Data Management Plan (DMP) & ethical guidelines

Deliverable D1.3

Version N°1.0

Grant Agreement	101147942
Project website	green-turn.eu
Contractual deadline	30/11/2024 (M4)*
Dissemination level	PU (Public)
Nature	Deliverable
Author(s)	Bartosz Kożuch (LPIT)
Contributor(s)	Renata Podlewska (LPIT)
Reviewer(s)	Niccolò Corti (Bax), Ignacio Magallón (Bax)

Funded by the European Union

GreenTurn has received funding from European Union´s Horizon Europe Programme under grant agreement no°101147942. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Change Log

Version	Description of change
V0.1	Initial version preparation
V0.2	GDPR compliance review and remarks
V0.3	Reviewed with comments and remarks
V1.0	Final version

List of abbreviations

Abbreviation/Term	Description
CA	Consortium Agreement
D	Deliverable
DMP	Data Management Plan
DOA	Description of Action
DPO	Data Protection Officer
EC	European Commission
EU	European Union
FAIR	Findable, Accessible, Interoperable, Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation
KER	Key Exploitable Results
KPI	Key Performance Indicator
MS	Milestone
NDA	Non-Disclosure Agreement
PC	Project Coordinator
PO	Project Officer
PSC	Project Steering Committee
SAB	Stakeholders Advisory Board
WP	Work Package
WPL	Work Package Leader

Disclaimer

Copyright message

GreenTurn is a project under the CIVITAS Initiative, an EU-funded programme working to make sustainable and smart mobility a reality for all. Read more - civitas.eu.

Table of contents

1. Executive Summary

The deliverable serves as GreenTurn's Data Management Plan (DMP), as well as provides the ethical guidelines that will be followed throughout the project's implementation. The DMP aims at ensuring the highest standards of data handling, while safeguarding the integrity of the research and adherence to Horizon Europe guidelines in the field.

The document presents a plan on handling of research data during and after the end of the project, what data will be collected, processed and/or generated, which methodology and standards will be applied, whether data will be shared or made open access and how data will be curated and preserved. Moreover, the Plan establishes the procedures to ensure that data are used in compliance with applicable legal frameworks, and in particular the General Data Protection Regulation (GDPR) - 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)(Text with EEA relevance).

Furthermore, GreenTurn's Data Management procedures will formalize a FAIR (Findable, Accessible, Interoperable, Reusable) data management framework, as per the EC directions, with the ultimate goal to make data openly accessible and interoperable, and addressing proper re-use considerations.

The DMP identifies the types of data generated or collected by the project, which of them would be suitable for open access following project closure and the standards that will be used for data representation. Special emphasis has been given to address the practises enforced by GreenTurn for the protection of personal data in compliance with GDPR covering, including internal processes that GreenTurn plans to apply. The document also outlines the key Data Management responsibilities of the Work Package Leaders, Project Management representatives from each consortium member, the Project Coordinator and the Data Owners.

A comprehensive quality assurance plan to monitor and maintain the quality of project outputs is also an element of the document. The scope of tasks that are to be executed within the GreenTurn project require the establishment of data management protocols, to ensure data security, sharing, and compliance with relevant regulations.

The provisions included in the deliverable shall also permit regular assessment of the project's adherence to quality, data, and ethical standards and address any issues identified; provision of training/guidance on gender equality early after kick-off. Thus, an ethics framework was established, including ethical guidelines and procedures for the responsible conduct of research.

1.1. Introduction

This report has been prepared in the framework of WP1 and Task 1.2 of GreenTurn. It covers the GreenTurn's Data Management procedures, including internal General Data Protection Regulations (GDPR) compliancy policies, as well as quality assurance procedures and ethical guidelines. The report describes the datasets that will be created, modified and utilized within GreenTurn and how these data relate to the project objectives and the WP structure. The procedures agreed towards Findable, Accessible, Interoperable, Reusable (FAIR) data

management (as per the EC directions) have also been incorporated, with the ultimate goal of making the data findable, including provisioning of meta data, making data openly accessible and interoperable, and addressing data re-use considerations and processes. Moreover, the deliverable describes the whole quality assurance process and measures that need to be taken in order to provide quality outputs, while detailing the scope of ethical commitments and standards that need to be ensured throughout the GreenTurn project.

This report is submitted to the EC as the GreenTurn's Data Management Plan (DMP) & ethical guidance (D1.3) by M4 of the project.

1.2. Deliverable Overview and Report Structure

The document consists of eight sections:

- Section 1 serves as a general introduction and the scope of the DMP document is provided along with the deliverable structure and its alignment to the corresponding GA descriptions and requirements;
- Section 2 presents the entire data lifecycle including different stages at which data will be created, managed or utilized as well as relation of DMP to the GreenTurn project and how DMP affects the GreenTurn processes and activities;
- Section 3 describes GreenTurn work space and repository and its security aspects;
- Section 4 provides FAIR Data Management in GreenTurn, following instructions covering processes in making data findable including provisioning of meta data, making data openly accessible and interoperable, data re-use considerations and processes.
- Section 5 includes GreenTurn's ethics management methodology, as well as GDRP compliancy methods.
- Section 6 presents the Quality Assurance methodological approach and details the components of the GreenTurn Quality Management Plan that will be followed by the consortium partners during the project implementation.
- Section 7 summarises the contents of the document and provides the conclusions from the work undertaken;
- The document concludes with references, lists of tables figures, as well as an Annex section that contains the tools and templates that will be used during the project implementation by the project partners in order to support their effort towards the high quality of the project outcomes.

2. Data Summary

This section defines the data collection concepts and data purposes as they relate to the project's Work Packages. Means of data collection, types of data that will be collected and formatting of data are presented.

2.1. Data Lifecycle

The Data Lifecycle Management process imposed in the GreenTurn project aims at ensuring that data is accessible and usable by those who need it from beginning to end, as well as beyond the project's implementation phase. Thus, the data lifecycle covers all the stages that the involved organisations, partners and participants must pass through in their interaction with data.

The cycle corresponds to the design-thinking approach, as the lessons learned and insights gleaned from one data processing inform the next step and conversely. In this way, the final step of the process feeds back into the first. The different stages at which data will be created, managed or utilized during the execution of the project and afterwards are considered. Then, an analysis of the data lifecycle as well as the means to control, manage and report the related data is provided. In each of the sections that follow, specific metrics for the data management and control have been included and are later summarized into the data management report template (Annex I: Data Management Report) that will be used at various project stages to control data management compliancy. The following diagram demonstrates an indicative typical GreenTurn data lifecycle, without excluding the potential of alternative data flows throughout this lifecycle.

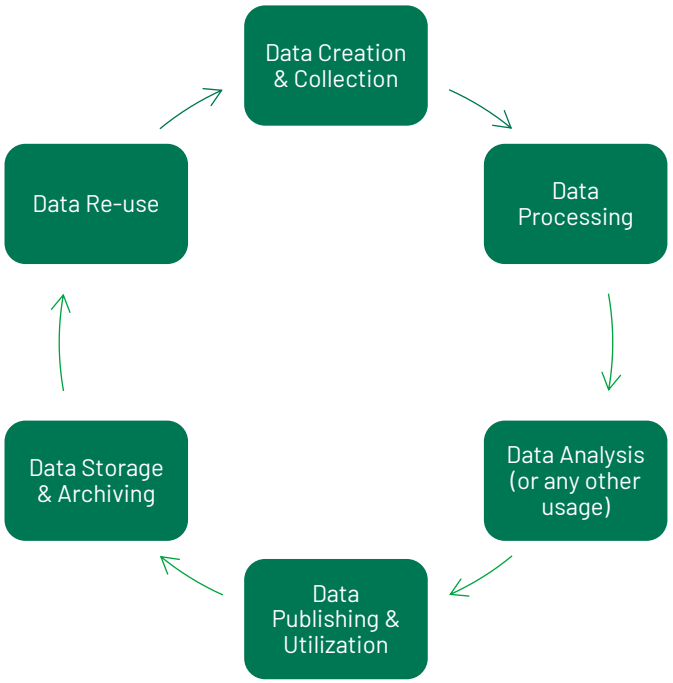

Figure 1. GreenTurn Data Lifecycle

2.2. Data Creation/Collection

The data creation and/or collection stage relates to various data generated within the GreenTurn project, including the envisioned digital and physical pilots, as well as the project reports and other documents/spreadsheets. This includes the creation of the data by each of the respective owner and collection in a structured approach and appropriate formats and layouts to enable their processing by the other project components/modules.

Specific evaluation criteria at this stage relate to the following:

Performance indicator	Means of verification	Target values	Compliancy
Data Creation			
Format	Compliance with existing standards of data exchange	XLS, XML etc	✓or ✗
Availability and Readability	Whole package of data available, non-corruption, whole percentage collected	100% received 100% accessible	✓or ✗
Fit For Use	Data follow data compliancy for proper processing and review	100% usable by intended beneficiary/ies	✓or ✗
Consistency and Completeness	Data are consistent and complete for the intended purpose	Including 100% of information for the intended purpose	✓or ✗
Relation	Data follow a precise relation to their purpose	100% purpose precision	✓or ✗

Table 1. Criteria for Data Creation/Collection

2.3. Data Processing and Analysis

Properly implemented data processing and analysis stage ensures that the involved entities (project partners) are able to perform data processing in a concise approach to fulfil the GreenTurn needs and outcomes. Thus, it includes all steps towards data verification, organization, transformation, integration and extraction for the intended use. Data analysis includes all the actions/methodology executed on the actual data that describe existing facts, identify outlines, develop data clarifications etc. This stage is closely related to the processing stage previously described.

Specific metrics at this stage relate to the following:

Performance indicator	Means of verification	Target values	Compliancy
Data Processing and Analysis			
Data logic	Data can be and are processed following a concise logic and approach	New and processed data follow precise data logic	✓or ✗
Organization and Utility	Suitable content organization of data under processing	100% organized data	✓or ✗
Validation	Ensuring that the data under processing are correct and relevant	100% validated and relevant data	✓or ✗
Aggregation	Whenever multiple data need to be aggregated ensure that this is done in a concise approach	100% aggregate-able data	✓or ✗
Transformation	Transformation of data to the proper format(s) for processing	Capability of data for transformation (if needed)	✓or ✗
Calibration	Calibration of data for their intended purpose	Data properly calibrated	✓or ✗

Table 2. Criteria for Data Processing and Analysis

2.4. Data publication and utilization

The Publication of data refers to the capability to share data openly to public, whereas utilization includes the steps towards data sharing (internally among GreenTurn partners). This implies that the data should be medium and agent independent, making sure that the transfer can be implemented. The purpose at this stage is to ensure that the data are shared with the appropriate controlling mechanisms to ensure protection of proprietary data as well as the data integrity itself. This stage is closely linked with data storage and archiving, as far as metadata is related to ensure data search-ability (as another feature of the FAIR data treatment).

Specific metrics at this stage relate to the following:

Performance indicator	Means of verification	Target values	Compliancy
Data Publication and Utilization			
Means-independent	Transferring of the data in a means-independent approach	100% means independent transferability	✓or ×
Security (a)	Data stored in a secure enough server	At least access control provided over a TLS protocol	✓or ×

Table 3. Criteria for Data Publication and Utilization

2.5. Data Storage, Archiving and Re-use

The storage and archiving stages are also very critical as it relates to the data access, sharing, storage, archiving (including search capabilities) and re-usage. An important factor here is the updated status of the data so that no newer versions exist (unless it is clearly indicated). This should also involve actions to secure from accidental data losses, corruption and unauthorized access. Data storage and archiving is also strongly linked to data re-usability that is also within the scope of the FAIR data treatment.

Specific metrics at this stage relate to the following:

Performance indicator	Means of verification	Target values	Compliancy
Data Storage, Archiving and Re-Use			
Up to date	Ensuring that the stored data are up to date for the specific purpose and no later version exists	100% updated	✓or ×
Meta Data	Existence of meta data in stored files	Relevant metadata have been included into the archive per data set	✓or ×
Security (b)	Access control provided	Access control setup	✓or ×
Security (c)	Server is considered as safe enough (TLS connection protocol)	At least TLS connection configuration	✓or ×

Bandwidth	Control of server bandwidth	Effective storage server bandwidth > 2 MBPS	✓or ✗
Expiration	Properly setting expiration dates for all data after which the data will be deleted	Expiration date noted	✓or ✗

Table 4. Criteria for Storage and Archiving

2.6. Data scope and description

The GreenTurn project collects a diverse range of data across its Work Packages, encompassing stakeholder engagement, consumer behaviour, logistics performance, sustainability metrics, and dissemination outputs. These datasets are critical for achieving the project's objectives, which focus on developing sustainable and scalable solutions for e-commerce logistics. The data spans qualitative and quantitative formats and includes sensitive and non-sensitive information, making a comprehensive data management plan essential to ensure integrity, accessibility, and compliance with FAIR principles.

Stakeholder and Consumer Data:

Work Package 2 generates stakeholder profiles and consumer personas derived from surveys, interviews, and behavioural experiments. This data may include demographic, behavioural, and preference-related attributes. While stakeholder profiles map the roles, needs, and relationships within the e-commerce ecosystem, consumer personas aim to offer insights into intersectional factors influencing delivery preferences and behaviours. These datasets are essential for tailoring project outputs to meet the diverse needs of stakeholders and consumers. To ensure compliance with ethical standards, all personal data is planned to be pseudonymized, and datasets are to be securely stored in accessible but controlled repositories.

Logistics and Environmental Data:

Work Packages 4 and 5 collect logistics performance metrics and sustainability indicators, such as delivery times, emissions, and energy consumption. Geo-spatial data is captured to optimize route planning and assess urban mobility impacts. Environmental metrics are aligned with international frameworks like EcoTransIT World and CountEmissions EU to ensure standardization and compatibility. These datasets enable the project to measure the economic, environmental, and social impacts of its solutions. The data is stored in interoperable formats like CSV and GeoJSON, facilitating integration with modelling tools and comparative analyses.

Prototyping and Business Data:

Work Package 3 focuses on ideation, prototyping, and business modelling, generating outputs such as MVP prototypes and sustainable business models. Data collected during ideation sessions includes stakeholder feedback and innovative solution concepts. These datasets guide the development and testing of tangible prototypes, ensuring they address stakeholder needs and align with project goals. Business model data, including market analyses and feasibility studies, supports the design of scalable and economically sustainable solutions. All datasets are to be documented and shared within the teams repository to promote transparency and collaboration.

Dissemination and Exploitation Data:

Work Package 7 captures data on dissemination activities and exploitation strategies. This includes outputs like newsletters, social media analytics, workshop feedback, and partner-specific exploitation plans. These datasets ensure effective communication of project results to stakeholders and the broader public, fostering awareness and adoption. Exploitation data identifies key exploitable results (KERs) and pathways for their market integration, leveraging feedback from surveys and external reviews to refine value propositions and address market barriers. All data is stored in open-access formats to facilitate broad dissemination and use.

In summary, the GreenTurn project's data management plan ensures that collected data is accurately documented, securely stored, and made accessible for analysis and dissemination. By adhering to FAIR principles and ethical standards, the project promotes the integrity, transparency, and reusability of its datasets, ensuring their value extends beyond the project's duration.

At this early stage of the project, and based on the general assumptions established during the proposal preparation, no collection or processing of personal or sensitive data is anticipated within the scope of all technical Work Packages. Should the need arise during the course of the project to collect or process personal or sensitive data, explicit confirmation of the lawful basis for such processing must be provided by the respective beneficiary.

This confirmation must outline the appropriate technical and organizational measures implemented to safeguard the rights of the data subjects and must be submitted in writing to the Project Coordinator. The provided confirmation will be thoroughly reviewed and subsequently included in an updated version of the Data Management Plan to ensure compliance with legal and ethical standards.

The initial data categories that are envisioned within the GreenTurn project are presented below:

WP2 – Empathise & define: Understanding stakeholders and behaviours

Data Category	Description	Format	Data Sensitivity	Data Origin	Purpose	Related Task(s)
Stakeholder Profiles	Profiles of stakeholders involved in the e-commerce supply chain, including roles, needs, and interactions.	CSV, JSON, DOCX	Medium (anonymized)	Surveys, interviews, stakeholder data analysis, desk research	To map relationships and interactions for effective ecosystem engagement.	T2.1
FAIR Principles:	**Findable**: Rich metadata; **Accessible**: Stored in GreenTurn repository **Reusable**: Detailed information about the data's origin, methodology, and conditions for use provided					
Consumer Personas	Intersectional profiles of e-commerce consumers based e.g. on demographics, preferences, and behaviours.	CSV, XLSX	Medium (pseudonymized)	Survey data, e-commerce analytics	To develop targeted solutions for various consumer segments.	T2.1, T2.2

FAIR Principles:	**Interoperable**: Standardized formats; **Reusable**: Detailed information about the data's origin, methodology, and conditions for use provided					
Behavioural Data	Insights on consumer preferences and willingness to pay for eco-friendly delivery and return options.	JSON, CSV, XLSX	Medium (anonymized)	Experimental studies, stated preferences	To model and predict consumer behaviour under different scenarios.	T2.3
FAIR Principles:	**Findable**: Indexed with unique identifiers; **Accessible**: Via secure yet open systems.					
Digital Communication Metrics	Data on consumer engagement with digital platforms for eco-friendly options.	JSON, HTML, CSV	Medium	Platform analytics, user feedback, surveys	To design effective communication strategies and raise awareness on sustainability.	T2.4
FAIR Principles:	**Findable**: Traceable analytics data; **Interoperable**: Compatible with digital tools used in pilots.					

WP3 – Ideate & Prototype: Co-creating with stakeholders

Data Category	Description	Format	Data Sensitivity	Data Origin	Purpose	Related Task(s)
Ideation Session Outputs	Results from brainstorming sessions, including proposed solutions and evaluation criteria.	DOCX, XLSX	Low	Workshop outputs, stakeholder feedback	To identify innovative solutions addressing stakeholder needs	T3.1
FAIR Principles:	**Accessible**: Open repositories for shared solutions; **Findable**: Indexed outputs.					
MVP Prototypes	Initial prototype data, including descriptions, specifications, and expected performance metrics.	PDF, XLSX	Medium	Prototyping workshops, pilot designs	To create tangible solutions for pilot testing and scalability.	T3.2
FAIR Principles:	**Interoperable**: Prototypes align with industry standards; **Reusable**: Open for refinement.					
Business Model Data	Data on sustainable e-commerce business models and their implementation.	CSV, DOCX	Low	Market analysis, literature reviews	To develop and test business models ensuring economic and environmental sustainability	T3.3
FAIR Principles:	**Reusable**: Frameworks for other regions; **Accessible**: Documented for stakeholders.					

WP4 – Test: Piloting in real and digital environments

Data Category	Description	Format	Data Sensitivity	Data Origin	Purpose	Related Task(s)
Logistics Performance Metrics	Delivery times, distances, returns, and efficiency data.	CSV, XML	Low to Medium	Pilot logistics reports, LSP databases	To evaluate logistics operations' efficiency and optimize solutions.	T4.2, T4.3
FAIR Principles:	**Accessible**: Available for comparison; **Interoperable**: Compatible with logistics systems.					
Geo-Spatial Data	Location-based data for route optimization and urban mobility planning.	GeoJSON, SHP	Medium (location-specific)	GIS systems, pilot logistics data	To optimize logistics operations and assess geographical impacts	T4.1, T4.2
FAIR Principles:	**Interoperable**: GIS standards compliant; **Reusable**: Cross-pilot compatibility ensured					

WP5 – Validate: Ensuring efficiency and sustainability

Data Category	Description	Format	Data Sensitivity	Data Origin	Purpose	Related Task(s)
Environmental Impact Metrics	Emissions, energy consumption, and ecological footprint data.	JSON, XLSX	Medium	Emission calculators, pilot operations	To measure and minimize environmental impacts of e-commerce operations.	T5.3
FAIR Principles:	**Reusable**: Open for other projects **Interoperable**: Aligned with international standards.					
Social Impact Data	Data on accessibility, working conditions, and social equity in logistics operations.	CSV, XLSX	Medium	Surveys, focus groups, spatial analysis	To assess and improve social sustainability outcomes.	T5.4
FAIR Principles:	**Findable**: Metadata indexed in registries **Reusable**: Defined accessibility policies.					

WP6 – Implement: Fostering replication and large-scale uptake

Data Category	Description	Format	Data Sensitivity	Data Origin	Purpose	Related Task(s)
Regulatory Analysis	Analysis of local, national, and EU regulations affecting e-commerce logistics and sustainability.	DOCX, XLSX, PDF	Low	Policy documents, expert analysis, interviews	To provide evidence-based policy recommendations for sustainable logistics.	T6.3
FAIR Principles:	**Accessible**: Reports publicly available; **Findable**: Indexed under regulatory frameworks.					

WP7 – Share & Valorise: Dissemination and Exploitation

Data Category	Description	Format	Data Sensitivity	Data Origin	Purpose	Related Task(s)
Dissemination Materials	Newsletters, website content, and social media updates.	HTML, DOCX, PDF	Low	Project updates, reports	To share project findings and engage stakeholders through strategic communication channels.	T7.1
FAIR Principles:	**Findable**: Indexed on platforms **Accessible**: Openly available to the public.					
Exploitation Strategies	Partner-specific plans for market uptake of project outcomes.	DOCX, XLSX	Low	Stakeholder discussions, internal reviews	To identify pathways for the practical application and uptake of the project's key results	T7.2
FAIR Principles:	**Reusable**: Framework adaptable for other projects; **Findable**: Indexed for partners.					
Workshop Outputs	Insights from webinars and workshops hosted under the project's academy and observatory.	PDF, DOCX, PPT, XLSX	Low	Workshop notes, stakeholder inputs	To facilitate knowledge sharing and inform project refinements.	T7.3, T7.4
FAIR Principles:	**Interoperable**: Formats compatible with academic and professional platforms.					

Table 5. GreenTurn WP7 Data Mapping

Finally, the technical and administrative coordination (including quality assurance and ethical standards) of the project will be led through project management activities in WP1 (Organize & Flow: Project Management). These tasks will create and process various types of documents and files in order to ensure the efficient and effective management of GreenTurn. These types of data will mainly consist of: documents, spreadsheets or presentation files, for managing and handling content related to meetings such as agendas, meeting minutes, presentations etc. in MS office (or similar) type of documents (.doc/.docx, .xls/.xlsx, .pdf, .ppt/.pptx etc). All partners are expected to have access to them while they will always be considered as internal documents to the GreenTurn consortium (not to be distributed outside GreenTurn). This also includes all documents and spreadsheet files for the collection and progress/periodic reporting (internally and/or to the EC) of GreenTurn. These will be circulated internally to the consortium or submitted as final versions to the EC and will be mainly MS office documents (.doc/.docx, .xls/.xlsx, .pdf etc).

At the same time WP1 will be responsible to ensure compliance with the 'ethics requirements' and the respective consent for the participation of stakeholders in the research, for the collection, storage, and protection of personal data and finally a declaration on compliance for collecting and processing personal data as described in the proposal. Other files that will be created in the framework of WP1 consist of quality management and templates for all the above (and possibly more) purposes. These files will most of the time be .doc, .docx, .pdf, .xls, .xlsx, .ppt, .pptx files created by the Project Coordinator/Quality Manager and used and shared by the GreenTurn partners. All related files in WP1, are restricted to the GreenTurn consortium, and will be stored

in the GreenTurn intranet (Teams), where all partners have personalized login details and therefore, access is considered fully controlled and safe.

Additionally, the current information that WP7 is gathering relates to the Stakeholders Advisory Board members and covers the following data:

- name;
- email address;
- organization and the role the SAB members;
- whether the member has sent a letter of interest for the proposal;
- whether the member has filled the GreenTurn NDA document, presented in CA;
- the member's expertise in relation to GreenTurn.

The aforementioned information is considered as 'personal' information. The data are kept only for the purpose of the project (and for its duration) and only with the consent of the Advisory Board members, as this will be acquired via a clear consent statement (also included in Advisory Board in CA).

Data Description	Data Origin	Data Format	Confidentiality	Restrictions
Management and Financial Reports (internal and EC)	Partners and Coordinator, EC	.doc, .docx, .pdf, .xls, .xlsx	Project Consortium	
Meeting Presentations	Partners and Coordinator	.ppt, .pptx	Project Consortium, unless jointly agreed to be public	Eliminate Business sensitive or personal data prior to public exposure
Meeting minutes	Partners and Coordinator	.doc, .docx, .pdf	Project Consortium	
Deliverables and internal reports	Partners and Coordinator, EC	.doc, .docx, .pdf	Internal/Public Deliverables, Reports are internal	As per Grant Agreement
Other templates (minutes, agendas etc)	Quality management templates	.doc, .docx, .pdf, .xls, .xlsx, .ppt, .pptx	Consortium Internal	

Table 6. GreenTurn WP1 Data Mapping

In order to ensure compliance with all the previously described data management decisions as they relate to the DMP, the following overall GreenTurn measures will apply:

- **WP leaders** will be responsible for adhering to the specifications above in their respective Work Packages;
- **Each project partner** will be responsible for the DMP actions and will be accessible by the partner team in case of issues related to DMP;
- **Data Owners** have the ultimate responsibility of complying with the specifics of the GreenTurn Data Management plan, as well as the related GPDR policies;

- For the overall GreenTurn project activities, **the Project Coordinator** has the overall responsibility for complying with the Data Management Plan;
- **The Project Manager** and the primary contact from each and every partner should ensure that personnel working on the project have read the Data Management Plan and apply/exercise all the principles as described in the document.

3. GreenTurn intranet

3.1. Data identification and searching capability

The GreenTurn intranet is a shared space used for project management, as well as communication, document repository and calendar. The intranet has been properly configured and structured in order to ensure data sharing and exchange between different consortium partners. The data and document repository allows data annotation and content setting with the use of tags, file grouping, commenting and keywords, as well as document versioning. These features - combined with the proper data and file-naming conventions - will provide an overall efficient data searching capability for GreenTurn directing precisely to the data itself, data owners, report owners/authors, as well as data contributors.. On top of this, the GreenTurn intranet provides also project categories, dates, activity overviews, roles and features, as well as notifications that will also aid the data management process. To further support searching capabilities, each report owner will also include some metadata (as keywords) to the document itself for easier searching in documents and reports/deliverables etc.

3.2. Metadata provisions and Data Interoperability

As stated above, the GreenTurn intranet allowed building the actual data model, that supports several identification mechanisms, based on key words, tags, unique identifiers etc. The owners of each data component will be responsible for using the proper naming and tagging conventions following the GreenTurn quality manual, so the respective metadata information can be easily kept, extracted and referenced for all purposes of data handling and utilization within the project.

Data interoperability is considered only for the internal purposes of GreenTurn and includes data re-use, interchanges and general utilization. For data interoperability outside the consortium, GreenTurn will follow IPR rules to ensure no project's foreground is released.

To maximize data interoperability, the consortium seeks to comply with commonly used filenames such as .XML, .XLS(X) etc. apart from the aforementioned commonly used standards (relating to commonly used filenames). If necessary, GreenTurn will investigate the possibility to follow other (internationally recognized) standards for both actual data and software produced. Metadata standards, such as: ISO 19115 (GIS data), ISO 14721 (Open Archival Information Systems (OAIS), ISO 16363 (audit and trustworthiness of digital repositories). Compliance to these will support digital data management in a longer term mentality. Other software related ISO standards will be also investigated (such as ISO 25010: ref systems and software engineering) and SQuaRE (systems and software quality requirements and evaluation).

3.3. Data Reusability of Existing and Non-Existing Data

In the reality of the GreenTurn project execution, the existing data will be considered as data not created by the projects activities. This mainly refers to the usage of logistics or sensor data from the envisioned pilots, including data generated through the simulations and assessments planned in WP5. A data flow of information from each of the physical and digital pilots towards the GreenTurn intranet during the implementation of the pilots is expected. The above shall be considered as data produced by the GreenTurn pilots.

The proper execution of pilots requires feeding the digital pilots with data including historical information to properly execute the envisioned simulations and assessments. Such data shall be shared with the GreenTurn consortium for the cases of models & systems experimentation and calibration. Thus, the term re-usability applies to data not being produced during GreenTurn's lifecycle, but data re-used and produced earlier by the same pilot environments. For the foreground data re-usability, the consortium will make sure that data is properly and securely stored in a convenient and secure server to enable easy and controlled access outside the consortium.

4. FAIR Data Management

The GreenTurn project adopts the FAIR principles—Findability, Accessibility, Interoperability, and Reusability—as a cornerstone of its data management strategy. This approach ensures that the diverse datasets generated across work packages (WP1–WP7) are well-documented, ethically managed, and readily available to stakeholders, fostering innovation and supporting long-term impact.

Findability:

All datasets generated during the project are assigned unique identifiers and enriched with detailed metadata to enhance their discoverability. For example, logistics performance metrics in WP4, such as delivery times and distances, are documented with metadata describing their source, collection method, and parameters. These datasets are published in repositories adhering to FAIR principles or institutional archives, ensuring persistent access through Digital Object Identifiers (DOIs). By implementing metadata standards, GreenTurn ensures that stakeholders and external researchers can easily locate relevant datasets.

Accessibility:

The project ensures that data is accessible to authorized users (consortium partners), while maintaining compliance with ethical and legal standards. Open-access datasets are made available in machine-readable formats (e.g., CSV, JSON) through public repositories. For sensitive or proprietary data, secure access mechanisms will be employed, restricting access to authorized personnel. For instance, should personal data be collected in the future, such as in WP2's consumer personas, appropriate safeguards will be applied, including anonymization and controlled access protocols.

Interoperability:

To maximize compatibility with other datasets and systems, GreenTurn adopts standardized formats and ontologies. Geo-spatial data (e.g. collected in WP4 to optimize logistics and urban

mobility) will be stored in GeoJSON and SHP formats, which are widely used in GIS applications. Sustainability metrics in WP5 will aim to be aligned with international frameworks such as CountEmissions EU, ensuring that the data can be compared or integrated into broader environmental studies. By following standardized metadata schemas and file formats, the project facilitates collaboration across disciplines and sectors.

Reusability:

The project prioritizes the long-term usability of its datasets by providing comprehensive documentation and licensing. For example, stakeholder profiles and consumer personas from WP2 are pseudonymized and accompanied by detailed usage guidelines, enabling their application in future projects while ensuring ethical compliance. Similarly, MVP prototypes and business model data from WP3 will be shared under Creative Commons licenses, promoting replication and adaptation by other researchers and organizations. By providing transparent documentation of data collection methods and processing workflows, GreenTurn enhances the value of its outputs for future studies.

In summary, GreenTurn's FAIR data management approach ensures that project datasets are not only accessible and interoperable but also ethically managed and reusable. By embedding these principles into its workflows, GreenTurn promotes transparency, fosters collaboration, and ensures that its outputs contribute to sustainable innovation and long-term impact.

4.1. Naming conventions for GreenTurn documents and data/document versioning

Within the framework of the GreenTurn quality plan and control, a series of documents/reports and templates have been created to ensure a consistent approach for all project's data and their versions. Details about these reports can be found in GreenTurn D1.1 (Project Management Plan & project intranet) and the Quality Assurance process described in Section 6 of this deliverable. For purposes of completeness we have added below some common material to indicate how the data versioning is aligned with the FAIR approach.

Document Type	Name structure to be used
Deliverables	GreenTurn_DX.X - Title_v0.0_Date_Partner.docx (working documents) GreenTurn_DX.X - Title_Partner.docx (Final document)
Minutes of a physical/online meeting	GreenTurn_MeetingID_MeetingCity_Title_Date_Minutes_v0.0.docx (Physical meetings) GreenTurn_MeetingID_Online_Title_Date_Minutes_v0.0.docx (Online meetings) Meetings identifiers: ▪ KOM=Kick Off Meeting ▪ PM=Project Meeting (concerns regular General Assemblies) ▪ PT= Pilot Level Meeting ▪ TM=Technical Meeting ▪ RM=Review Meeting
Presentations	GreenTurn_MeetingID_ShortTitle_Date_Partner.pptx

Table 7. Document types and naming conventions

4.2. Contribution to Open Data Research Pilot (data openly accessible)

The deliverable is aligned and serves GreenTurn's aim to contribute data to open research. Data sets eligible for sharing will be checked to ensure that:

- they are not confidential; they do not include personal or commercially sensitive information;
- permission from the relevant stakeholders and/or data subjects has been obtained;
- sharing the data does not damage exploitation or intellectual property rights.

Accordingly, datasets will be reviewed by the Data Owners and have to be approved before becoming eligible for contribution to the open research. Together with the respective technical consortium partner(s), Data Owners will then agree licensing for example creative commons or public domain. Following such approval, GreenTurn will then make the dataset available through the Observatory & Academy and upload content to the existing relevant and suitable open access repositories. Where data must be embargoed towards IP protection or exploitation, a timeline for its release will be provided.

The approval of the availability of data in an open approach will need to be sent to the Project Coordinator from the actual data owners via email. For this, a consent that the data can be distributed outside the consortium must be included in the approval email to the Project Coordinator. The following information should be included:

Data Owner	Description of data	Data filenames and version	Consent to publish data outside the GreenTurn consortium
Who is the data owner	*What the data include*	*Filenames and depository position*	*[YES/NO]*

Table 8. Data Ownership

5. GreenTurn Ethics Management Methodology

The section describes ethical and legal issues that may arise throughout the implementation of the GreenTurn project. The main elements of the ethical guidelines are:

- establishing an ethics management methodology, which takes into account the ethical requirements of all demonstration activities in the 5 pilot sites of the project;
- outline current European and national legislation in pilot sites, and assure compliance;
- describe the role of the GreenTurn Ethical Advisory Board;
- present potential ethical risks.

5.1. Ethical issues and requirements

The guidelines and ethical requirements are to be considered anytime the consortium members are performing an activity that involves data collection from end-users:

1) provide informed consent forms for the processing of personal data (if applicable);
2) provide information about data management process: collection, storage, protection, retention, handling and destruction, according to national and EU legislation;
3) provide reasonable justification for collecting and processing personal data;
4) prior to both pre-piloting phase and pilot deployment, all involved end-users must agree and sign informed consents (the consent form will depend on the final pilots frameworks);
5) prior to final integration and piloting, all foreseen NDAs will have been signed by the involved consortium members (if applicable);
6) all personal data will be held private and will be pseudo-anonymised during data processing;
7) the acquired personal data will under no circumstances be used for commercial purposes.

5.2. Guidelines & methodology

The ethics management methodology defines four phases that need to be followed to support the project's implementation plan, including the work breakdown structure and – specifically – the envisioned pilots' activities from the ethical and legislation point of view. The ethics management methodology consists of three main stages, including; Planning, Setting the Principles and Pilot-related Activities. These are further supported by the Data Management Plan, as described in Sections 2 to 5 of the deliverable.

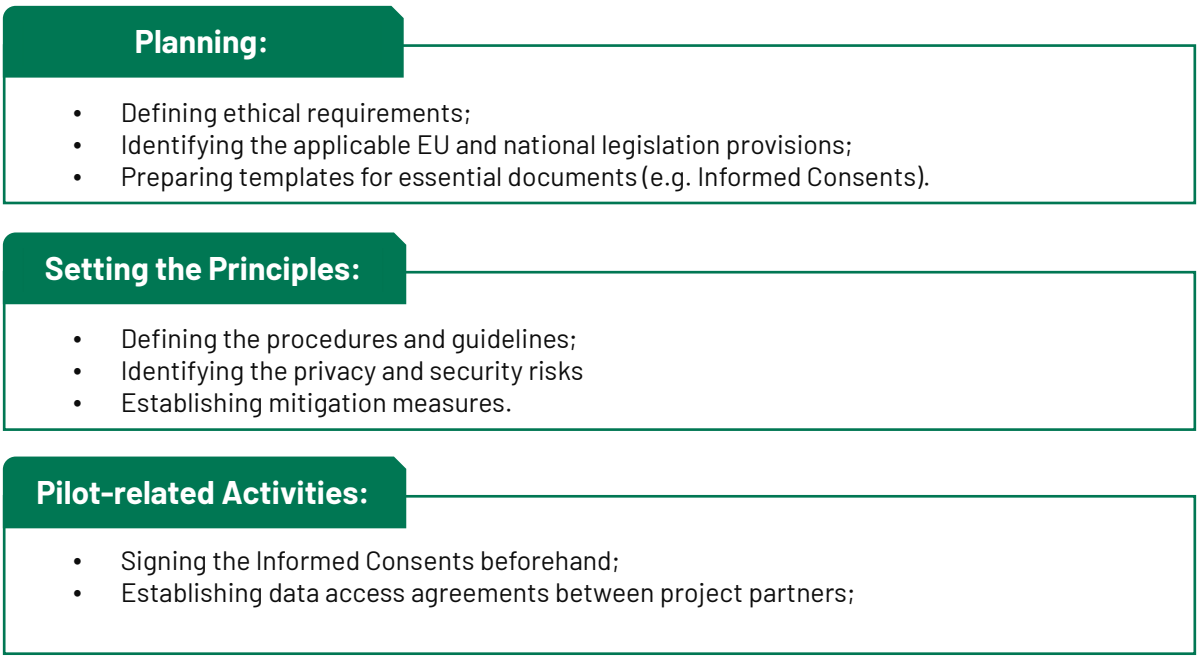

Figure 2. GreenTurn Ethical guidelines scheme

Proper implementation of such constructed ethical guidelines shall ensure:

- compliance with EU and national regulations in relation to data management;
- proper awareness of consortium partners, stakeholders and end-users of the data that will be collected and the reasons for collecting them;
- no sensitive data will be shared with external parties;
- no improper use of data or its transfer is taking place (data used only in relevance to the GreenTurn project);
- data minimisation principle is in use (only data essential to accomplish the research is collected).

5.3. GreenTurn Ethical Board

The GreenTurn Ethical Board (EB) will provide ongoing support concerning ethical and legal issues to the consortium, including support on privacy issues related to data collection in pilot sites. The Ethical Board leads the project's ethical compliance, monitoring the objectives and implications of GreenTurn, to ensure that it conforms to the highest ethical standards, e.g. monitors tasks which have ethical considerations and guides partners in their work and provides input regarding ethical compliance.

Moreover, EB will provide guidelines and recommendations to consortium partners involved in the development of GreenTurn tools, as well as to end users in the pilot sites. The Board will monitor and oversee the pilots, validation and evaluation of GreenTurn results in terms of ethics, security and privacy requirements. In particular, EB will warrant that all technical activities, trials, data management and data processing will be carried out in an ethical way that respects privacy and regulatory constraints.

The Ethical Board is composed of the Project Steering Committee representatives (the Project Coordinator representative – EB Coordinator and Work Packages Leaders representatives), as well as all pilot Operational Leads and Technical Leads representatives. If necessary, external experts will be appointed to assist the EB members. The synthesis of the GreenTurn Ethical Board is presented in Table below.

Partner:	Person Name:	Contact:
LPIT	Anna Woś	anna.wos@pit.lukasiewicz.gov.pl
UAEG	Ioannis Karakikes	ikarakikes@aegean.gr
ECON	Gerda Hartmann	g.hartmann@econsult.at
RUG	Rina Koning	a.c.koning@rug.nl
FZC	Raquel Povar	rpovar@fundacionzcc.org
BAX	Ignacio Magallon	i.magallon@baxcompany.com
INPO	Bartłomiej Banaszek	bbanaszek@inpost.pl
LOG	Marianne Ramser	marianne.ramser@logpoint.at
LOK	Ioannis Manolis	im@logika.gr
ZGZ	Ana Jiménez	ajimenez@zaragoza.es
POZ	Jan Kosmecki	jan_kosmecki@um.poznan.pl

Table 9. GreenTurn Ethical Board

The EB Coordinator will supervise the activities and provide directions to the board. One person will be nominated per pilot site as responsible for following the provided recommendations as well as the national legislation.

5.4. Ethical Risks Identified

In scope of the GreenTurn project implementation, privacy and security risks were investigated in order to reduce the possibility of causing any harm to individuals, e.g. through the misuse of their personal information. As a result, the below list of ethical risks along with possible mitigation measures was created:

Risk:	Impact:	Proposed mitigation measures:
Inadequate security of data related to personal information, logistics service providers and retailers input may result in data breaches	Potential data breaches compromising sensitive information about consumers, LSPs, and retailers.	Special attention will be given to provide confidentiality and protection against data breaches in the context of WP1. If required, additional security mechanisms will be implemented by the partners.

Different laws regarding collection and processing of personal information among the 5 countries of the pilot sites may increase complexity	Complexity and legal risks in managing data across multiple pilot countries.	Security and privacy tasks will be considered separately per use case and stakeholder affected. For activities common to all stakeholders, national legislation of all participating countries will be considered.
Limited participation of end-users to pilots due to privacy & security concerns	Reduced participation from stakeholders fearing misuse of their data.	For the engagement of end users, proper material explaining data collection and security measures will be distributed. Moreover, informed consent forms will be easy to comprehend. Lastly, specifically assigned persons per pilot site will be responsible to explain GreenTurn activities
Incomplete Stakeholder Representation	Misrepresentation of stakeholder needs due to incomplete or biased data, leading to ineffective solutions.	Ensure diverse and comprehensive data collection across all pilot regions and validate findings with stakeholder feedback.
Flawed Customer Experience Mapping	Inaccurate mapping of customer journeys may result in solutions that fail to address key touchpoints and pain points.	Conduct iterative validations with focus groups and external experts to refine customer journey mappings.
Unethical Behavioural Influence	Ethical concerns over manipulating consumer behaviour through interventions without transparent consent.	Clearly communicate the purpose and methods of behavioural interventions and obtain explicit consent from participants.
Misrepresentation in Communication	Potential for greenwashing or social washing through misrepresentation of ecological and social impacts.	Implement strict validation protocols for ecological and social data and engage independent reviewers to ensure transparency.
Exclusion in Solution Development	Exclusion of minority stakeholders from the ideation process, leading to non-inclusive solutions.	Actively engage diverse stakeholders during brainstorming sessions and validate ideas against inclusivity KPIs.
Unsustainable Prototyping Practices	Ethical concerns about prototyping solutions that may not be feasible or sustainable in the long term.	Perform thorough feasibility and sustainability assessments during the prototyping phase, involving stakeholders at every stage.

Unequal Business Model Opportunities	Risk of small retailers being overshadowed by larger players in proposed business models.	Design business models that explicitly account for the needs of small and medium retailers, ensuring equitable opportunities.
Safety Risks in Piloting Activities	Risks of exposing participants to unsafe environments during physical pilot testing.	Develop and enforce rigorous safety protocols for all pilot activities, including regular risk assessments.
Overlooked Environmental Impacts	Failure to account for all environmental impacts, such as indirect emissions or supply chain effects.	Adopt a comprehensive life cycle approach and align assessments with international frameworks like EcoTransIT World and CountEmissions EU.
Ineffective Consumer Engagement	Risk of backlash if consumers perceive awareness campaigns as patronizing or overly prescriptive.	Design awareness campaigns that are educational and collaborative, incorporating feedback from consumer focus groups.

Table 10. GreenTurn ethical risks

5.5. Protection of personal data – GDPR compliance

The GreenTurn project is fully committed to ensuring compliance with the General Data Protection Regulation (GDPR) throughout its activities. While the project does not anticipate the collection or processing of personal or sensitive data at this stage, robust mechanisms are in place to safeguard data subjects' rights if such data is required. Any personal data collected during the course of the project, such as through stakeholder engagement or surveys, will be processed based on a lawful basis, with explicit consent obtained where applicable. The project ensures that data subjects are informed of the purposes, processing methods, and their rights, including the right to access, rectify, or delete their data.

To comply with GDPR's data minimization and privacy-by-design principles, GreenTurn applies strict data handling protocols. Only data strictly necessary for achieving project objectives will be collected, and any personal data will be anonymized or pseudonymized to reduce privacy risks. For example, consumer personas developed in WP2 will use aggregated or pseudonymized data to prevent identification of individuals. The project will implement secure data storage solutions with access controls to ensure that sensitive information remains protected. Should personal data be transferred between project partners across different jurisdictions, GreenTurn will adhere to GDPR's cross-border data transfer requirements and ensure that all beneficiaries comply with relevant regulations.

In cases where personal data processing is required, explicit confirmation of lawful processing and the implementation of technical and organizational safeguards will be provided in writing to the Project Coordinator. This documentation will include details of measures such as encryption, secure access protocols, and regular data audits. These confirmations will be reviewed and included in updates to the Data Management Plan. By maintaining transparency and adhering to GDPR requirements, GreenTurn ensures that all personal data processing activities uphold the

highest ethical and legal standards, safeguarding the rights of data subjects and maintaining trust with stakeholders.

WP2 – Empathise & define: Understanding stakeholders and behaviours

Data Category	Related Task(s)	GDPR Compliance
Stakeholder Profiles	T2.1	Collected anonymously. If personal data is collected, explicit consent and secure storage measures will be applied, including pseudonymization.
Consumer Personas	T2.1, T2.2	Data is pseudonymized, with no direct identifiers. Compliance ensured through aggregation and explicit consent when surveys are used.
Behavioural Data	T2.3	Data is anonymized; explicit participant consent is obtained before conducting surveys or experiments.
Digital Communication Metrics	T2.4	Data collected in compliance with platform-specific GDPR policies. User anonymity is maintained unless explicit permission is granted.

WP3 – Ideate & Prototype: Co-creating with stakeholders

Data Category	Related Task(s)	GDPR Compliance
Ideation Session Outputs	T3.1	Personal data is not anticipated. If stakeholders provide input, explicit consent and anonymization protocols will be followed.
MVP Prototypes	T3.2	No personal data collected; focus is on operational data related to prototype performance.
Business Model Data	T3.3	GDPR compliance not applicable as personal data is not involved.

WP4 – Test: Piloting in real and digital environments

Data Category	Related Task(s)	GDPR Compliance
Logistics Performance Metrics	T4.2, T4.3	Data involves operational metrics only; personal data is not collected or processed.
Geo-Spatial Data	T4.1, T4.2	GIS data collected excludes personal identifiers; compliance ensured through anonymization and secure storage protocols.

WP5 – Validate: Ensuring efficiency and sustainability

Data Category	Related Task(s)	GDPR Compliance
Environmental Impact Metrics	T5.3	Data involves operational and environmental metrics, not personal data; GDPR compliance is not applicable.
Social Impact Data	T5.4	Surveys are anonymized, and no direct identifiers are stored; explicit consent is obtained from participants before data collection.

WP6 – Implement: Fostering replication and large-scale uptake

Data Category	Related Task(s)	GDPR Compliance
Regulatory Analysis	**T6.3**	Personal data is not involved; GDPR compliance is not applicable.

WP7 – Share & Valorise: Dissemination and Exploitation

Data Category	Related Task(s)	GDPR Compliance
Dissemination Materials	T7.1	Personal data collected for mailing lists or engagement activities (if any) follows GDPR rules, including explicit consent and secure storage.
Exploitation Strategies	T7.2	No personal data is anticipated; if collected, consent protocols and anonymization measures are followed.
Workshop Outputs	T7.3, T7.4	If personal or stakeholder-specific data is collected, compliance with GDPR regulations is ensured through consent and secure handling measures.

Table 11. GreenTurn Data GDPR compliance

6. Quality Assurance

Quality Assurance is an integral part of the overall project management process that deals with ensuring the quality of the project deliverables. Project deliverables, either in the form of reports or software components are important outputs of the project and therefore appropriate attention should be given to monitoring every stage of their preparation and also to assessing and improving their contents in order for the final outputs to be of the expected quality.

For this purpose, quality assurance process was made an integral part of Project Management Plan and aims at defining the processes and tools, the roles and responsibilities of the involved parties and also for setting the rules for an efficient cooperation and coordination of the deliverable production process.

The Green Turn quality assurance process consists of five main components. These are:

1. the quality objectives for the quality assurance process;
2. the ecosystem of stakeholders that are involved in the quality assurance process and the assignment of roles and responsibilities to them;
3. the deliverable production process;
4. the Quality Control and Improvement mechanism;
5. the available tools and instruments that will support the Quality Management ecosystem to fulfil its purpose.

6.1. Quality objectives

The main quality objectives in alignment to the scope, vision and requirements of the project as these are defined in the Grant Agreement and the WP objectives. Therefore, the main quality objectives can be summarized as:

1. Consistency of the project outputs with the Grant Agreement. All project results should be fully aligned to the Grant Agreement both in terms of addressing all the issues described in the tasks and the overall project objectives;
2. Consistency of the project outputs with the project plan in terms of following the established procedures and time plan for their delivery as well as the contribution of these outputs to other project activities and the overall project objectives; and
3. Adequate quality of the project outputs in terms of presentation and readability for the report deliverables and user friendliness for the software components.

These objectives will define the actions of the consortium regarding the quality assurance procedures that will be established.

6.2. Quality Assurance ecosystem

Ensuring the quality of the project outputs is a team work and a process that requires the involvement of several stakeholders and management committees within the consortium. More

specifically, the ecosystem of the Quality Management includes the following stakeholders/committees:

- The **Project Coordinator (PC)** who is responsible for the integrative, cross-disciplinary issues of the project, for planning and monitoring progress and supervise implementation of any necessary corrective measures. The PC also holds the role of GreenTurn's **Quality Manager (QM)**, who is responsible for developing and supervising the quality assurance process through project quality checks and monitoring. The Quality Manager is organizing and supervising quality review/peer reviews for all deliverables, as well as produces quality reports;
- The **Project Steering Team (PST)**, which consist of the Project Coordinator and all WP leaders and contributes to the project's quality management by ensuring that all activities are executed in accordance with the Description of Work (DoW);
- The **WP leaders**, who have responsibility to monitor the progress of reports and provide support in the case of a query by the author and seek assistance if the problem remains. They also provide guidance on translating the task requirements and assist the authors to structure the document correctly. The WP leaders give regular feedback to the PSC about the development and progress of work of their WPs and advise on known or potential problems that require management action and propose changes in future plans;
- The **Deliverable owners** who are the primary responsible for the quality of the deliverables. In the case of reports, they are the main responsible for writing, structuring of the deliverable and assigning of partners involved in writing. They collect the inputs, complete the content and check the quality of the deliverable as it progresses according to the established time plan and perform/coordinate any improvement actions that may emerge from the quality control process. Finally, all deliverable owners also have the responsibility to notify in time the WP leader of any delays, problems and developments in order for corrective measures to be applied;
- The GreenTurn **consortium members** that are responsible for performing the peer reviews of all the deliverables (2 reviewers per each deliverable). The SAB members will not be assigned to perform any peer reviews of the deliverables unless their expertise is required to perform a review and this expertise is not available within the consortium; instead, a compendium of the submitted deliverables will be provided to the SAB members before each SAB meeting in order to get their feedback on the deliverable contents.

6.3. Deliverable production process

The deliverable production is a process starting with the initiation of the corresponding task(s) and ends with the deliverable submission to the EC. During this period, GreenTurn foresees a three-stage process that will secure the timely completion of the deliverables and which includes the following activities and milestones:

1st stage: This stage is the main period for the deliverable preparation which starts with the initiation of the task(s) and **lasts up to 6 weeks before the final submission** of the deliverable to the EC. During this period the deliverable owner will establish the work plan for the deliverable preparation, assign tasks to the involved partners and manage

the deliverable production process. By the end of this period the deliverable owner should have the deliverable content fully completed and ready for the quality control and improvement process that will follow. Within this stage three main milestones are foreseen to ensure the smooth progress of the deliverable production:

1. Until 4 months before the final deliverable submission date, the deliverable owner should have confirmed the Table of Contents (ToC) of the report. Following this procedure, a confirmation email will be sent to the PC including the finalized and approved ToC;
2. 3 months before the submission date, the WP leader informs the PC and the PSC regarding the progress of the deliverable preparation and the level of its completion (through an email or a meeting). Moreover, the WP leader will inform about possible problems/issues that may have emerged and hinder the timely submission of the deliverable and are requiring intervention;
3. 6 weeks before the submission date, the deliverable owner should have collected all inputs from the contributing partners and the deliverable should be completed in the final-draft stage, ready for the quality control process. The deliverable is then provided to the PC and the assigned reviewers in order for the peer review process to start.

2nd stage: This stage is the period when the complete deliverable is assessed for its quality and all required improvement actions are taking place. It starts 6 weeks before the submission date and ends at the deliverable due date with the deliverables ready and approved for their final submission to the EC. Within this stage the following milestone are foreseen:

4. 3 weeks before the submission date, the PC and the deliverable owner should have received the feedback from all the reviewers. The deliverable owner then has two weeks to address the reviewer's comments and provide an updated version to the PC and to the WP leader who will perform a final review and send the document for the final adjustments (if any) to the deliverable owner in order to get the final approval. The Deliverable owner will have a few days to make any final adjustments before providing the final version ready to be submitted.

3rd stage: In this final stage, the Project Coordinator receives the final version of the deliverable, approved by the WP leader and submits it in PDF version to the EC.

A more detailed description of the activities of each stage and the corresponding timeframes is provided in Table 6.

Production Stages	Due date	Description
1st	**4 months before the submission**	At the first stage of the deliverable production process which lasts until 4 months before the final submission, the deliverable owner should submit the ToC to the WP leader and jointly evaluate its coherence and alignment to the corresponding deliverable and task(s) descriptions, making any corrections deemed necessary in order to eliminate major content corrections during the final revision. Once this process is completed, a meeting is scheduled between the deliverable owner, the WP leader, the Project Coordinator and the assigned reviewers for the final ToC approval.

		Moreover, during this period the deliverable owner and the WP leader jointly preview the work plan for the deliverable production and the deliverable owner assigns tasks and their time plan to the partners involved in writing. Those assigned to contribute are responsible for providing appropriate content in time.
	3 months before the submission	The responsible WP leader who monitors the progress of the deliverable production informs the Project Coordinator (through email or a meeting) about the rate of completion of the deliverable and for existing problems and possible risks hindering the timely submission of the deliverable in order to provide enough time for corrective actions. It should be noted that this activity serves as an official internal checkpoint of the deliverable progress. Besides this, the progress of deliverables is regularly checked and discussed between the WP leader and the Project Coordinator (and in PST meetings also) in order to allow the main author(s) to communicate problems and delays that need to be addressed for the successful completion of the deliverable and that may require appropriate intervention through the WP leader. Any need to re-plan and reschedule work should be handled in agreement with the Project Coordinator. The Project Coordinator informs the Project Officer accordingly and provides feedback from the partners involved in the WP and deliverable at issue.
	6 weeks before the submission	The deliverable owner should have received all required input from the contributing partners and the deliverable should be completed and in the final-draft stage. The deliverable is submitted for the internal reviewing process which may last up to 3 weeks.
2nd	**3 weeks before the submission**	The deliverable owner should have received all feedback from the reviewers assigned in order to begin to respond to the reviewer's comments. If additional information or clarifications are needed, bilateral meeting can be scheduled between the involved partners. Additionally, the deliverable owner should perform a final editing of language and style before the deliverable is submitted to the WP leader and Quality Manager for final approval. The deliverable addresses the reviewer's comments and provide an updated version to the Quality Manager and to the WP leader who will perform a final review and send the document for the final adjustments (if any) to the deliverable owner in order to get the final approval. The Deliverable owner then will have a few days to make any final adjustments before providing the final version ready to be submitted.
3rd	**Deliverable due date according to the GA**	After the final approval by the WP leader, the document is sent to the project coordinator to be submitted to the EC (pdf version).

Table 12. Deliverable production stages

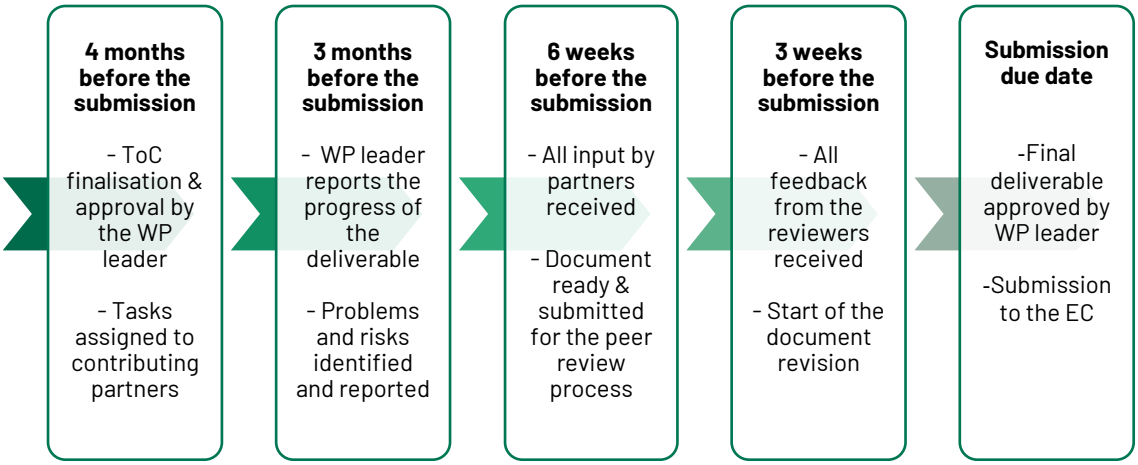

Figure 3. Deliverable production milestones description

Finally, it should be noted that the deliverable production process described above will be applied for deliverables that are due by M6 onwards, due to the limited available time for the deliverables which are to be submitted within the first months of the project. For these deliverables, it is foreseen that the above stages will be adjusted to last for a shorter period of time in order for the deliverables to be properly prepared, assessed for their quality and submitted to the EC within the deadlines set in the Grant Agreement.

6.4. Quality control and improvement mechanism

The quality control and improvement mechanism of GreenTurn consist of three main elements:

1. **The peer reviewing process.** The peer reviewing process starts with the assignment of the task to two reviewers for each deliverable, mainly from within the consortium who are not directly involved in the specific deliverable`s preparation, so that all deliverables will be independently peer reviewed, according to the Grant Agreement provisions. The peer reviewing of the deliverables starts 6 weeks before the submission date and lasts up to 3 weeks.

   Once the owner of a given deliverable has determined that the document is ready to be forwarded for peer review, the document is marked in the **Drafts** folder that has been created in the GreenTurn intranet. After placing the document in this folder, the deliverable owner notifies through an e-mail the assigned reviewers and the Project Coordinator that the document has been forwarded for review. When the review process is complete, the reviewers inform the PC and the deliverable owner via email that the review process is over and then the latter proceeds with the document's revision taking into account the feedback from the reviewers.

   When the updated version of the deliverable is ready, the deliverable owner notifies the Project Coordinator and the Work Package leader who performs the final review of the document and requests for some final adjustments (if any) in order to give their final approval. When the revised document is ready, the Work Package leader notifies the deliverable owner and the Project Coordinator of his approval and then the peer

reviewing process is completed. The Project Coordinator uploads the deliverable to the EC and the final version of the document is moved to the **Submitted** folder.

2. **The quality criteria.** In order to perform the assessment of the project deliverables, a set of quality criteria is established, along with corresponding indicators, that reviewers and WP leaders will use to assess the quality of each deliverable. The role of reviewers is to assess the document based on these criteria but also to underline the points that need revision to the deliverable owner(s). The quality criteria are related to the contents of the document, the structure and readability of the text, but also to the presentation of the document. The detailed indicators used for assessing each of the three quality criteria are described in Table 11 below.

Quality Criteria category	Indicators
Contents	Alignment of contents to the DoW & complete coverage of the DoW requirements, deliverable objectives achieved.
	Use of proper and well justified methodology
	Existence of any state of the art, previous work, related projects, regulations or best practices that has been overlooked
	Absence of plagiarism in the document
	Existence of a conclusions chapter with well justified contents by the work performed
	Highlighted value of the deliverable results to the project implementation
Structure and Readability	Text with good flow and easy to read
	Appropriate and easy to follow structure
	Absence of syntax, spelling or grammatical mistakes
	Easy identification of where the tasks are addressed (as described in the DoW)
Presentation	Proper application of the project template provided (fonts, font sizes, paragraphs etc.)
	Figures, graphics, photos are clear and readable, properly numbered and referenced
	Document length less than 100 pages
	Proper reference of all external sources used (e.g. papers, regulations, past projects, best practices) and also of all input from other GreenTurn WPs and/or activities
	Annexes are of appropriate length and referenced in the main part of the document
	Existence of Definition of terms/ Glossary table

Table 13. Report Deliverables Quality criteria and indicators

3. **The list of reviewers.** Peer reviewers are key to the quality assurance activities of the project and are technically/scientifically knowledgeable partners with the skills and expertise to critically evaluate the deliverable reports or outputs

and conclude whether task requirements are met or adjustments are needed before the submission of the document. The selection of reviewers was made based on four criteria:

- relevance of the reviewer expertise to the deliverable contents;
- no direct or major involvement in the preparation of the deliverable;
- optimal distribution of the reviewing workload for each partner within the project duration in order not to burden their other activities;
- equal distribution of the reviewing effort among partners to the degree that this is possible.

From the beginning of the project, the list of reviewing partners has been defined covering all deliverables of the first period of the project (M18) taking into account the expertise and workload of each assigned partner, to the extent that this was possible. The detailed list can be found in Table 12

Del	Deliverable Name	WP	Lead Beneficiary	Reviewers	Type	Dissemination Level	Due Date
D1.1	Project management plan (PMP) & project intranet	WP1	L-PIT	BAX*	R	SEN	M2
D1.2	Risk and innovation management plan		BAX	L-PIT*	R	PU	M4
D1.3	Data management plan & ethical guidelines		L-PIT	BAX*	DMP	PU	M4
D1.4	Updated DMP (interim actualization)		L-PIT	BAX UANT	DMP	PU	M18
D2.1	Mapping of stakeholder ecosystem	WP2	ECON	RUG LOK	R	PU	M6
D2.2	Intersectional analysis		UAEG	UANT LOGP	R	PU	M6
D2.3	E-commerce customer journeys		L-PIT	CHA INPO	R	PU	M9
D2.4	Behavioural models and willingness to pay		UAEG	ALICE BAX	R	PU	M9
D2.5	Impact communication strategies		RUG	ECON ZGZ	R	PU	M9
D3.1	KPIs and metrics framework for co-creation and impact assessment	WP3	UANT	LPIT LOK	R	PU	M9
D3.2	Analysis of logistics operations & business models		CHA	UAEG LOGP	R	PU	M9
D3.4	Ideas and concepts from co-creation sessions		LPIT	FZC CHA	OTHER	PU	M12
D3.3	Prototypes and MVPs co-created		UAEG	ECON RUG	OTHER	PU	M15

D4.1	Framework of requirements for pilots	WP4	RUG	UANT INPO	R	PU	M15
D6.3	City profiles and review of relevant EU directives	WP6	BAX	LPIT FZC	R	PU	M12
D7.1	Dissemination strategy	WP7	LPIT	BAX LOK	R	PU	M6
D7.2	Exploitation plans: review and methodology		ALICE	UAEG ZGZ	R	PU	M12

** due to the fact that these are strictly organizational documents and must be created in the initial phase of the project, it is assumed that they will be verified in a simplified way, by one entity (except the author)*

Table 14. List of reviewers for the first-period (18 months) deliverables of the project

6.5. Available tools for the quality assurance process

In order to facilitate the quality assurance activities of GreenTurn, a set of tools and templates has been developed. These include:

- a peer reviewing scoring sheet for supporting reviewers perform their task in a standardized and uniform way and highlighting the deliverable owners the deliverable parts that require revision. The scoring sheet can be found in Annex III;
- project templates, including the document deliverable template, the project presentation template, the meeting minutes template and the participants list (in physical or online meetings) template. Deliverable templates are important for providing a standardized format of reporting outcomes/ findings and for minimizing confusion. Moreover, they act as check lists to ensure that vital parts of the output are included and it assists readers (internal or external) to easily navigate and comprehend the message throughout a number of different reports. Moreover, a specific naming structure must be followed in order to have an official and unique way of identifying the project's documents. Table 13 below presents the overall guidelines including the naming scheme for each document type followed by examples.

Document Type	Name structure to be used
Deliverables	**GreenTurn_DX.X - Title_v0.0_Date_Partner.docx (working documents)** **GreenTurn_DX.X - Title_Partner.docx (Final document)**
Minutes of a physical/online meeting	**GreenTurn_MeetingID_MeetingCity_Title_Date_Minutes_v0.0.docx** (Physical meetings) **GreenTurn_MeetingID_Online_Title_Date_Minutes_v0.0.docx** (Online meetings) **Meetings identifiers:** ▪ KOM=Kick Off Meeting ▪ PM=Project Meeting (concerns regular General Assemblies) ▪ TM=Technical Meeting ▪ RM=Review Meeting
Presentations	**GreenTurn_MeetingID_ShortTitle_Date_Partner.pptx**

Table 15. GreenTurn file naming structures

- the project document repository which supports the exchange of information and optimizes the efficiency of the work. Files and folders are structured according to the project processes (including the quality assurance process) and in alignment to the WPs in a clear and comprehensible way. Finally, issues of data security and digital privacy remain crucial to ensure that work is not reached by not authorized personnel, therefore user authentication was used. Documents (deliverables) in the process of creation can be placed in the **Workspace** folder, where, in addition, appropriate subfolders are created for each WP (see Figure 4. Workspace folder on Teams group
-). Placing working files (under creation) in this space gives users the opportunity to work on a given document in parallel and make changes that are visible to everyone.

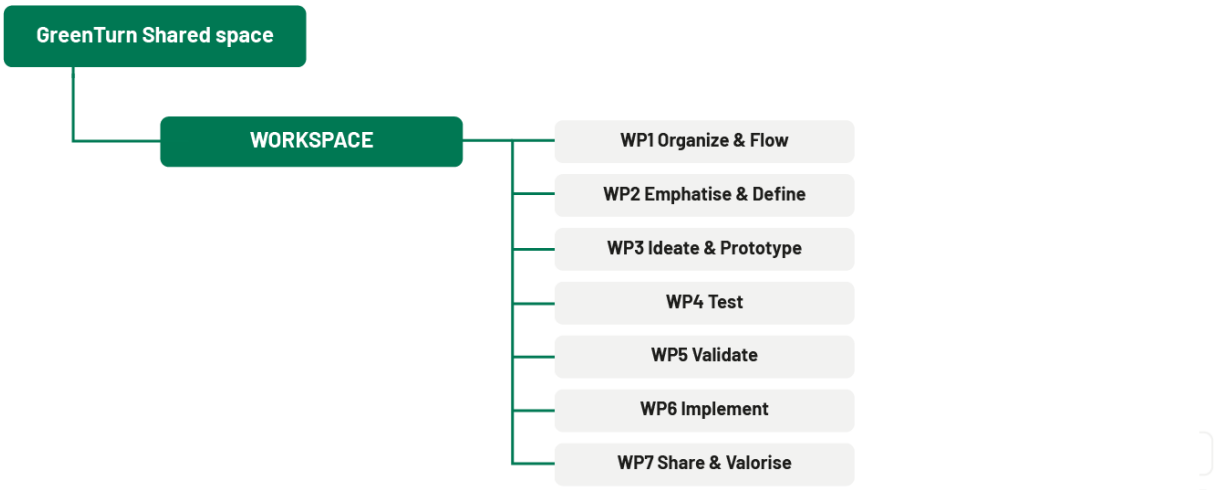

Figure 4. Workspace folder on Teams group

Finally, the rules and order of placing the deliverable files in the appropriate areas of the Teams shared space is illustrated inFigure 5.

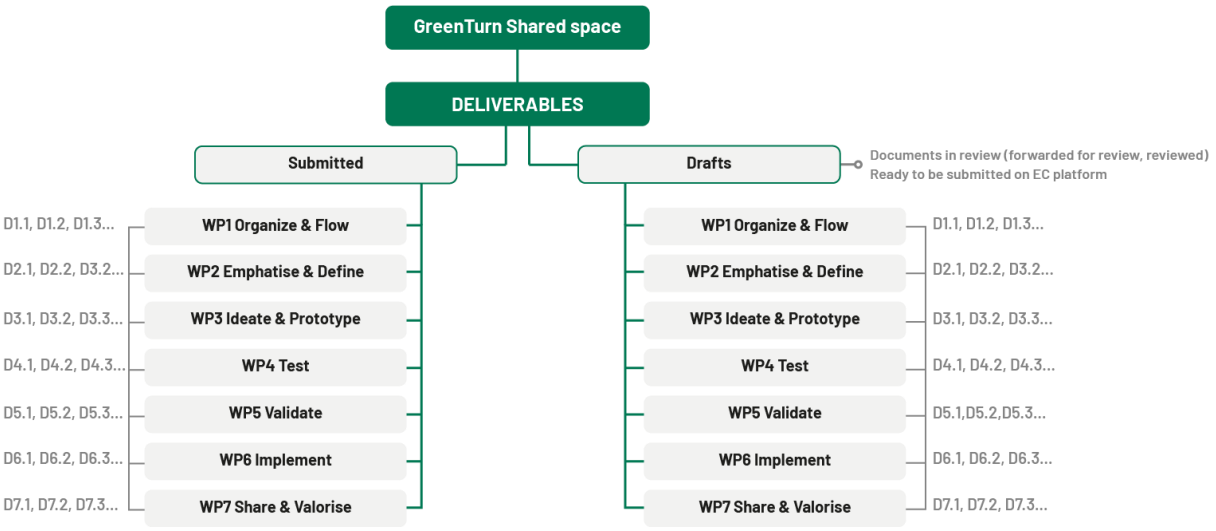

Figure 5. Deliverables folder on Teams group

7. Conclusions

This document is the first release of the GreenTurn's Data Management Plan (DMP) and describes in detail the data and the way it will be managed in the context of the project. It includes an overview of the data that will be created, processed or utilized within the GreenTurn scope, with details on the type and nature of the data involved in specific Work Packages, as well as their relationship with the project objectives. A structured approach has also been established and documented to ensure that GreenTurn's data management will be following the FAIR data principles as defined by the EC.

A full section of this report has been dedicated to address the protection of personal data in compliance with GDPR (regulation) that has been designed to harmonize data privacy laws across Europe, and protect and empower all EU citizens' data privacy, reshaping the way organizations across the region approach data privacy. This section also covers all practices that GreenTurn will follow to comply with the above and internal processes that GreenTurn plans to enforce and apply.

Moreover, the report covers all the aspects of the Quality plan including the criteria, the rules and the procedures that need to be followed during the GreenTurn project implementation, including the different stages of the deliverable's preparation, writing and submission. Furthermore, the document describes the actions and processes to monitor the Quality Assurance, ensuring that the project deliverables meet the defined quality standards, while conforming to the security requirements. It also defines the peer reviewers for the first period deliverables, selecting independent and appropriate reviewers in each case, while an attempt was made to allocate the effort proportionally between them.

8. 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): Regulation - 2016/679 - EN - gdpr - EUR-Lex (europa.eu);
2. Research Ethics Guidance, Economic and Social Research Council, UK Research and Innovation: Research ethics guidance – ESRC – UKRI

List of tables

List of figures

Annex I Data Management Report

Performance indicator	Means of verification	Target values	Compliancy
Data Creation			
Format	Compliance with existing standards of data exchange	XLS, XML etc	√ or ×
Availability and Readability	Whole package of data available, non-corruption, whole percentage collected	100% received 100% accessible	√ or ×
Fit For Use	Data follow data compliancy for proper processing and review	100% usable by intended beneficiary/ies	√ or ×
Consistency and Completeness	Data are consistent and complete for the intended purpose	Including 100% of information for the intended purpose	√ or ×
Relation	Data follow a precise relation to their purpose	100% purpose precision	√ or ×
Data Processing and Analysis			
Data logic	Data can be and are processed following a concise logic and approach	New and processed data follow precise data logic	√ or ×
Organization and Utility	Suitable content organization of data under processing	100% organized data	√ or ×
Validation	Ensuring that the data under processing are correct and relevant	100% validated and relevant data	√ or ×
Aggregation	Whenever multiple data need to be aggregated ensure that this is done in a concise approach	100% aggregate-able data	√ or ×
Transformation	Transformation of data to the proper format(s) for processing	Capability of data for transformation (if needed)	√ or ×
Calibration	Calibration of data for their intended purpose	Data properly calibrated	√ or ×

Data Publication and Utilization			
Means-independent	Transferring of the data in a means-independent approach	100% means independent transferability	√ or ×
Security (a)	Data stored in a secure enough server	At least access control provided over a TLS protocol	√ or ×
Data Storage, Archiving and Re-Use			
Up to date	Ensuring that the stored data are up to date for the specific purpose and no later version exists	100% updated	√ or ×
Meta Data	Existence of meta data in stored files	Relevant metadata have been included into the archive per data set	√ or ×
Security (b)	Access control provided	Access control setup	√ or ×
Security (c)	Server is considered as safe enough (TLS connection protocol)	At least TLS connection configuration	√ or ×
Bandwidth	Control of server bandwidth	Effective storage server bandwidth > 2 MBPS	√ or ×
Expiration	Properly setting expiration dates for all data after which the data will be deleted	Expiration date noted	√ or ×

GDPR Compliancy To be completed for each type of data falls under GDPR or is connected to it in any way		**Data Subjects Details**		**Overall Compliancy**	
Personal Data Description Overall data description	**Access** Determines who has access to the particular data (internal, external to consortium).	**Storage** Storage places of actual data	**Purpose** Intended purpose of data and reasons for keeping.	**Duration** Duration of stored data (until when they will be kept).	**Check**
e.g. conference programme	*Internal and external*	*GreenTurn document server, website*	*Dissemination of GreenTurn conference*	*GreenTurn finish date/*	*[Y/N]*

Annex II GreenTurn's GDPR Policy

This Global Data Protection Policy (the "**Policy**") is drafted by L-PIT (the "**Project Coordinator**") with regards to the EU Horizon Europe Project GreenTurn, Contract Number 101147942 (the "**Project**") executed by the list of partners included therein (the "**Project Partners**") in order to:

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

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

Definitions

For the purposes of this Policy, the GDPR definitions, as set in Article 4 of the GDPR, apply. Therefore, the following terms have the following meaning:

"**Personal data**" means any information relating to an identified or identifiable natural person that is processed by any Project Partner and Policy Recipient during execution of the Project.

"**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"**Processing**" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Consent**" of the data subject means any freely given, specific, informed, unambiguous and **in writing** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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

Aim of the above definitions is to particularise and complement the definitions of Article 4 of the GDPR. Policy Recipients are advised to consult both texts in order to formulate the applicable definitions each time.

Data protection roles and responsibilities

With regard to the actors involved in personal data processing, the consortium was able to identify the following roles:

Controller

Data controller determines the purposes and means of the processing of personal data, its key responsibility is to **ensure that data collection and processing within the scope of GreenTurn, will be carried out in accordance with EU and national legislation**.

Lukasiewicz-PIT, as Project Coordinator, has been appointed as Data Controller.

Łukasiewicz-PIT, has appointed internally a Data Protection Officer (DPO). DPO can be reached at office@pit.lukasiewicz.gov.pl.

Identification

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

Accountability

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

Data protection by design

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

Data protection by default

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

- Personal data is processed for purposes not different from the original purposes;
- Only data necessary for these purposes are collected;

- Data are not disclosed without human intervention.

Joint controller

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

Processor

Unless otherwise specified expressly in this Policy, **all GreenTurn partners handling personal data are considered as Data Processors**, meaning that they process personal data under the control and guidance by the Data Controller.

A processor processes personal data on behalf of the Controller – that is, the Controller delegates all or part of the processing activities to them. In such event the Project contract assumes the role of the relevant required written agreement as per GDPR requirements.

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

Auditing

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

Security

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

DPO

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

Lukasiewicz-PIT, has appointed internally a Data Protection Officer (DPO). DPO can be reached at office@pit.lukasiewicz.gov.pl.

Identification

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

Designation compulsory vs. voluntary

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

Professional requirements

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

Tasks

The organization assigns to the DPO at least the tasks listed in the GDPR.

Notification to Supervisory Authority

Whenever a DPO is appointed the organization notifies the Supervisory Authority of such designation and publishes DPO's contact details.

People in charge of processing

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

Training and awareness

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

Policies and procedures

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

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

Policy scope

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

Establishment

Each Project Partner is established on the territory of EU Member States. In the event of any change in establishment, the respective Project Partner shall notify the Project Coordinator duly and in writing.

Unless otherwise expressly specified, each Project Partner is considered the controller in that Member State.

Processor outside the EU

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

Personal data processing

Personal data

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

Special categories of data

Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation as well as the processing of genetic data and biometric data for the purpose of uniquely identifying an individual.

In the event of such processing the Controller and/or Processor respectively comply with specific rules related to the processing of such data of special categories, as collecting specific informed consent from data subject and applying stricter safeguards.

When the Controller and/or Processor relies on data subject's consent as a legal ground for processing special categories of data, it will meet all legal consent requirements; otherwise, they are only processed if and to the extent it is based on one of the legal grounds listed in the GDPR for the processing of such data.

Data anonymisation

Whenever possible, including non-detrimental to Project execution purposes, Controller and Project Partners shall undertake efforts to keep personal data processed by them for Project purposes anonymous or pseudonymous.

According to the GDPR, "*anonymous information*" is information which does not relate to an identified or identifiable natural person, or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In this context, the GDPR does not apply to the processing of such anonymous information, including for statistical or research purposes.

Similarly, "*pseudonymisation*" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Newsletters, social media and other dissemination material

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

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

Special categories of data

Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation as well as the processing of genetic data and biometric data for the purpose of uniquely identifying an individual.
It is not anticipated in the GreenTurn project to collect or process any special categories of personal data. However, in the event of such processing the Controller and/or Processor respectively comply with specific rules related to the processing of such data of special categories, as collecting specific informed consent from data subject and applying stricter safeguards.
When the Controller and/or Processor relies on data subject's consent as a legal ground for processing special categories of data, it will meet all legal consent requirements; otherwise, they are only processed if and to the extent it is based on one of the legal grounds listed in the GDPR for the processing of such data.

Data subjects

The individual whom the data refers to is the data subject. The GreenTurn project assumes the following data subjects to be involved:

- Individuals whose personal data are generated from GreenTurn actions connected with interviewees and experts providing opinions and evaluations to the project as well as individuals participating in the project activities (e.g. surveys, focus group interviews, workshops, pilots).
- Individuals whose personal data are being collected, held or processed by GreenTurn partners for the purposes of dissemination and consultation.
- Partners themselves.

It is not foreseen that any processing of children's personal data, which by Law require a special legitimate basis and a different consent procedure, will be carried out. In the event of such processing the Controller shall be informed in advance and in writing by Project Partners.

Rights of data subjects

The project applies GDPR rules in terms of protection of data of all individuals whose personal data are generated from GreenTurn actions connected with interviewees and experts providing opinions and evaluations to the project as well as individuals participating in the pilots as well as all individuals whose personal data are being collected, held or processed by GreenTurn partners for the purposes of dissemination and consultation enabling requests coming from web page communication or contact details of responsible person.

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

- ***Right of access***

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

  - ***Right to rectification***

    Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request rectification of their personal data. The procedure specifies in which cases rectification is legitimate. If a data subject's request for rectification is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

  - ***Right to erasure***

    Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request erasure of their personal data. The procedure specifies in which cases erasure is legitimate. If a data subject's request for erasure is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

- ***Right to restriction of processing***

  Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request restriction of processing of their personal data. The procedure specifies in which cases restriction is legitimate. If a data subject's request for restriction of processing is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

- ***Right to data portability***

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

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

Portability right can be exercised when:

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

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

- ***Right to object***

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

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

- ***Automated decision making***

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

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

- ***Timely response to exercise of rights***

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

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

Data recipients

The GreenTurn project assumes the following data recipients to be involved:

- Project partners, who will receive personal data (alone or embedded into other project-related data) for the development of tools and measures.
- For GreenTurn deliverables that will be made public, personal data will be eliminated or anonymized from the delivered data sets (only statistical type of information will be present).

Transmission of data among GreenTurn partners

Personal related data, collected as part of the GreenTurn project, may be shared among partners for project specific purposes only. However, such data will never be sufficient to lead to individual identification (all personal identity disclosing values i.e., names, IDs, VAT No, social security numbers etc. will be eliminated). The same applies for addresses and locations that might lead to person identification. If postcodes will be used, they will be disambiguated to ensure a single specific individual or household cannot be identified. All personal data will be considered, analysed and transformed to a level of granularity not leading to or identifying an individual.

Despite of these measures, GreenTurn does not consider personal data processed under its scope as not identifying individuals ("anonymous data"), something that would exclude application of any data protection law. On the contrary, GreenTurn applies all EU and national data protection law requirements, on top of warranting the above level of encryption to all personal data exchanges carried out in its course.

According to the Project's Description of Action while collection will be undertaken by certain project partners, the outcome of this process will be made available to others in order to execute the relevant processing.

It is the Consortium's understanding that not all of the GreenTurn partners will undertake personal data processing, neither will personal data be shared or made available to all GreenTurn partners as well. This information has been conveyed to it by the Project Coordinator and may be also confirmed through examination of the Project's Description of Work. Consequently, a distinction needs to be made among GreenTurn partners, as follows:

- GreenTurn partners who will process personal data by way of collection,
- GreenTurn partners who will process personal data by way of data transfer,
- GreenTurn partners who will not undertake any personal data processing under the project.

Consequently, the Consortium recommends that all GreenTurn partners under points (a) and (b) above are instructed to undertake relevant data protection measures. These may include, depending on each particular case, either collection of consent forms by the individuals concerned and/or registration with the appropriate (according to the place of establishment)

Data Protection Authority, whenever applicable under the post-GDPR legal environment, and/or adherence to the GreenTurn project online privacy policy (see below).

Transmission of personal data to state authorities

While no transmission of personal data to state (in particular, law enforcement) agencies is scheduled to take place under the GreenTurn project, the Consortium felt it important to discuss the relevant issue. It is the consortium's understanding that the exchange of information from project partners is listed among the European Commission's objectives in order to achieve an increased level of security in the field. Therefore, GreenTurn project is likely to enable, if not warrant, such exchanges of personal data. In this context, the Consortium believes that the issue needs to be taken into consideration, even if it is not directly connected to the GreenTurn project deliverables.

The transmission of personal information by private entities (corporations) to state law enforcement authorities in order for it to be processed in the security context poses legal and ethical issues. Individuals may willingly, or in the normal course of their business, provide their personal information for standard business processing but may feel less willing if they are aware that security state agencies will also be granted access to this information. There is a qualitative change between processing by corporations and processing by security agencies. In addition, if personal data enter the law enforcement system in a particular country, individuals also need to know to which other countries these data may be made available, because this may affect their travelling or international communications routines. While it may be true that personal data collected under the GreenTurn project are common data (name, job title and description, address etc.), it is not unlikely that if they are correlated, they may reveal religion or other sensitive information (see the analysis on profiling that follows). Consequently, the Consortium believes that the issue of transmission of data in the context of the GreenTurn project to state law enforcement authorities needs to be dealt with separately. After all, such processing exceeds the scope of the GDPR and enters into the realm of the Police and Criminal Justice Data Protection Directive (Directive 2016/680), which normally exceeds the boundaries of this Project.

It is therefore the Consortium understanding that **the project plan of GreenTurn does not prescribe any personal data exchange with authorities**. Further, as described above, GreenTurn does not hold personal data information with respect to the applications developed, and the project developed datasets will be audited to guarantee that the above condition is constantly in place without any violation. However, the data controller was made aware of the above distinctions.

In addition, in view of unforeseeable future developments, such as a project extension, the Consortium recommends that special measures are undertaken by the Project Coordinator in the event that personal data under the GreenTurn L project are transmitted to state law enforcement authorities. In the event that such measures are difficult to implement or could seriously affect the deliverables and success of the project, the Consortium invites the Project Coordinator to consider not undertaking any such exchanges at all during the GreenTurn project execution stage.

Technical and organizational measures

The Controller and each Project Partner, as appropriate, adopts appropriate technical and organisational measures with regard to Project execution (the "Measures"), and reviews and updates them where necessary.

Technical measures involve passwords and safekeeping of the data repository system of Teamwork. Registering credentials of users (checking who has access to data). Project partners are allocated with proper access levels and rights to data repository to ensure data safety.

Organizational measures, on the other hand, involve the processes in identifying the data sets used, updating them and keeping track of who has what. These involve:

- Meetings/ management calls in case there is a need to discuss data processing
- Data Management Plan as a data inventory exercise
- Reports/ records for data to update live information.
- Allocation of roles and responsibilities amongst the consortium as to who does what in terms of the personal data processing and security

A set of technical and organisational measures have been specified to ensure and to be able to demonstrate that processing is in compliance with GDPR.

Data anonymization principle

Whenever possible, including non-detrimental to Project execution purposes, Controller and Project Partners shall undertake efforts to keep personal data processed by them for Project purposes anonymous or pseudonymous.

According to the GDPR, "*anonymous information*" is information which does not relate to an identified or identifiable natural person, or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In this context, the GDPR does not apply to the processing of such anonymous information, including for statistical or research purposes.

Similarly, "*pseudonymisation*" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Both methods involve masking personal data by removing or encrypting the data field that makes it possible to link the information to an individual, such as name, address or passport number. So, if data is breached the party acquiring the data cannot really make use of it as there is a key missing decoding the data. However, the difference between the two is that pseudonymization can be reversed. Using separately held information, such as an encryption key, one can retrieve the identifiable information when needed to link the data back to an individual. Once data has been anonymized, however, it can never be linked back to an individual. Anonymization is permanent.

Data protection documentation system

Register of processing activities

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

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

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

Register of data breaches

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

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

Data breach

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

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

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

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

Data transfers to third countries

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

In the event that any Project Partner wishes to carry out such personal data processing, it shall notify the Controller in writing and in advance. Unless otherwise expressly specified, any international data transfers carried out by any Project Partner for any reason during Project

execution take place at its own exclusive liability and responsibility; same Project Partner shall hold all other Project Partners (including the Controller) harmless from any legal or other claims arising for such personal data processing.

Sanctions and damages

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

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

Data processing

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

Principles for legitimate processing

European Union data protection law set forth the following specific principles which have to be complied with for the processing to be legitimate.

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

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

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

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

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

- determine what the applicable (minimum and maximum) retention periods are for the personal data that is being processed;
- ensure that relevant retention periods are monitored.

People in charge of processing

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

Training and awareness

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

Policies and procedures

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

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

Notice and consent

Notice

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

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

Free and informed consent

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

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

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

- performance of a contract;
- legal obligation;
- public interest;
- legitimate interest of the controller or third party.

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

Withdrawal of consent

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

Data protection assessment

Assessment

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

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

Adequacy of protection

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

Impact assessment in case of high risk (DPIA)

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

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

Prior consultation to Supervisory Authority

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

GreenTurn list of Stakeholders Advisory Board Contacts

The GreenTurn list of Stakeholders Advisory Board (SAB) contacts relates to an excel sheet that includes the names of all the SAB Members and contact persons and their email address. It also indicates their expertise (justifying the purpose of contacting each of them) along with the organisation they belong. Both the Project Coordinator and Consortium Partners have access to this list of contacts. The purpose of this list is to keep a well organised list of Project SAB contacts for the GreenTurn communications. The data will be erased after the project end and not kept or maintained after the project end. This list is being stored at the Green Turn Teams server. Any person has the right to opt out of this list by direct email to the project coordinator.

Meetings' related material

This relates to any document created and used for the purposes of project meetings. These may relate to agendas, presentations, minutes, signature lists or any other internal document created for the purposes of GreenTurn meetings. All these documents will be created and maintained for internal purposes of GreenTurn and only GreenTurn partners will have access to them at GreenTurn Teams under the meetings section. They will be kept for 5 years after the project end (for auditing reasons). Any person has the right to opt out of being mentioned in these by direct email to the project coordinator before or after the meeting.

Workshops/Conferences and Training sessions

These data relate to the creation of workshops, agendas, programmes, participants' lists etc. and in general dissemination material related to GreenTurn organised workshops. Regarding the external publication of this material, we consider that this material can be fully anonymized so that it excludes personal information from the presenters/participants in the related programmes/agendas that will be shared publicly. For the parts of the related material that will be used for the workshop organisation internally to GreenTurn, the related files will be stored in the GreenTurn Teams server under the section meetings. The data will be kept for 5 years after the project end for auditing reasons. Any person has the right to opt out of being mentioned in these by direct email to the project coordinator before or after the event.

Reporting

Reporting refers to internal and external (EC) documents including GreenTurn's progress of activities, technical overviews etc. Related files will be including documents (reports with no personal identifiable information) and financial data (C forms) sometimes including personal data. The purpose of these data is financial so that partners can claim budget requests for their related effort in GreenTurn. C forms will be maintained by the project coordinator only and stored at internal and secure server. These (per partner) data are not to be shared with anyone internally or externally to GreenTurn, will be kept for 5 years after the project end (for audit purposes) and will be deleted after this date. Opting out of these data will be possible but will require an updated Form C to be submitted by the project partner.

Deliverables, internal documents and other GreenTurn reports

During GreenTurn project run-time, a large series of documentation and reporting will be provided relating to the project deliverables and/or internal documents etc. These files will be used for the project contractual obligations and shared to: GreenTurn partners, EC, public (depending on dissemination level). In these documents, the names of authors will be included. Following this, as far as the internal (to GreenTurn) and EC distributed documents are related, they will be used only for the purposes of reporting and stored in the GreenTurn Teams channel under the deliverables section. Reports that will be shared publicly (public deliverables) will mention only the partner name and not any other personal information. All reports will be kept for 5 years after the project end for auditing.

Source codes

As far as the inclusion of personal information inside source codes is concerned, GreenTurn intends to not use any such information into actual source code files produced in the framework

of GreenTurn foreground. In case that any partner wishes to include any personal information, a related consent form will have to be created, used and signed by the data owner(s).

Usage of cookies (in GreenTurn sites)

In the cases that in a GreenTurn application (web) the usage of cookies is needed, a related pop-up window informing the user must be present, prompting the user to accept (or not) the conditions under which her/his personal information are stored. GreenTurn will maximize efforts to reduce the usage of cookies in its web developments.

Lists of stakeholders and GreenTurn contacts

This list refers to internal GreenTurn lists of external stakeholders including potential technology/results up-takers, major links with end-users and other stakeholders. This list will be used for communication purposes of GreenTurn, no external access will be allowed (restricted to GreenTurn partners) and will be collected and stored by WP leaders. When people are being registered to this list, a consent by email will have to be sent by the data owner. The data will be kept until the GreenTurn project's end. Any person has the right to opt out of being mentioned in these by direct email to the project coordinator.

Project related research data (data from pilots)

Any data circulated internally to GreenTurn for research purposes (i.e., data from pilots for source code analysis, sensor data for analytics etc.) must be fully anonymized by the data owner (in this case the data controller) and not relating in any case to personal information, as stated in the sections above.

Any other GreenTurn related data

In case that personal information needs to be added in any other document in GreenTurn project, the controller (document creator) will have to notify the data owners of their personal details being included into the related document, purpose, retention, storage etc.

Personal data in newsletters, social media and other dissemination material

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

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

Annex III Peer Review Chart

GreenTurn Peer Review Reporting Sheet

Deliverable Number		Score Values	
Deliverable Name		OK, perhaps some minor comments	
Version		Is of reasonable quality, needs some re-work	
Review result		Needs substantial rework or additional work	

	Name	Organisation	Email	Phone
Deliverable Author				
Reviewer				

Content

#	Criteria	Explanation	Score	Explanation of Score by Reviewer	Suggested improvements	Response from Author/Writer
1	Main objective of the deliverable	Does it set out to do what it says in DOW? Are objectives clearly and simply stated and in line with the Description of Work (task description)? Further is it clear how these objectives are relevent to the overall targeted results of the project as a whole?				
2	Conformance of Results	Did the deliverable do what was promised? Is the aim of the deliverable achieved? Do the findings and results of the work match the objectives as described in the Description of Work and are these results clearly described in the deliverable.				
3	Methodology	Was the work, development, trial, experiment or study conducted in a sensible way? Are the Methods/procedures appropriate and correct?				
4	References and building on previous work	Have they overlooked any state of the art, previous work, related projects, regulations or best practices Does the report include and make use of relevant and necessary references?				
5	Plagarism	Is there plagarism in the document and is previous work or work of others clearly identified as such?				
6	Conclusions	Is there a conclusion chapter and does it make sense? The conclusion chapter reflects all described main important issues in the report. The conclusions are well based, relevant and applicable.				
7	Usefullness of results	Is the deliverable (and associated results) actually useful to downstream tasks or customers. Is it clear that the results are useful and relevent? Is it clear how results can be accessed Are plans realistic and actionable? Is it clear that they are not committing downsteam tasks to something impossible. For example KPI targets which cannot be reached or measured.				

Structure and readability

#	Criteria	Explaination	Score	Explaination of Score by Reviewer	Suggested improvements	Response from Author/Writer
8	Readability	Can you understand it easily? Is the document easy to read and understandable.				
9	Structure	Is the structure of the deliverable logical and easy to follow? If you feel it is not, please suggest changes to the structure to make it more accessible.				
10	Language	Are there any obvious spelling or grammar mistakes? Is the English in the deliverable good? Is the writing style clear, consise and accessible?				
11	Consistency with Description of work	Can the reader easily tell (e.g. by looking at the table of contents) where in the document each point in the DOW is addressed? Is it clear that the deliverable reflects the description of work?				

Presentation

#	Criteria	Explaination	Score	Explaination of Score by Reviewer	Suggested improvements	Response from Author/Writer
12	Template	Is the document template properly applied?				
13	Graphics	Are figures and tables legible and referred to in the text?				
14	Length	Is deliverable less than 100 pages in total?				
15	Referencing	Are the papers and other sources correctly cited and referenced?				

16	**Terms**	Are terms defined in the glossary? Unusual technical terms and acronyms should be added to the glossary. Ideally they should also defined in text the first time they are used unless this reduces readability or they are well known.				
Overall conclusion						
#	**Criteria**	**Explaination**	**Score**	**Explaination of Score by Reviewer**	**Suggested improvements**	**Response from Author/Writer**
17	**Quality**	Green - The deliverable can be submitted as is but could be improved if the issues raised are addressed. Amber - The issues raised must be addressed before submission. Red - There are substantive issues with the deliverable they need to be addressed and it will require a second review.				
Write general remarks/comments and conclusions						