

GREENGAGE

ENGAGING CITIZENS - MOBILIZING TECHNOLOGY - DELIVERING GREEN DEAL

Privacy Impact Assessment


Work Package 6, Deliverable D6.3

Privacy Impact Assessment

Work package 6, Deliverable D6.3

Please refer to this report as follows:

Javed, B., Khan, Z., Gebetsroither-Geringer, E. (2025). Data Privacy Impact Assessment. Deliverable D6.3 of the Horizon Europe project GREENGAGE.

Project information	
Project name:	GREENGAGE – Innovative governance, environmental observations and digital solutions in support of the Green Deal
Grant Agreement No.	101086530
Start date:	01/01/2023
Duration:	36 months
Coordinator:	AIT Austrian Institute of Technology Giefinggasse 4, 1210 Vienna, Austria
Contact:	Jan Peters-Anders, Research Engineer
	Funded by the European Union GA n° 101086530.
Deliverable details	
Description:	This document provides the Data Privacy Impact Assessment and procedures for the GREENGAGE project
Version:	Final
Dissemination level:	PU (Public)
Due date:	30/06/2025
Submission:	30/06/2025
Lead:	University of the West of England, UK
Author(s):	Javed, B., Khan, Z. (University of the West of England), UK Gebetsroither-Geringer, E. (AIT - Austrian Institute of Technology), Austria

Legal Disclaimer

All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user, therefore, uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors' view.

Users wishing to reuse material from this work that is attributed to a third party, such as tables, figures or images, are responsible for determining whether permission is needed for that reuse and for obtaining permission from the copyright holder. The risk of claims resulting from infringement of any third party-owned component in the work rests solely with the user.

© 2025 by GREENGAGE Consortium

Table of Contents

Content

1	GREENGAGE summary	2
2	Introduction	3
3	GREENGAGE Personal Data Types and Origin of Personal Data	4
4	Data Protection Impact Assessment.....	6
5	Assessment of Personal Data.....	7
6	Data Protection Officer	9
7	General Data Protection Principles and Obligations of Controllers and Processors in relation to Data Protection	10
7.1	General Data Protection principles.....	10
7.2	Obligations of Controllers and Processors.....	10
7.2.1	Controllers/Joint Controllers Responsibilities	11
7.2.2	Processors' Responsibilities.....	13
8	Data Subject Rights.....	15
9	Ethical principles and regulatory framework	17
10	GREENGAGE app publication on Google and Apple Stores	18
11	Lessons Learned and Recommendations.....	19
	References	21
	Appendix.....	22

List of Figures

Figure 1: Structure of project GREENGAGE.....	2
---	---

List of Acronyms

BCC	Bristol City Council
Borghi	I Borghi piu Belli D'Italia
BUAS	Breda University of Applied Sciences
CO	Citizen Observatory
DEUSTO	University of Deusto
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
KPI	Key Performance Indicator
MPA	Miljøpunktamager
POI	Point of Interest

UWE	University of the West of England Bristol
-----	---

Glossary

Citizen Observatory	According to European project WeObserve, “Citizen Observatories (COs) are community-based environmental monitoring and information systems, that invite individuals to share observations, typically via mobile phone or the web. Throughout these activities citizens become able to participate in environmental management/local governance.” [Reference: D2.1 - GREENGAGE Methodological Framework]
Data protection by design and by default	<p>Data protection by design is about considering data protection and privacy principles from the start of any processing operations. According to the principle of data protection by design (Art. 25 (1) GDPR), data controllers shall adopt technical and organisational measures to implement data protection principles and to protect the rights and freedoms of data subjects both at the time of the determination of the means for processing and at the time of processing itself. This principle requires appropriate safeguards to take place before the processing begins and the responsibility of deciding the process and mechanisms of processing rests with the controller. Periodic assessment of the adequacy of data processing measures shall be adopted during the whole duration of the processing.</p> <p>According to the principle of data protection by default (Art. 25 (2) GDPR), the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This principle is applied to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. This principle also requires that a given technology used to process data adopts by default the most privacy-preserving method to perform it. Furthermore, the organizational measures adopted to support processing operations should comply with the principle of personal data minimisation (e.g. collecting only necessary personal data).</p>
Pilot Owner	Pilot owner role is assigned to partners, mainly public administrations or organisations who are in charge of the setting up and running the Citizen Observatories in GREENGAGE project. For instance, Bristol City Council is pilot owner for the Bristol pilot. Borghi is pilot owner for Turano and Gerace pilots. MPA is pilot owner for Copenhagen pilot and Province of North Brabant is pilot owner for the North-Brabant pilot.

Executive summary

This document presents a thorough data **privacy impact assessment** which was performed by following the Regulation (EU) 2016/679 (General Data Protection Regulation), Regulation (EC) No 45/2001 on the protection of processing personal data by the Community institutions and bodies and on the free movement of such data; and other national regulations such as United Kingdom's Information Commissioner's Office (ICO). The aim was to identify potential data related risks and strategies to handle those risks in GREENGAGE. This document presents the types of personal data being handled by GREENGAGE project and how the personal data is processed and managed in the project by both technology partners and city pilots. Furthermore, detailed assessment of personal data as per General Data Protection Regulation is covered in this document. The document also covers in detail the obligations of controllers and processors in relation to data protection. Finally, the document presents recommendations.

Related documents

Deliverable D1.9 - Ethical Management and Activities Plan 1
Deliverable D1.10 - Ethical Management and Activities Plan 2
Deliverable D1.11 – Data Management Plan 1
Deliverable D1.11 – Data Management Plan 2
Deliverable D2.1 - GREENGAGE CO Methodological Framework
Deliverable D2.2 - Use Cases and Requirements Analysis 1
Deliverable D2.3 - Use Cases and Requirements Analysis 2
Deliverable D2.4 - Smart Governance Models 1
Deliverable D2.5 - Smart Governance Models 2
Deliverable D2.6 - GREENGAGE Technological Requirements 1
Deliverable D2.7 - GREENGAGE Technological Requirements 2
Deliverable D4.1 - GREEN Engine and Manual 1
Deliverable D4.2 - GREEN Engine and Manual 2

1 GREENGAGE summary

The pan-European Innovation Action, funded under the Horizon Europe Framework Programme, aims to promote innovative governance processes, and help public authorities in shaping their climate mitigation and adaptation policies. To achieve this aim, the GREENGAGE project will leverage citizens' participation and equip them with innovative digital solutions that will transform citizen's engagement and cities' effectiveness in delivering the European Green Deal objectives for carbon neutral cities.

Focusing on mobility, air quality and healthy living, citizens will be inspired to observe and co-create their cities by sensing their urban environments. The aim is to complement, validate, and enrich information in authoritative data held by the public administrations and public agencies. This will be facilitated by engaging with citizens to co-create green initiatives and to develop Citizen Observatories (CO). In GREENGAGE, Citizen Observatories will be a place where pilot cities will co-examine environmental issues integrating novel bottom-up process with top-down perspectives. This will provide the basis to co-create and co-design innovative solutions to monitor environmental problems at ground level with the help of citizens.

With two interrelated project dimensions, the project aims to enhance intelligence applied to city decision-making processes and governance by engaging with citizen observations integrated with Copernicus, Global Earth Observation System of Systems GEOSS, in-situ, and socio-economic intelligence, and by delivering innovative governance models based on novel toolboxes of decision-making methodologies and technologies.

The envisioned Citizen Observatories campaigns will be deployed and fully demonstrated in 5 pilot engagements in selected European cities and regions including: Bristol (the United Kingdom), Copenhagen (Denmark), Turano and Gerace (Italy) and the region of North Brabant (the Netherlands). These innovation pilots aim to highlight the need for smart city governance by promoting citizen engagement, co-creation, as well as gathering new data which will complement existing datasets and evidence-based decision and policymaking.

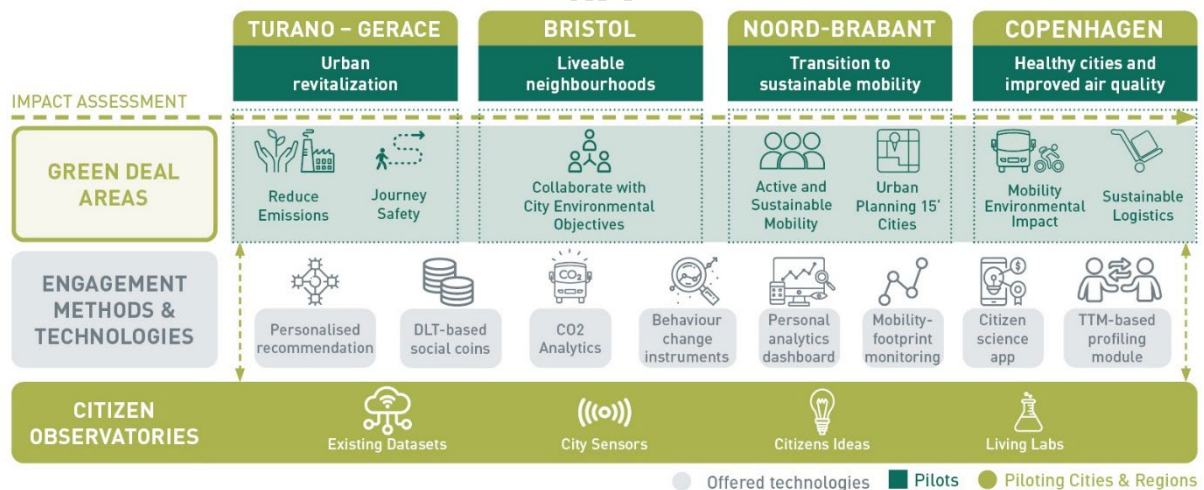


Figure 1: Structure of project GREENGAGE.

2 Introduction

The GREENGAGE project aims to promote innovative governance grounded on collaborative evidence-based decision-making, where citizens are actively involved in governance structure to co-create green initiatives to accelerate sustainable development, and to develop Citizen Observatories (CO); which also support the delivery of European Green Deal¹. Citizens will be facilitated to observe and co-create their cities by sensing their urban environments that will complement, validate, and enrich information held by public administration and/or environment agencies derived from remote sensing data and obtained via other authoritative observations. For this purpose, GREENGAGE technology partners provide a suite of interoperable tools to support needs of specific piloting use cases whereas GREENGAGE's pilot cities Bristol (the United Kingdom), Copenhagen (Denmark), Turano and Gerace (Italy), and the region of North Brabant (the Netherlands) will be involved with citizens' engagement, organising CO campaigns, and assist in bottom-up initiatives.

The above-mentioned aim indicates that during the life of the project, diverse data has been generated and used (refer to D1.11 and D1.12 Data Management Plan 1 & 2) including personal data. Given diverse data being collected in GREENGAGE project, Data Protection Impact Assessment (DPIA) was needed. This document details the assessment of personal data that is being collected and handled in GREENGAGE project.

The report is structured as follows: **Chapter 3** covers GREENGAGE personal data types and origin. **Chapter 4** gives overview of data protection impact assessment. **Chapter 5** presents assessment of privacy of the personal data. Details on GREENGAGE DPO is given in **Chapter 6** whereas **Chapter 7 and 8** covers general data protection principles and obligations of controllers and processors and Data subject rights. Evaluation of ethical principles and regulatory framework is presented in **Chapter 9**, GREENGAGE app publication on google/apple in **Chapter 10**. Finally, lessons learned, and recommendations are given in **Chapter 11**.

¹ https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en

3 GREENGAGE Personal Data Types and Origin of Personal Data

In GREENGAGE following types of personal datasets are collected and managed.

Data contributors and users of the applications. The personal data involve username, first name, last name, email address, password, profile picture, GREENGAGE ID, City Connection ID. Sociodemographic data also includes language (English, Danish, Italian, Dutch), acquaintance level of digital tools, role in the co-production process, age-range, social/disadvantaged group, education level, gender, and type of organisation to which the user belongs, work status, and city where the user lives. For U18s, school, parent name, and email address are collected as part of the consent protocols.

Origin of the data: The login data (email address, username and password) is required to provide a single-sign-on to different GREEN Engine tools e.g., GREENGAGE app², MindEarth for GREENGAGE app³, Collaborative environment⁴, Superset⁵ etc. The sociodemographic data is collected to measure statistical Key Performance Indicators i.e., number of users signed up using the **GREEN Engine**, number of users signed up from different age group and social groups to assess level of inclusivity in GREENGAGE COs. We also need this information to create a valid useful dataset in the context to know which social group answered the surveys in the GREENGAGE App.

From Citizens as active sensors. This mainly includes data collected from GPS tracking such as users' location (Geographical GPS Coordinates (e.g., Spots in GREENGAGE app)). GPS tracking information in form of AIT Mode Binary data⁶ (which is transformed into GeoJSON and contains the user-id).

Origin of the data: The **GREENGAGE app** is collecting information of Point of Interests (POI) from users and experiment related task data e.g., answering pre-defined questions related to a specific POI. Tracking data is also collected and analysed by the app. Similarly, **MindEarth for GREENGAGE app and Atomtube sensors** collect GPS linked data. Citizen data such as GPS location is used to verify adherence to mission brief, to verify quality of collected data and geo-locate features extracted from anonymised imagery. Further, dashcam recording frames for road surface defects include GPS coordinates.

Workshop or Survey Data. This data is collected and handled by the Pilot Owners, based on their standard practices, methods and tools. This data includes socio-demographic data in line with established organisational procedures of the Pilot owners and no GREENGAGE technology is used for collecting such data. For example, Bristol City Council gathers personal data as per their equality considerations for standard survey or consultation procedures. The Pilot Owners collect the personal data to analyse whether collected data is representative enough and ensure data quality. For privacy and confidentiality, none of this personal data is shared with the GREENGAGE consortium partners or any 3rd party. This data is required e.g., to determine and ensure engagement with under-represented groups is achieved. For example, North-Brabant collects personal data to highlight contrasts in age or gender to illustrate the varied nature of maintenance requirements such as to improve the road infrastructure and make biking more appealing; understanding these differences can lead to a more target-audience approach. Survey Data is used to determine the base data, POIs, formulation of research questions, usability of tools and to evaluate and determine the impact of GREENGAGE COs.

Origin of the data: GREENGAGE pilot owners have been using both online and paper-based approaches to collect survey, workshops, walks, and interview data. For online surveys, MS forms, Google forms, EU Survey or Qualtrics are used to collect the responses.

GREENGAGE only collects socio demographic data through <https://me.greengage-project.eu/>. Cities have their own standard practices to conduct surveys. To involve representative groups, they might collect additional personal data, but it is not used and shared with GREENGAGE project.

Interview data. With the help of pilot support teams, pilot owners will conduct interviews and focus group meetings with citizen observers and other stakeholders (e.g., local businesses), to seek their viewpoints about the GREENGAGE innovation pilots and Citizen Observatories. The focus will be on the

² [GREENGAGE APP API - GREENGAGE Documentation](#)

³ [MindEarth for GREENGAGE app - GREENGAGE Documentation](#)

⁴ [Collaborative Environment - GREENGAGE Documentation](#)

⁵ [Apache Superset - GREENGAGE Documentation](#)

⁶ [MODE - GREENGAGE Documentation](#)

usability, benefits of GREENGAE Citizen Observatory and what practical implications this must sustain these COs in future. The analysis of interviews will be used in reports in aggregated form. In some cases, and with the consent of the participants interviews maybe used for dissemination and communication activities.

Origin of the data: Manual notes and recordings will be done by using GDPR compliant tools such as UWE MS Teams or other GDPR compliant mobile recording devices.

The format of these datasets is detailed in GREENGAGE's Data Management Plan (refer to D1.12 Data Management Plan 2).

4 Data Protection Impact Assessment

The Data Protection Impact Assessment (DPIA) process assesses the risk associated with projects, systems or processes that involve or may involve the collection or handling of personal information. It identifies risks to individuals' privacy rights and/or corporate risks (such as failure to comply with relevant data protection legislation) and, where relevant, identifies measures required to mitigate those risks.

The DPIA should be carried out before the data collection and any processing is performed, considering the possible implication from the beginning even if the processing operation have not been clearly defined yet. In the latter case, the DPIA will need to be updated once the data processing officially starts and maintained throughout the lifecycle of the project, to reflect the actual state of the activities involved and maintain compliance.

The DPIA is needed when personal data processing is likely to result in a high risk to the rights and freedoms of data subjects. The primary right of data subjects is the right to data protection and privacy. Other fundamental rights are freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience, and religion. The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*"⁷. It is particularly relevant when a new data processing technology is being introduced.

In cases where it is not clear whether a DPIA is required, the Article 29 Data Protection Working Party⁷ recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law. This article provides a following common European Union list of processing operations for which a DPIA is mandatory:

- **When using evaluation or scoring methods, including profiling:** this may involve information and/or prediction related to data subject's performance at work, economic situation, health, personal preferences or interests, behaviour, location, or movements.
- **When employing automated decision-making.**
- **When systematic monitoring of data subjects is performed:** this includes processing of data collected through networks or from a publicly accessible area.
- **When processing sensitive data or data of a highly personal nature:** This incorporates special categories of personal data and data relating to criminal convictions (Art. 9 and 10 GDPR).
- **When data is processed on a large scale:** This in specific includes the volume of data processed, the duration, and the geographical extent of the processing.
- **When matching or combining datasets:** when datasets originate from two or more data processing operations performed for different purposes and/or by different data controllers (exceeding the reasonable expectations of data subjects) then DPIA is needed.
- **When data subjects fall under vulnerable category:** Examples include minors, other vulnerable groups.
- **When applying new technological or organisational solutions:** such as AI or IoT.
- **When the processing itself prevents data subjects from exercising a right or using a service or a contract.**

In the light of the above points, DPIA was carried out in GREENGAGE because minors are involved, and GREENGAGE app collects location data. Similarly, personal data is also collected by pilots during interviews and surveys. DPIA was carried out by UWE (Questionnaire is given in Appendix) to assess any potential risk associated with handling/processing of personal data by both pilots and technology partners. As a result of DPIA, the collected responses were assessed in the light of GDPR. The rest of the document covers how GREENGAGE abides to GDPR to handle the personal data collected by both technology partners and pilots.

⁷ WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (WP248 rev.01, 4 October 2017) 9-11.

5 Assessment of Personal Data

GREENGAGE's personal data

- aligns with UK⁸ and EU⁹ GDPR guidelines
- follows the “Data protection by design and by default” approach
- considers ethical considerations to process personal data
- is in line with the project associated agreements (Grant agreement, consortium agreement).

5a. GREENGAGE personal data aligns with both UK and EU GDPR guidelines. Bristol City Council follows UK GDPR guidelines for handling the personal data whereas other pilots Miljøpunktamager (Copenhagen, Denmark), I Borghi piu Belli D'Italia (Turano/Gerace, Italy), and Noord-Brabant Provincie (North Brabant, The Netherlands) abides to EU GDPR guidelines.

5b. Personal data in GREENGAGE is processed and handled using data protection by design and by default approach. Potential risks of tracking and identifying individuals are considered from the start of the GREENGAGE project. **Data Protection by Design** is conceptualised/implemented at both tool level and other means of collecting and processing personal data such as surveys and interviews. For instance, User ID, name and email address are used to login and give personalised experience to users using the GREENGAGE app. However, these data elements are removed once the final data is stored on GREENGAGE DRUID data storage and DRUID storage is completely anonymous. The GREEN Engine tools process personal data at the time of collection. GREEN Engine's login data (i.e., Personal data generated by data contributors and users of the applications (see section 3a)) which is stored in a protected database is encrypted and is not used for the purpose of sharing and profiling.

Personal data collected from Citizens as active sensors (Section 3b) i.e., GPS-linked data collected by the MindEarth for GREENGAGE app is encrypted and anonymised at the time of collection. All images collected through the MindEarth for GREENGAGE app are immediately encrypted locally on the local drive before being securely transmitted to the cloud server for anonymisation, deletion and storage. This prevents any misuse of locally stored data. In addition, the access to collected anonymised data and data processing tasks is restricted to authorised MindEarth personnel. Unique authentication credentials and/or a strong password associated to each authorised user are required to access and process data.

Personal Data collected by pilots through surveys and interviews (Section 3c and 3d) are protected by using their internal standards and procedures. The personal data collected by pilots is not shared with the GREENGAGE project. For example, both Bristol City Council and Borghi Più Belli d'Italia collect personal data via paper-based and online surveys and interviews but as the personal data is handled as per their internal procedures and policies and personal data not being shared with GREENGAGE, the GREENGAGE app does not require assessment and management of their personal data.

As the North Brabant pilot was not using the GREENGAGE app in the first place, the way personal data was handled was as follows. The pilot gathered GPS data of travel patterns and details of commuting (including origin and destination of trips). Later, in-depth interviews were conducted relating to travel choices. These interviews were based on written questionnaires and notes, without recording requirements. These interviews happened individually, but could also happen in a group setting, facilitated by the data visualisation of the Digital Twin. The GPS and interview data were anonymised. The interview and survey results were presented as general trends or remarks, and GPS patterns were quantified in origin-destination matrices. Aggregated travel pattern data has no need for personal data but has general origin destination relations. Files containing personal data are locked away or saved on secure servers and are only accessible to involved researchers. North Brabant pilots implemented following measures to mitigate any loss of data:

- All important data is stored on the BUAS Research Drive which grants access only to involved researchers
- Involved researchers have to login on BUAS Research Drive with SURFconnect (Multifactor Authentication)

⁸ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>

⁹ <https://gdpr.eu/>

- Back-ups of the data stored on BUAS Research Drive are made every 24 hours
- The personal data collected by North Brabant is not shared with REENGAGE.

REENGAGE also ensures **Data Protection by Default** by only allowing the collection and processing of necessary personal data. For example, the pilots collect personal data to ensure that the participating groups are representative. This personal data is important for analysis purposes from the perspectives of socioeconomic background, minors, ethnicity, gender etc. In terms of tools, the GREEN Engine only contains necessary personal data such as username, email, and password. Other personal details such as date of birth, home address, etc. are not captured.

5c. To process personal data, ethical guidelines are followed in REENGAGE. To enable participation in the REENGAGE project, formal consent is sought from all participants before participating in the study. Participants are also reassured of their freedom to withdraw from the project where data is not anonymised and until the final report is being prepared (details are presented in Section 8). Information sheets and consent forms are shared before they participate in COs. In general, all user involvement activities are on a voluntary basis and the users receive appropriate information on the processing of their personal data and all other ethical implications during the piloting. The ethical guidelines and regulatory framework used in REENGAGE are presented in Section 9 (refer to Deliverable D1.9 and D1.10 Ethics Management and Activities 1 & 2).

6 Data Protection Officer

We do not have a DPO for the project. The data protection breaches are handled at partner level as per their data protection/GDPR policies. Section 7 provides data protection principles that all partners abide to.

7 General Data Protection Principles and Obligations of Controllers and Processors in relation to Data Protection

This section provides an overview of the main principles involved in the management of personal data within the GREENGAGE project which the partners have considered whilst designing their data management strategy together with an overview of commitments of the partners undertaken to respect these principles. This section also covers obligations of controllers/joint controllers and processors in relation to the personal data protection.

7.1 General Data Protection principles

Article 5 of the UK GDPR and EU GDPR sets out seven key principles of the general data protection. The principles are as follows:

- **Lawfulness (Art 5(1a)):** For personal data processing, a legal basis must be identified. As per Art. 6 (1) GDPR, personal data processing is lawful only at least when one of the following applies:
 - (a) The data subjects have freely given an explicit consent for processing his or her personal data for one or more specific purposes
 - (b) processing for the necessity for the performance of a contract of which the data subject is part of or to take steps at the request of the data subject prior to entering into a contract
 - (c) Necessity for the compliance with a legal obligation to which controller is a subject
 - (d) Necessity to protect the vital interests of the data subject or of another natural person
 - (e) Necessity for the performance of a task carried out in the public interest or
 - (f) Necessity for the purposes of the legitimate interests pursued by the controller or others, except if overridden by the data subjects' fundamental rights and interests.
- **Fairness (Art 5(1a)):** Processing of personal data should ensure fair balance of the data subjects' rights and freedoms against the controller's interests.
- **Transparency (Art 5(1a)):** Personal data must be processed in a transparent manner, providing data subjects with all necessary information with regards to processing their personal data including the processing activities, the purposes of the processing, as well as the parties with which their data is shared.
- **Purpose limitation (Art 5(1b)):** Data must be processed only for specified, explicit, and legitimate purposes. Any further processing, such as scientific research or statistical purposes, must be compatible with the initial purpose(s).
- **Data minimisation and storage limitation (Art 5(1c) and Art 5(1e)):** Only the data that are strictly relevant and necessary to the purpose must be processed. The data must not be retained than what is required to attain purpose of a project/research.
- **Accuracy, integrity and confidentiality of the data (Art 5(1d) and Art 5(1f)):** Personal data processed must remain accurate and up to date. It must be processed in a secure manner, adopting technical and organisational measures to help protect the data against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- **Accountability (Art 5(2)):** Compliance with the relevant personal data protection principles (mentioned above).
- **Data protection by design and by default (Art 25):** Data protection must be considered from the beginning of the project and adequate, state-of-the art measures must be adopted to protect data subjects' rights and freedoms.

7.2 Obligations of Controllers and Processors

As stated in the Data Management Plan (refer to D1.12 Data Management Plan 2), GREENGAGE has joint controllers. Both UK and EU GDPR explicitly state the obligations of controllers and joint controllers for processing personal data. Similarly, data processors must also abide to data protection principles.

This section states the obligations of controllers and processors and how these obligations are fulfilled in GREENGAGE.

As per Art 26 of GDPR, Joint controllers must enter into a Data Controllership Agreement. According to this article, joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the GDPR and reflect their respective roles and relationships vis-à-vis the data subjects. GREENGAGE's joint controllers have identified their roles and responsibilities which aligns with the GDPR. How the personal data is dealt with is also communicated to data subjects as part of the consent procedure which includes sharing a Participant Information Sheet. Apart from Art 26, Controllers and Joint controllers must also share the following responsibilities.

7.2.1 Controllers/Joint Controllers Responsibilities

In GREENGAGE, data controllers are responsible for protecting the data lifecycle i.e., from collection to processing, storage, security, and sharing. They also define purpose and means of data processing. In GREENGAGE, GDPR principles (Section 7.1) are strictly followed in addition to other responsibilities that controllers must abide to.

- **According to Art 5(1a), Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.** In GREENGAGE, the personal data handled by the pilots and technology partners is processed fairly, lawfully, and in transparent manner. Citizens/users are informed through Consent form and Participation Information Sheets. Users' consent is also needed when they are using the GREEN Engine tools.
- **Art 5(1b) requires personal data to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes i.e., purpose limitation.** As per GREENGAGE's grant agreement, representative samples should participate in Citizen Observatories as well as GREENGAGE promotes inclusive participation, therefore pilots collect socio-demographic personal data so that representative citizens could be included. Furthermore, frequency of personal data collection is minimum and as per the project's needs. Pilots collect personal data "Once at the start, before involvement in the pilot". Similarly, a registration process is applied to allow participants to provide socio-demographic details and create a login that can be used across all tools provided by the GREENGAGE project; in case of the MindEarth for GREENGAGE app, when users carry out, complete, and upload missions then street imagery is also collected but is anonymised.
- **Art 5(1c) demand all personal data collected, processed, or transferred within the project to be adequate in relation to the purpose of the project (data minimisation).** In GREENGAGE, tools only collect personal data which is needed for proper functioning of tools and needs of the project e.g., representation analysis. Similarly, pilots collect personal data so representative sample could be included in the project. Technology partners and pilots do not use personal data outside the scope of the project; for example, Collaborative Environment uses personal data for statistics of how many users created co-production processes. As the central authentication solution (i.e., KeyCloak) collects personal data for authentication and authorisation and to login to the GREENGAGE app, Collaborative Environment, and Discourse. Pilots collect personal data to assess whether the participation is representative as well as to determine whether certain Key Performance Indicators (KPIs) have been met.
- **Art 5(1e) emphasise on storage limitation i.e., retain personal data as long as absolutely necessary.** After completion of the GREENGAGE project (December 2025) personal data will be retained for as long as necessary to provide evidence of compliance with good scientific practice in accordance with the relevant guidelines. Research data must currently be retained for a period of ten years in principle. If this period changes in the future personal data will be stored for a correspondingly shorter or longer period. After the lifetime of the project, AIT will oversee data retention and all the components of the GREEN Engine will be on AIT premises (except for the GREENGAGE app back end). This aspect will be further discussed in Deliverable D7.15 Replication and Sustainability Roadmap V2.
- **Art 5(1d) and Art 5(1f) requires accuracy, integrity, and confidentiality of personal data.** Pseudonymisation and anonymisation techniques are used by GREENGAGE technology partners and pilots for maintaining confidentiality of personal data.

- **Data protection by design and by default (Art 25).** How GREENGAGE follows data protection and design principles is elaborated in Section 5.
- **Art 5(2) emphasises on accountability under which controllers shall ensure and document that the activities carried out comply with applicable data protection laws and implement any necessary technical and organisational measures.** In GREENGAGE, both organisational and technical measures are recommended to ensure data protection. For technology, a pseudonymised approach is used to delink socio-demographic data with the mission or experiment data. This personal demographic data is not shared with other parties and project partners and only used to perform social analysis e.g., participation levels from different genders etc. The handling of personal data rests with the controllers of the GREENGAGE project. Under this article of GDPR, the project should comply with other data protection principles. The points above show that GREENGAGE abides to general GDPR principles.

In addition to abiding to general data protection principles, data controllers are also responsible for defining relations with processors, security of data processing, and handling duty of cooperation and any data breaches. All partners are working under a consortium agreement which mandates compliance to GDPR and data protection regulations.

- **Relations with processors (Art. 28): As per this article, controllers can appoint only those processors that can ensure compliance with the GDPR, through a written contract, laying down clear rules, limitations and obligations for the processing activity.** GREENGAGE has multiple processors including UWE, BUAS, VRViS, MindEarth, Sushi Dev, Deusto, AIT, and Pilot Owners (the details of data processors and their responsibilities are given in the D1.12 Data Management Plan). As per Art 28, data processors comply with the GDPR. Data processing and analysis by processors are done as such that participants are not identifiable. It has been agreed in the project that personal data will be either anonymised or pseudonymised by controllers before sharing with the processors. For example, data shared on UWE OneDrive is anonymised/pseudonymised before transmission by controllers.
- **Security of data processing (Art. 32): Controllers shall ensure data security, integrity and confidentiality, avoiding to the greater extent possible accidental or unlawful destruction or loss, alteration, unauthorised disclosure of or access to data.** Strict security measures are taken by both pilot owners and technology partners for protecting the personal data. GREENGAGE's pilots used both online and paper-based approach to collect survey, workshops, walks, and interview data. For the paper-based approach pilots store the data in physical folders in secure cabinets. The folders can only be accessed by authorised and associated staff or researchers. Furthermore, anonymised and/or aggregated data is kept on UWE's OneDrive. Therefore, UWE has defined the folder structure on their OneDrive where data is stored. Only selected GREENGAGE partners have controlled access to those folders.

The personal data (e.g., age group, gender etc.) which is gathered in surveys is aggregated (for paper based or other survey tools) and pseudonymised (especially those which are linked with DEUSTO's KeyCloak) or anonymised (which are not linked with the DEUSTO's KeyCloak) to protect privacy. Data stored on UWE's secure OneDrive is in aggregated form and no personal data is stored. Digital copies of consent forms are also stored on UWE OneDrive folders. Only the pilot owner and selected UWE staff has controlled access to consent forms' folder. Further, different access levels are provided to these folders depending on co-researchers' needs.

North Brabant data is being managed by BUAS. During the research, raw and processed data is stored on the BUAS Research Drive (BUAS branded instance of SURF Research Drive). This secure environment has been specifically created for storage, meeting the BUAS Regulation pertaining to Research Data Management. Physical data, such as the paper-based signed consent forms, are stored in physical folders in locked cabinets, only accessible to associated researchers (like digital data). Next to that they are digitised and added to the BUAS Research Drive as Data Documentation.

In addition to pilots, personal data is also managed and handled by technology partners. To apply privacy by design principle, the pseudonymisation data technique is used to protect privacy of participants. Rather than having fully anonymous records, each record is associated with the participants' unique ID (in GREENGAGE it is called GREENGAGE ID). Participant credentials are managed by KeyCloak¹⁰, the

¹⁰ KeyCloak - <https://www.keycloak.org/>

open-source identity and access management system, deployed and managed by DEUSTO. Once the data is analysed/summarised the data is anonymous and cannot be traced back to the participants. No personal data is made available in the public domain to ensure that privacy of participants is protected. Only anonymised data will be published. Personal data captured using GREEN Engine is managed by KeyCloak. No personal data is transferred to the GREENGAGE project's central data repository DRUID¹¹. Only selected GREENGAGE partners have access to KeyCloak storage.

In addition to the above security measures, further measures are applied to datasets and are detailed as follows:

- **MindEarth for GREENGAGE app mission data:** collected by the MindEarth for GREENGAGE app follows the following security measures: (i) Encryption: All images collected through MindEarth for GREENGAGE app are immediately locally encrypted before being securely transmitted to the cloud server for anonymisation, deletion and storage. This prevents any misuse of locally stored data (ii) Restricted access: Access to collected anonymised data and data processing tasks are restricted to authorised MindEarth personnel, via specific software- authorised machines using a strict authentication method (i.e., access key) at specific locations (i.e., as identified by their IP address). Unique authentication credentials and/or a strong password associated to each authorised user are required to access and process data (iii) Security at Access Level: raw, unprotected street-level imagery is not retained or shared with any third parties, including members of the GREENGAGE consortium.
- For **street quality survey data**, the GREENGAGE app relies on numerous industry standards (such as Claim-Based Authentication) to ensure data integrity within the overall context. In addition to common features like HTTPS connections, there are also content-specific mechanisms for COs to supervise data integrity qualitatively and, most importantly, collaboratively (e.g., Validation tasks/missions). Authentication via the GREENGAGE app, by default, integrates the KeyCloak and Username/Password mechanisms. Endpoint wise any data mutation needs to be authenticated via a JWT (JSON Web Token).
- **Community air quality observations** (such as by Atmotube): Atmotube data security measures are covered in their privacy policy: <https://atmotube.com/privacy> GREENGAGE retrieves device specific data from Atmotube cloud storage by using a unique API key and the HTTPs protocol. The API key is received by registering physical address and serial number of the sensor, see details here: <https://atmotube.com/atmotube-support/atmotube-cloud-api>
- **Co-production data** (by Collaborative Environment): the data is password protected and personal data such as email can only be accessed by authorised users.
- **The Discourse platform** prioritises data security by hosting the service on a secure AWS server located in the European Union. Access to the platform is exclusively via HTTPS, ensuring encrypted communication, and is protected through OAuth authentication provided by KeyCloak for robust identity and access management. Data collected includes essential personal information such as usernames, email addresses, and optional profile details, along with user-published topic data. Sensitive information like email addresses is treated as strictly confidential, while public-facing data is visible to platform participants. The platform complies with GDPR by minimising data collection and retaining user information only as long as necessary. Users are informed of their data protection rights and can manage their data through a control panel, ensuring a secure and privacy-compliant experience.
- **Data breaches notification (Art. 33 GDPR):** **Controllers shall notify data breaches to the competent DPO and to data subjects, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.** Since GREENGAGE does not have a DPO, the data protection breaches are handled at partner level (by controllers) as per their data protection/GDPR policies. In case of any data breaches, data controllers are responsible for notifying data subject and handling the case.

7.2.2 Processors' Responsibilities

This section illustrates the responsibilities of processors as per EU and UK GDPR. Data Processors of GREENGAGE are UWE, BUAS, VIRViS, MindEarth, Sushi Dev, DEUSTO, AIT, and Pilot owners. Their

¹¹ DRUID - <https://druid.apache.org/>

responsibilities in the project are detailed in D1.12 Data Management Plan. In terms of privacy data protection, their responsibilities are as follows:

- **Confidentiality (Art. 28(3b)):** This article requires that persons who are authorised to process the personal data should be committed to ensure confidentiality or are under an appropriate statutory obligation of confidentiality. GREENGAGE strictly ensure confidentiality. As data is anonymised or pseudonymised, it is not possible to identify individuals whilst performing data analysis and summarisation. It is also ensured that individuals data is not processed without their knowledge and are only processed with their 'explicit' consent. Furthermore, personal data is not shared with 3rd party organisations. Similarly, personal data will not be disclosed in any research publications.
- **Sub-processors (Art. 28(2) and 28(4)):** Processor can also assign the responsibilities of data processing to further sub-processors. However, engaging another processor requires prior written authorisation of the controller. A sub-processor can be appointed using a written contract which places on the sub-processor the same data protection obligations placed on the processor by the controller. In GREENGAGE, no sub-processors are involved.
- **Deletion or return of data (Art. 28(3g)):** As per this article, processors are obliged to delete or return all the personal data to controllers unless Union or Member State law requires storage of the personal data. GREENGAGE processors do not handle the personal data, and the responsibility rests with the controllers. For instance, UWE who is one of data processors does not handle any personal data and the data shared with UWE is anonymised by controllers (before sharing the data).
- **Security measures (Art. 32 (1)):** Adopting all the technical and organisational measures to ensure a level of security appropriate to the risk of processing. Security measures are applied by controllers as discussed in the previous section. Data processors in GREENGAGE are not responsible for applying data security.

8 Data Subject Rights

The Charter of Fundamental Rights (Article 8) of the EU¹² provides the core elements of the right to personal data protection. These core elements are further developed by the GDPR, which establishes new rights for data subjects. Therefore, GREENGAGE partners (both pilot owners and technology partners) are obliged to commit to respect, guarantee, and facilitate the exercise of these rights (where applicable), as follows:

- **Right to information** (Art. 13 and 14) permit data subjects to learn, among others, who is collecting and processing their data, for which purpose and on which legal grounds, the duration it will be kept and with whom it shall be shared, unless otherwise stated in the legislation.
- **Right to access their personal data and obtain a copy** (Art. 15) of the information which refers to them.
- **Right to rectification** (Art. 16) of their personal data where it is inaccurate or incomplete.
- **Right to erasure (also known as “right to be forgotten”)** (Art. 17), gives data subjects the right to erase their data, unless there is an exception.
- **Right to restrict** the processing of subjects’ data (Art. 18).
- **Right to data portability** (Art. 20), where applicable, in a commonly used and machine-readable format.
- **Right to object** (Art. 21) to the processing of their data where the data was not collected directly from them, unless compelling legitimate grounds override their interests and rights.
- **Right to not be subject to automated decision-making and profiling** (Art. 22), unless it is necessary for entering into a contract between the data subject and a data controller or it is authorised by Union or Member State law to which the controller is subject, or it is based on the data subject’s explicit consent.

The data subject rights are established in GREENGAGE by first acquiring ethical approval (the process of ethical approval is covered in D1.9 and D.10 – Ethics Management and Activities 1 & 2) and then getting consent of participants using a consent form before their data collection (Art 13 and 14). Participants information sheets and consent forms are shared before they participate in COs. In general, all user involvement activities are on a voluntary basis and the users receive appropriate information on the processing of their personal data and all other ethical implications during the piloting.

Participants were informed of all relevant aspects of the pilot that might reasonably be expected to influence their decision to participate. Furthermore, informed written/accepted consent by the participants is a requirement for their participation in the GREENGAGE project tasks. Following are the ways in which the data subjects’ rights are established in GREENGAGE.

- Art 13 and 14 – Data Subjects are informed about: The purpose and expected duration of the study; Potential risks (if any) and benefits of participating in the study; Which data will be collected in the study, in particular, the data directly related to the volunteer and to what degree (and how) confidentiality of such data will be ensured; Who will oversee storing the collected data and who will have access to it; What kind of processing will be performed with the collected data and for how long the collected data will be maintained; Contact persons for the study who can answer any questions the participant may have.
- Art 15 – GREENGAGE allows participants to receive a copy of their personal data which allows them to check that this data is lawfully processed.
- Art 16- Any personal data that is inaccurate or incomplete can be rectified in GREENGAGE.
- Art 17- Participants are reassured of their freedom to withdraw from the project. However, the withdrawal of consent does not affect the lawfulness of processing based on the consent before its withdrawal. Those who do not wish to give their consent are not included in any studies and resulting publications. A proper procedure is defined and is accessible to participants if they wish to withdraw from the study. Participants can withdraw their consent from GREENGAGE by

¹² Charter of Fundamental Rights of the European Union [2012] OJ C 326/391

unticking the consent form acceptance checkbox in the site <https://me.greengage-project.eu/>, which collects profile data for those partaking in GREENGAGE's thematic co-explorations. As a result, participants can no longer log on into GREENGAGE tools. The withdrawal request issued through privacy@greengage-project.eu will be met within one month (with extensions for some cases). Also, in the consent form it is mentioned that participants can withdraw from the study by following this set procedure. The partner responsible for the data collection ensures that all instances of the records are removed. However, it is not possible to withdraw and delete data where anonymised data is collected, or data has been summarised prior receiving withdrawal request. This is clearly indicated in the consent form.

- Art 18 – Data subjects have rights to request the restriction of processing of their personal data. This enables them to request to suspend the processing of their personal data. For example, data subjects can request to establish the data's accuracy or the reason for processing their data.
- Art 20 – Data subjects can request to transfer their personal data to another party thus allowing them right to data portability.
- Art 21 – Data subjects have the right to object to personal data processing. Data subjects can raise their concerns via privacy@greengage-project.eu. If data subjects are not satisfied with any aspect of our handling of their personal data, they have right to make a complaint at any time to GREENGAGE coordinator (coord@greengage-project.eu). This information has also been communicated to data subjects.
- Art 22 – Though the GREENGAGE tools gather qualitative data provided by the users/Citizen Observers; the App processes the data, but it does not create an explicit profile of its users.

9 Ethical principles and regulatory framework

GREENGAGE comply with ethical and legal principles, standards, and regulations which includes undertaking activities in compliance with the following ethical principles:

- GREENGAGE does not collect personal data for the purpose of selling it or using it for any other purpose other than intended.
- GREENGAGE collects only relevant data, and any additional personal data obtained, but not intentionally collected, during the course of the pilots will be immediately erased. Personal data is anonymised or pseudonymised where needed.
- Personal data is dealt by data controllers in GREENGAGE. GREENGAGE does not allow sharing of personal data with other controllers/processors or third parties.
- Where natural persons are recruited as participants to the activities of the projects (such as surveys), COs, appropriate measures are taken to ensure their privacy is respected and their information remains confidential. Furthermore, to ensure that no discrimination takes place in the context of the project, participants with diverse backgrounds participated in COs activities.
- Personal data will not be shared or disclosed in publications or other dissemination activities. Results will be presented in aggregated form.

In addition, GREENGAGE has introduced and applied a comprehensive ethical framework monitored by the GREENGAGE Ethics Board and is covered in D1.9 and D1.10 Ethics Management and Activities 1 & 2.

10 GREENGAGE app publication on Google and Apple Stores

Additional scrutiny was applied by Google and Apple, when the GREENGAGE app was submitted for publication on Google's and Apple's stores. The GREENGAGE privacy policies, personal data collection procedures and app features were thoroughly vetted by Google and Apple before publishing the app through their stores. For the publication on the app store, it was important to disclose/state the GREENGAGE privacy policy on (i) sharing of collected data with the third party for advertising purposes (ii) any data collected by app linked to the third-party data (iii) users should be able to delete their account.

As per GREENGAGE privacy policy (<https://www.greengage-project.eu/privacy-policy-greengage-app/>), data collected by the GREENGAGE app is neither shared with any third party nor linked to any third party. Further, deletion of both user account and data is possible in GREENGAGE. Users can request for account/data deletion by sending the request to privacy@greengage-project.eu. However, it is not possible to delete data once the data is aggregated and anonymised.

GREENGAGE Sign-up process collects information about users. The GREENGAGE app collects name and e-mail address. In the latter case the username is not collected but users need to authenticate themselves.

11 Lessons Learned and Recommendations

The privacy impact assessment was not a straightforward task. At the start of the project a lot of time and effort was spent to ensure that there is a proper understanding about the ethics as well as privacy implications among the project partners. Thus, several meetings and trainings were organised. It was also important to ensure that data flows were clear to everyone so if there were any privacy elements, for example any personal information was moving from one partner to another then its implications could be understood. Several meetings were organised, and a Miro board was used to share the ideas on the data flow. Several meetings were also required to establish full understanding about the datasets, also making sure that someone in the project is aware of the ethical implications, especially with regards to GDPR compliance to fully adopt all these practices.

In addition to above challenges, when we had to publish the REENGAGE app on Google's and Apple's stores, the project was required to fulfil vendors' requirements such as a possibility to use Google ID was needed for users if the app offered and Apple ID login (and vice versa).

Based on the experience from the project, following are some recommendations.

Early identification of controllers/processors

It is important to identify early in the project who will be controllers, joint-controllers, and processors. This is specifically important when many partners are involved and are managing a citizen science project facilitating participation of citizens. Early identification of roles and responsibilities and agreement among partners is essential for effective management of personal data and for smooth communication among partners and with citizens.

Early Agreement between Partners

Early agreement among partners on managing and handling of personal data. This is specifically important for a project like REENGAGE where many partners are involved and has multiple controllers/joint controllers' roles.

There were different products from different vendors which added to the complexity of data structures which require transformation/harmonisation before these can be used by other tools. Furthermore, this also added challenges regarding privacy protection policies because each partner has their own data protection policies and protocols in place. Therefore, early discussion is needed to have consensus.

Agreeing on project-wide data privacy protocols

It is important to define and agree on project-wide data privacy protocols at the start of the project to have consistency in the project and to identify and address any data privacy-related issues earlier in the project. In addition to this, data privacy protocols must be established/defined for individual partners as well (as in case of REENGAGE project) where data management is complex in nature and requires data management at partner as well as at project level.

Continuous Monitoring

In a Citizen Science project where citizens are largely involved, continuous monitoring and logging of access activities is needed to maintain accountability. For example, pilot support teams (PSTs) could be setup for a project. Regular meetings of pilot support teams can help to track what is happening in a project and they can ensure that privacy policies are being followed.

Data Register

It is a good practice to develop a live data register to track all data collected, process, stored and shared within a project. The data register can include various fields which are essential to determine data lineage, security and privacy. For example, REENGAGE has a live data register that provides a catalogue of all datasets collected within REENGAGE project, containing the information on who has access to those datasets, where are these datasets stored, are they encrypted and/or protected, etc.

Reporting of Data Breaches

A set defined procedure must be established early on for managing any data breaches. Furthermore, early identification of possible breaches and methods to manage them is important for smooth handling of any unforeseen situations. In REENGAGE the Ethics Board advises partners if any data breaches occur.

Pseudonymisation and Anonymisation Techniques

For safeguarding privacy, pseudonymisation and anonymisation techniques must be employed for a project and how these techniques are applied in a project must be documented and communicated at a project-level.

Ethical Standards

Personal data collection and processing must comply with ethical standards defined in a project.

References

All references are in the footnotes.

AWAITING VALIDATION BY THE EUROPEAN COMMISSION

Appendix

Privacy Impact Assessment Questionnaire

A Data Protection Impact Assessment (DPIA) is a legal obligation ([GDPR.EU](https://gdpr.eu)) and request from organisations or projects to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

Please note that Processing in the questionnaire implies Processing of Personal Data.

General Information

1. Partner Name:
2. Tool Name*:

* If there are more than one tools/technologies and their data management/privacy related answers are different then please mention clearly for which tool your answer belongs to.

A. Data Collection (This section gathers the information regarding collection and processing of personal data)

- i. What types of personal data are collected? And what is the source of personal data?
- ii. What is the specific purpose of collecting personal data?
- iii. How does these personal attributes contribute to achieve the research objectives?
- iv. Is the collection of personal data minimized to what is necessary for the research purpose?
- v. How is informed consent obtained from participants for data collection?
- vi. How is awareness raised among participants about their data protection rights and the research's data handling procedures?
- vii. Are researchers and staff involved in data collection adequately trained on data protection principles and practices?
- viii. What types of processing identified as likely high risk?
- ix. Does the data include special category or criminal offence data?
- x. What is the frequency of personal data collection?
- xi. How much of personal data will be collected?
- xii. Would individuals be affected by the collection or processing of data?
- xiii. What geographical area does it cover?

B. Context of Processing

Describe the context of the processing:

- i. What is the nature of your relationship with the individuals? How much control will they have? Do they include children or other vulnerable groups?
- ii. Would they expect you to use their data and how? Are there prior concerns over data processing or security flaws? Is it novel in any way?
- iii. Are participants provided with clear and comprehensive privacy notices detailing how their data will be used?
- iv. What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

C. Purpose of Processing (these set of question explores the need of processing personal data)

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

D. Managing Personal Data

- i) How and where will the personal data be stored? What security mechanisms are in place to protect the confidentiality and integrity of the data?
- ii) How will you ensure data quality and data minimisation?
- i) What access controls are implemented to restrict unauthorized access to the data? How are requests for data access, rectification, or erasure handled?
- ii) How long the data will be retained?

E. Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular:

- iii) What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome?
- iv) How will you prevent function creep (occurs when information is used for a purpose that is not the original specified purpose)?
- v) What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply?
- vi) How do you safeguard any international transfers?

F. Data Breach (This section captures details on possible data breach and if it happens what measures will be in place)

- i) What is the impact of data breach for each dataset?
- ii) How will you declare data breach?
- iii) What is the time to report a data breach?
- iv) How will you handle a data breach?
- v) How will you deal with situations when data breach cannot be handled?

G. GREEN ENGINE or Pilot specific Thematic Exploration Related QUESTIONS

1. Will there be any personal data involved in the data workflow (from collection, processing, storage to sharing)?
2. In case of tool's integration with other tools, who will manage and store your data?
3. What are privacy implications and how will you address those and who will be responsible for assessing this?
4. In case of using central server, which part of the data will be stored at your local server and which part of the data will be stored on central server?
5. What data will be stored by technology partners and what will be managed on central server?
6. Who will be responsible for managing data on central server and what are the associated privacy concerns? Who will ensure DPIA in this scenario?

H. Identify Risks and Measures for Mitigation of Risks

Risk ID	Description	Pre-Mitigation			Consequences	Mitigation	Post-Mitigation		
		Likelihood of harm (Remote, possible or probable)	Severity of harm (Minimal, significant or severe)	Overall Risk (Low, medium or high)			Effect on risk (Eliminated reduced accepted)	Residual risk (Low medium high)	Were Measure approved? (Yes/No)
Technical Risks (such as: insufficient data, cost of collecting data, data and codes loss, users have no technical background etc)									
1.									
2.									
3.									
Impact on Individuals (such as identification of individuals from their data or by combination of data etc)									

Personal Data Management Risks (such as in storage, transfer of data)									
Data Breach Risks									
Tool's integration Risks (such as storage, personal data management etc)									
Other Risks (associated compliance and corporate risks)									

GREENGAGE Pilot specific data management Questions:

1. What data will be passed on to other tool for further processing?

Answer:

2. How pilot specific raw and processed data from multiple tools will be shared and managed?

Answer:

3. What measures are taken to ensure security and privacy are maintained when the data is shared between different GREENGAGE tools?

Answer: