phone number: […]
(iii) E-mail: […]
(iv) Postal Address: […]

Notices to be made by virtue of the present Agreement will be in writing and will be (at the election of the Party's which will send the notice): (i) personally delivered; (ii) sent by certified mail or registered fax, with acknowledgment of receipt; (iii) sent by e-mail with acknowledgment of receipt; or (iv) sent by courier.

Any change of contact person, domicile, phone number or e-mail will be notified in writing to the other Party.

22. Any disputes or claims that may arise from this Agreement, will be governed by the Belgian law. Likewise, the Parties irrevocably and unconditionally agree that such disputes and claims will be exclusively subject to the jurisdiction of the Courts and Tribunals of the city of Brussels (Belgium)

Netcompany

Signature: _____

Name: [ ], by virtue of public deed of [ ], granted before the Notary Public of [ ], Mr. [ ], on [ ], under number [ ] of his protocol.

Position: [ ]

Adress: [ ]

Date: _____/_____/_____

Participant: [COMPANY NAME]

Signature: _____

Name: [ ], by virtue of public deed of [ ], granted before the Notary Public of [ ], Mr. [ ], on [ ], under number [ ] of his protocol.

Position: [ ]

Adress: [ ]

Date: _____/_____/_____

APPENDIX I

The GREEN-LOG consortium is composed of the following organisations

Organisation	Country
NETCOMPANY-INTRASOFT SA	LU
FRONTIER INNOVATIONS EE	EL
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER	EL
FUNDACIÓ EURECAT	ES
PANEPISTIMIO AIGAIOU	EL
AIMSUN SLU	ES
MOSAIC FACTOR SL	ES
MOBY X SOFTWARE LIMITED	CY
UNIVERSITEIT ANTWERPEN	BE
HOGSKOLAN I HALMSTAD	SE
E-NOVIA SPA	IT
FACTUAL CONSULTING SL	ES
DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS	EL
ACS TACHIDROMIKES IPIRESIES MONOPROSOPI ANONYMI EMPORIKI ETAIREIA	EL
FERROCARRILS DE LA GENERALITAT DE CATALUNYA	ES
STAD LEUVEN	BE
STAD GENT	BE
STAD MECHELEN	BE
VLAAMS INSTITUUT VOOR DE LOGISTIEK VZW	BE
POLIS - PROMOTION OF OPERATIONAL LINKS WITH INTEGRATED SERVICES, ASSOCIATION INTERNATIONALE	BE
MUNICIPIUL ARAD	RO
HELSINGBORGS KOMMUN	SE
VALGA VALD	EE
AUTORITAT DEL TRANSPORT METROPOLITÀ	ES
SOLUCIONS ULTIMA MILLA SL	ES
FEDEX EXPRESS GREECE SINGLE MEMBER LIMITED LIABILITY COMPANY	EL

And associates partners

Organisation	Country
MASTIHA WORLD LTD	UK
OXFORDSHIRE COUNTY COUNCIL	UK
UNIVERSITY OF WOLVERHAMPTON	UK
Pedal & Pour LTD T/A Pedal & Post	UK