



Deliverable 6.2: Data Management Plan and Open Science

Eghbali, A. & Fisher, E.

31 July 2024

Project title: Research Ethics and Integrity for the GREEN transition

Project acronym: RE4GREEN

Grant Agreement no.: 101131706

Lead contractor for this deliverable: Trilateral IE



This document is shared under a CC BY 4.0 license.



Deliverable **factsheet:**

Action:	101131706, Data Management Plan and Open Science
Lead author(s):	Eghbali, Alaleh & Fisher, Evan
Dissemination level:	PU - Public
Document type	Report
Work Package:	6
Due date according to contract:	31 July 2024
Contributor(s):	TRI IE, all
Reviewer(s):	Anais Resseguier (TRI IE), Julie Vinders (TRI IE), Carly Seedall (UBO), Teodora Konach (EARMA), Nakajima Takahiro (UTokyo)
Keywords:	Data Management Plan, GDPR, FAIR guidelines, Open Science

Consortium:

	Role	Name	Short Name	Country
1.	Coordinator	University of Bonn	UBO	Germany
2.	Partner	European Network of Research Ethics Committees	EUREC	Germany
3.	Partner	Trilateral Research	TRI IE	Ireland
4.	Partner	University of Twente	UT	The Netherlands
5.	Partner	Austrian Institute of Technology, GmbH	AIT	Austria
6.	Partner	Aarhus University	AU	Denmark
7.	Partner	National Technical University of Athens	NTUA	Greece
8.	Partner	European Association of Research Managers & Administrators	EARMA	European network
9.	Partner	European Citizen Science Association	ECSA	European network
10.	Partner	Korean University	KU	Korea
11.	Partner	Universitat Autònoma de Barcelona	UAB	Spain
12.	Partner	University of Cape Town	UCT	South Africa
13.	Partner	Amsterdam UMC	VUMC	Netherlands
14.	Partner	Women Engage for a Common Future	WECF	International Network
15.	Partner	University of Tokyo	UTokyo	Japan

Revision History

Version	Date	Revised by	Reason
1.0	29/03/2024	All project partners	Addition of data collection, storage, and processing details
1.1	25/05/2024	TRI IE	Writing and application of comments from internal review
2.0	28/05/2024	TRI IE	Final editing for submission for review
2.1	17/07/2024	TRI IE	Edit and applying recommendations from reviewers

Table of contents

Executive summary	9
Introduction	10
Background	10
Structure of the report.....	10
Overview of RE4GREEN data	11
Applicable standards, guidelines, and principles	13
Meeting the FAIR requirements	14
The FAIR Guiding Principles.....	14
Making data findable, including provisions for metadata.....	15
Making data openly accessible.....	16
Increase data re-use.....	17
Protection of personal data	18
Data transfer to non-EU countries.....	19
Data security	20
Open Science	21
ICT tools and GDPR compliance	22
Ethics and integrity aspects	23
Roles and responsibilities	24
Conclusion	25
References	26
Appendix I.....	27
Appendix II.....	34
WP1: Analyse, Identify, Assess.....	34
WP2: Engage, Learn from, and Co-create through Social Labs.....	37

WP3: Produce and/or adapt Guidelines and Develop Policy Recommendations.....	43
WP4: Develop and Implement Training Programmes.....	47
WP5: Make Impact and Ensure Sustainability.....	50
WP6: Coordination and Management.....	53
Appendix III.....	58
Appendix IV.....	63
Appendix V.....	69

Tables and Figures

Figure 1: The FAIR Guiding Principles (EC 2016)

Table 2: Glossary of terms

Table 3: Overview of RE4GREEN data

Table 4: Personal data

Table 5: Data security

Table 6: ICT tools and GDPR compliance

List of abbreviations

CA	Consortium agreement
DMP	Data management plan
FAIR	Findable, Accessible, Interoperable, Re-usable
GA	Grant agreement
GDPR	General Data Protection Regulation
ICT	Information communication technology
LIA	Legitimate Interest Assessment
OSF	Open science framework
T	Task
WP	Work Package

Glossary of terms

Term	Explanation
Data collection	The process of gathering information or data.
Data management plan	A plan that includes information on the handling of research data during and after the end of the project, what data will be collected, processed and/or generated, which methodology and standards will be applied, whether data will be shared or made open access, and how data will be curated and preserved, including after the end of the project (EC, 2016).
FAIR	Ensuring that data are "findable, accessible, interoperable and reusable" (EC, 2016). The European Commission recommends that Horizon Europe beneficiaries make their research data FAIR.
Metadata	Data that describe other data.
Research data	"Information, in particular facts or numbers, collected to be examined and considered as a basis for reasoning, discussion, or calculation." (EC, n.d.).
Personal data	"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (GDPR, 2016, Art. 4(1)).

Table 2: Glossary of terms

Executive summary

This deliverable presents the data management plan (DMP) for the RE4GREEN project. It details the RE4GREEN consortium's plan to manage the production, collection, and processing of its data and scientific publications, during and after the project. It is a living document that will be updated during the project and reviewed by the consortium at a minimum following the periodic evaluations of the project. Each project partner handling and bearing responsibility for data collected, stored, or used in RE4GREEN will ensure compliance with the strategy outlined herein. This document follows EU guidelines for data management.



Introduction

Background

The project's Data Management Plan (DMP) (T6.2) contains information on the handling of research data during and after the end of the project. It indicates what data will be collected, processed, and/or generated; which methodology and standards will be applied; what – if any – data will be shared or made open access; and how data will be curated and preserved (including after the project's end). The plan will be updated throughout the project lifetime if significant changes arise (e.g., new data or changes in policies or in the consortium). As a minimum, the DMP will be updated around the time of the project's interim review (M18). The consortium will be guided by the FAIR (findable, accessible, interoperable, and reusable) Guiding Principles for scientific data management. To facilitate data exchange and re-use, partners will use common, standardised file formats in a consistent manner.

Structure of the report

This report follows the structure recommended in the European Commission's Horizon 2020, FAIR DMP Guidelines of 26 July 2016 (EC, 2016).

Section 2 (overview of RE4GREEN data) presents an overview of research and personal data that will be collected, processed, and generated in the project. These include data such as contact lists, literature, data from empirical studies, communication materials, and scientific publications.

Section 3 (applicable standards, guidelines, and principles) covers the applicable standards, guidelines, and principles that RE4GREEN will follow in the management of its data collection, use, sharing, and preservation.

Section 4 (meeting FAIR requirements) explains how RE4GREEN will meet the FAIR requirements, as laid out by the FAIR Guiding Principles for scientific data management. **Section 5 (protection of personal data)** covers data security – measures RE4GREEN partners take to ensure safe and secure data storage and support good security practices. **Section 6 (data security)** discusses the protection of personal data which is collected and processed in the context of the project. **Section 7 (open science)** addresses the open science commitment of project partners. **Section 8 (ICT tools and GDPR compliance)** indicates the various information communication tools that will be used in the project and their related policies for GDPR compliance. **Section 9 (ethical aspects)** covers ethical aspects. **Section 10 (roles and responsibilities)** outlines roles and responsibilities of partners, and **Section 11 (conclusion)** concludes the report. The Legitimate Interest Assessment (LIA), full tables on overview of the data, protection of personal data, data security, and ICT tools are provided in Annexes.

Overview of RE4GREEN data

This section presents RE4GREEN data per work package (WP) and task (T), detailing the type of data collected or processed in each task and corresponding WP as well as a description of the data lifecycle and proposed handling. Each task ensures that data are processed securely, stored appropriately, and disseminated internally and publicly as required, balancing project needs and regulatory compliance. The full tables detailing each WP, Task leads and contributors, types of data, life cycle, and handling are provided in **Annex II**.

WP1, led by UT, involves identifying key concepts in environmental and climate ethics. In T1.1, internal documents and academic literature reviews produced during the lengths of the project will be stored securely on a project-managed cloud drive. The data, including codebooks and metadata, are processed and updated as needed, with final outputs being published and made publicly accessible. Task 1.2, led by UBO, focuses on analysing research ethics and integrity challenges related to Green Transition technologies. It handles scientific information and draft manuscripts that are securely stored and updated until finalised, with publications shared internally and publicly. Task 1.3, managed by VUMC, identifies gaps in training materials, collecting and analysing qualitative and quantitative data, stored securely and shared internally, with some outputs published on Zenodo. Task 1.4, led by TRI IE, reviews existing ethics frameworks and guidelines, performing gap analysis to inform deliverable D1.3, with data handled similarly through secure storage and internal dissemination, and some results published on Zenodo. Each task ensures data is carefully processed, stored securely, and disseminated appropriately, balancing internal use and public accessibility.

In WP2 of the research project, led by AIT, various tasks are centred on engaging, learning, and co-creating through Social Labs. Task 2.1, led by AIT, focuses on designing a common methodology for the Social Labs, producing internal notes and a Social Lab methodology document stored securely on a project-managed cloud drive, with dissemination to consortium partners and publication on Zenodo. Task 2.2 involves recruiting and interviewing participants, handling stakeholders' contact details and interview recordings, and ensuring secure storage and pseudonymisation of data, with dissemination limited to internal partners and aggregate reporting to the EC. Task 2.3, which facilitates dialogue on ethics and integrity issues, manages participant contact details and meeting results stored securely, with pseudonymised summaries shared internally and a Social Lab implementation report published publicly. Task 2.4 elaborates and validates strategies, analysing both online and in-person Social Lab meetings, with secure data storage and pseudonymising dissemination of findings, culminating in a public implementation report. Lastly, Task 2.5 packages Social Lab learnings for training support, securely managing internal notes and draft manuscripts, with final outputs published on Zenodo and the project website. Each task ensures that data are securely handled, processed, and disseminated according to rigorous protocols.

WP3, led by TRI IE, focuses on producing or adapting guidelines and developing policy recommendations, managing various types of data with strict protocols. Task 3.1, led by AIT, incorporates the "do no significant harm" principle, handling internal notes and stakeholder contact details, storing data securely on a cloud drive, and pseudonymising interview transcriptions for internal use, with public dissemination of the guidance report on

Zenodo and the project website. Task 3.2, led by TRI IE, produces operational ethics and integrity guidelines, based on findings from WP1 and WP2, securely storing documents, and disseminating guidelines both internally and publicly. Task 3.3, led by UBO, develops recommendations on environmental risk assessments, compiling normative assessment materials and ethical practices feedback, stored securely and shared internally, with recommendations publicly available upon completion. Task 3.4, led by TRI IE, develops policy recommendations on R&I governance, managing stakeholder contact details and consultation recordings, securely storing data, and publicly disseminating policy briefs on Zenodo and the project website.

WP4 which is led by VUMC, focuses on developing and implementing training programs. Task 4.1, led by VUMC, involves creating training materials, including internal notes and a corpus of training materials, securely stored on a project-managed cloud drive. The Delphi study survey responses are also managed securely, with anonymised data only mentioned in publications with participants' explicit consent. The final micromodules, stored securely, will be disseminated to partners and made publicly available on platforms like Zenodo and the Embassy of Good Science. Task 4.2, also led by VUMC, pilots and refines training pathways, managing participants' personal data with strict consent and secure storage protocols, with final training programs being disseminated internally and publicly. Task 4.3 focuses on the implementation and dissemination of these training programs, storing tools and materials securely and ensuring final programs are accessible on platforms such as the Embassy of Good Science.

WP5, led by NTUA, focuses on enhancing impact and ensuring sustainability of the project. Task 5.1, led by NTUA, augments the plan for dissemination, communication, and exploitation, handling internal notes and RE4GREEN press kits, all securely stored and disseminated through RE4GREEN channels, with the project's branding made publicly available on Zenodo and the project website. Task 5.2, also led by NTUA and with contributions from UBO, develops the project website and social media presence, continuously updating online content and disseminating it through all project channels. Task 5.3 implements the dissemination and communication plan, monitoring partners' activities and maintaining a secure list of newsletter subscribers, ensuring GDPR compliance. Task 5.4 focuses on the exploitation, uptake, and sustainability activities, monitoring dissemination efforts and storing data securely, with regular updates and reporting to the EC.

WP6, led by UBO, focuses on coordination and management of the project. Task 6.1, led by UBO with contributions from all partners, involves project coordination and administrative and financial management. This task stores documents securely on the project's cloud-based drive and GDPR-compliant servers, shared internally. Task 6.2, led by TRI IE, addresses the compilation of the DMP and promotion of open science, storing documents securely and updating them as necessary, with public dissemination of the data management plan on Zenodo and the project website. Task 6.3, led by WECF, focuses on capacity building on gender expertise, handling training materials and recommendations, with public dissemination of training methodology and checklists on Zenodo and the project website. Task 6.4, led by EUREC, manages stakeholder and advisory board interactions, securely storing their contact details, meeting transcriptions, and a stakeholder database, with anonymised data shared internally.

Applicable standards, guidelines, and principles

The RE4GREEN project follows the regulations, standards, guidelines and principles listed below in the management of its data collection, use, sharing and preservation:

- European Parliament and the Council, Regulation (EU) 2016/679 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, repealing Directive 95/46/EC (**General Data Protection Regulation or GDPR**). This defines key terms, including personal data and pseudonymisation, and sets legal obligations for data controllers. See the section on Protection of Personal Data and Annex III for detailed information about the protection of personal data in RE4GREEN;
- European Commission Directorate-General for Research & Innovation, H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, Version 3.0, 26 July 2016;
- European Commission, H2020 Programme Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020, Version 3.2, 21 March 2017;
- Any national data protection regulation applicable for any of the partners and tasks.
- Research integrity standards, especially the ALLEA European Code of Conduct for Research Integrity.

In addition to the laws and standard listed above, RE4GREEN will consider and respect the wider understanding of privacy, such as those contained within the European Convention on Human Rights (Article 8), the EU Charter of Fundamental Rights (Articles 7 & 8) and related case law, and their relation to the security of information technology systems, as outlined within the ISO standard ISO/IEC 29134:2017.

Where national law differs from EU law and sets a higher standard, legislation from the countries where the use cases are based (Spain, Greece, and Germany) will be followed.

Meeting the FAIR requirements

As noted in the Guidelines for Horizon 2020, to which reference is made in the absence of updated guidelines for data management in Horizon Europe projects, data that are made findable, accessible, interoperable, and reusable (FAIR) can be managed more effectively, and this can foster better science through enabling others to reproduce results and re-use data for future research. In accordance with this guidance, this section outlines how RE4GREEN fulfils the FAIR principles.

The FAIR Guiding Principles

The European Commission recommends that Horizon 2020 beneficiaries "make their research data findable, accessible, interoperable and reusable (FAIR), to ensure it is soundly managed" (EC 2016). Based on this guidance, this section outlines how RE4GREEN operationalises this. The figure below illustrates the FAIR Guiding Principles:



Figure 1: The FAIR Guiding Principles (EC 2016)

Data produced and stored in the context of RE4GREEN will be made FAIR (findable, accessible, interoperable and reusable) by following the Data Management Plan (DMP). The RE4GREEN DMP supports long-term data storage, describes curation strategies where needed, and indicates the metadata used. The impact of RE4GREEN will be maximised by supporting open access for all produced publications. The RE4GREEN consortium is committed to the EU's efforts to improve access to research results and to highlight the positive impacts of public investment

in research under the Horizon Europe framework programme. The RE4GREEN consortium will use its members' experience to publish important results and outputs in high-impact, peer-reviewed open access scientific journals.

Making data findable, including provisions for metadata

1. Making data findable internally

Internal project documents and administrative data are stored in a centralised, password-protected online repository – SharePoint – owned by EUREC and co-managed by UBO that is accessible to all the partners working on the project. EUREC Office is the repository owner and will provide partners with access to the folder and editing rights.

To make data findable and reusable, the following measures are in place:

- **Location:** All documents are stored in relevant folders, organised by WP, in a variety of formats (e.g., Word documents, PDFs, Excel spreadsheets, PowerPoints, or other standard data formats). Partners are responsible for storing documents related to their work on the project in the correct location.
- **Naming of files:** The file names include a short descriptive title of the document and the date of creation or revision, to make them uniquely identifiable and distinguishable (e.g., "D1.2 DMP V01 April 2024").
- **Reports and documents:** All RE4GREEN reports and documents contain information on authors and contributors, clear version numbering, dates, and keywords.

UBO is responsible for curating the internal project data after the end of the project and when the project SharePoint is taken down.

2. Making data findable externally

The following provisions will ensure that RE4GREEN outputs are findable externally:

- All public deliverables (in some cases redacted versions) and outputs are published on the RE4GREEN website and on the open access repository Zenodo as soon as submitted with the watermark "pending EC approval" (unless they are under embargo for publication) and the Embassy of Good Science.
- Zenodo issues a digital object identifier (DOI) to each RE4GREEN upload to ensure effective and consistent citation.
- The project coordinator will advise all partners of the availability of data and changes to data and their location to facilitate access and wider sharing (as deemed fit).

Making data openly accessible

1. Open access to scientific publications

Per annex 5 of the RE4GREEN Grant Agreement (GA), each RE4GREEN beneficiary will ensure open access (free of charge online access for any user) via green or gold open access routes to all peer-reviewed scientific publications relating to its results. Two special issues with contributions from the consortium and a minimum of five peer-reviewed scientific publications are planned. RE4GREEN has a dedicated budget for this purpose. As per the GA, beneficiaries shall

- Deposit, as soon as possible and at the latest upon publication, a machine-readable electronic copy of the published version or final peer-reviewed manuscript accepted for publication in the Zenodo repository; the beneficiary also aims to deposit at the same time the research data needed to validate the results presented in the deposited scientific publications.
- Ensure open access to the deposited publication — via the Zenodo repository — at the latest:
 - (i) on publication, if an electronic version is available for free via the publisher, or ^[1]_[SEP]
 - (ii) within six months of publication (twelve months for publications in the social sciences and humanities) in any other case. ^[1]_[SEP]
- Ensure open access — via the repository — to the bibliographic metadata that identify the deposited publication. The bibliographic metadata is in a standard format and includes all of the following: (1) the terms "European Union (EU)" and "Horizon Europe", (2) the name of the action, acronym and grant number, (3) the publication date, (4) length of embargo period if applicable, and (5) a persistent identifier.

2. Open access to research data

In accordance with Annex 5 of the RE4GREEN GA pertaining to dissemination of results, the project will ensure open access to research data via a trusted repository, Zenodo. These data are to be deposited under the latest available version of the Creative Commons Attribution International Public Licence (CC BY) or Creative Commons Public Domain Dedication (CC 0) or a licence with equivalent rights.

However, in line with the guiding principle of "as open as possible as closed as necessary", research data will not be made open access if one of the following factors are applicable:

- (i) It would be against the beneficiary's legitimate interests, including regarding commercial exploitation; or
- (ii) It would be contrary to any other constraints, in particular the EU competitive interests or the beneficiary's obligations under the GA.

Before sharing any data, either with the consortium or externally, the partners will ensure that no disclosive information is included.

Public deliverables and outputs (redacted, if needed) are published on the RE4GREEN website as soon as submitted to the EC (with watermark "pending EC approval") and without watermark once approved by the EC.

Making data interoperable

RE4GREEN partners exchange information using, as appropriate, a variety of means, e.g., e-mail and SharePoint. To allow for data exchange and re-use between researchers, institutions, organisations, and countries, RE4GREEN ensures data interoperability through the consistent use of common, standardised file formats. The consortium uses file formats that, even when originating in or primarily used with proprietary software and/or code, are accessible with open-source software. When available and not otherwise in conflict with data security, protection, or processing measures and requirements, the consortium uses open-source software applications.

Through its use of common, standardised file formats and software, RE4GREEN seeks to facilitate any legitimate and lawful data re-combinations with different datasets from different origins.

Increase data re-use

1. Re-use of existing data

Some of RE4GREEN's work will, where appropriate and needed, re-use (aggregate, synthesise, or analyse) materials (e.g., figures, tables, quotations) from existing literature (academic, policy, or other documents). In such cases, they will be properly referenced and acknowledged; in addition, any necessary permissions for re-use will be obtained. RE4GREEN partners will use literature (both academic, grey literature, and press articles) relevant to the tasks.

2. Increasing re-use of RE4GREEN results

The deliverables classified as public will be made publicly accessible via the project website, Zenodo, and the Embassy of Good Science. A creative commons licence CC-BY (requiring attribution) or CC-0 (no rights reserved) will be used for all project deliverables to ensure that they are shared with minimal restrictions, aside from attribution to the authors or creators.

Protection of personal data

This section covers the collection and processing of personal data during the project for each project partner. The personal data collected and processed falls into three broad categories:

- Name, personal contact information, and demographic data (e.g., email address, age, gender);
- Audio or video recordings of participants to qualitatively evaluate training materials;
- Responses of participants to quantitatively evaluate training materials.

The project will collect and process personal data only as necessary to carry out project activities, in compliance with the GDPR. This will include primary quantitative and qualitative data about relevant areas of R&I and relevant technologies, environmental and ethical issues and considerations, and impacts (such as those gathered through engagement in the social labs and with the Stakeholder Advisory Board); data collected and analysed from secondary literature, grey literature, and other European projects' outputs; data generated by the project, including project outputs such as reports, methodologies, training materials, guidelines, policy recommendations, and communication materials.

This section presents the technical and organisational measures for data security at each project partner's organisation. The section shows that, at a minimum, all project partners store data on secure servers which are in line with GDPR provisions. Data are stored in password-protected folders, and access is restricted to members of the project partners.

All data collected will be relevant and limited to the purposes of the research project (in accordance with the data minimisation principle) and, where possible, pseudonymised. Where data cannot be pseudonymised (as may be the case in some qualitative interviews), the data will be kept in a secure physical location or on an encrypted file server. If any personal data are transferred from the EU to a non-EU country or to an international organisation, all such transfers will be in accordance with Chapter V of the General Data Protection Regulation 2016/679. Likewise, if any personal data are transferred from a non-EU country to the EU (or another third state), RE4GREEN partners will ensure that such transfers will comply with the laws of the country in which the data were collected and that a data-sharing agreement will be signed if and when needed between data controllers and data processors. The research does not involve profiling. The assessment of competencies and educational needs will be related to roles of the individuals and not their personal status. For WP2, and the Social Labs, a Legitimate Interest Assessment (LIA) was performed to provide the legal basis for the processing of personal data in the RE4GREEN project for the purpose of compiling and using a contact list of stakeholders, whom will be contacted periodically by e-mail, to provide information about RE4GREEN and invite them to participate in social labs. The LIA is available in Appendix I.

Breakdown of procedures of protecting data when sharing with external partner can be found in Table 3 (personal data protection), **Annex III**.

Data transfer to non-EU countries

In cases where personal data transfer to and from non-EU countries will be needed, RE4GREEN will comply with the GDPR requirements. Non-EU countries in the RE4GREEN project include South Korea, Japan, and South Africa. Non-EU partners are required to comply with Chapter V of the GDPR on international data transfers. The consortium will sign a data-sharing agreement with UCT to ensure any transfer of personal data is compliant with the GDPR and other relevant applicable requirements in the case that data transfer becomes necessary. If non-EU partners transferring data into the EU, they need to explain why they are doing this, what data they are transferring, and explain how the data was collected lawfully in the country from which it is being transferred.

Data security

This partners have outline their technical and organisational measures for data security at organisational level. At a minimum, all project partners store data on secure servers in line with GDPR provisions. Data are password-protected, and access to the data is restricted to project partner members.

A breakdown of all these measures for each partner can be found in Table 4 (data security), **Annex IV**.

Open Science

The consortium is well-versed and experienced in delivering on open science practices and will implement a strong open science approach which will be developed and monitored through the Data Management Task, T6.2. Open science lies at the heart of RE4GREEN bottom-up approach through the social labs that will ensure the inclusion throughout the project duration of a wide range of stakeholders, including research ethics and integrity experts, researchers, research managers, relevant policy-makers, industry actors, citizen scientists, civil society organisations. This inclusive and participatory approach will be further strengthened by a Stakeholder Advisory Board (SAB) that represents a diversity of perspectives and the ethics bodies represented by EUREC, ENRIO, ENERI as well as the research ethics committee members part of the consortium and the SAB.

The consortium intends to give the project's results and deliverables the widest possible reach via the project website, emails, social media, publications, etc. An appropriate creative commons licence CC-BY (requiring attribution) or CC0 (no rights reserved) licence will be used for the project's outputs to ensure that they are shared with minimal restrictions (unless otherwise agreed/justified), aside from attribution to the authors or creators. Open access will be provided to project publications featured in peer-reviewed journals through publication via the 'gold' or 'green' route. The decision will be based on the publisher selected, the scope of the article (results it shares) and the partners who have contributed to the publication. The consortium has allocated a budget to cover the cost of gold open access publishing. For the green route, the consortium members have agreed that the material will be deposited immediately upon publication and that the article will be open access after the shortest embargo period allowed by the respective publication (publishers with short embargo periods, such as 6 months, will be preferred). Furthermore, partners will favour open review processes for publications, such as with the Open Research Europe platform (one of the consortium partners is a Collection Advisor at ORE).

Additionally, the project will be (pre-)registered via Zenodo by the coordinator (UBO) to increase transparency and strive to contribute to commit to promotion and elimination of unethical and questionable research practices. The Zenodo repository will be used as a default for project's results, unless a more specific repository is assessed by the consortium as being better suited for the material and/or is more consistent with the partner's institutional norms and requirements.

ICT tools and GDPR compliance

RE4GREEN partners will use various information communication technology tools to conduct various activities of the project. The list of identified tools how they are used, and provide information on their GDPR compliance can be found on Table 5 (ICT tools and GDPR Compliance), **Annex V**.

Ethics and integrity aspects

RE4GREEN partners comply with Article 14 of the GA which states that all activities must be carried out in compliance with ethical principles. Partners conduct research in accordance with fundamental principles of research integrity, such as those described by ALLEA in its European Code of Conduct for Research Integrity. These principles are reliability, honesty, respect, and accountability (ALLEA 2017, p. 4).

In keeping with the highest standards of research integrity, and to ensure the privacy, safety, and dignity of data subjects, RE4GREEN partners will provide participants with project information sheets and consent forms in a language and in terms fully understandable to them. These forms describe the aims, methods and implications of the research, the nature of the participation and any benefits or risks (e.g., to privacy) that might be involved. They explicitly affirm that participation is voluntary and that participants have the right to refuse to participate and to withdraw their participation, or data, at any time, without any consequences. The forms outline how partners collect and protect data during the project (e.g., use of pseudonymisation), and then destroy it or re-use it (with consent). Researchers will ensure that potential participants fully understand the information and do not feel pressured or forced to give consent.

Roles and responsibilities

This section establishes the roles and responsibilities for personal data protection in the RE4GREEN project.

TRI, as the T6.2 lead, is responsible for the preparation of the data management plan and presenting it to the consortium. TRI will ensure that this deliverable is available in the shared RE4GREEN repository for researchers to access and review. TRI is also responsible for the periodic review and update of this report, with the support of all partners.

All RE4GREEN partners will provide support and contributions regarding personal data management related to their relevant WPs and project tasks. All partners are responsible for safeguarding the rights and freedoms of data subjects and preventing unauthorised access to personal data and breaches of the principles of confidentiality and privacy. Each partner who collects and processes personal data in RE4GREEN is responsible for the following:

- Ensuring compliance with the standards and practices outlined in the project DMP (D6.2);
- Ensuring that individuals working on RE4GREEN have read this document;
- Implementing and adhering to their own organisational and technical measures;
- Informing TRI of any changes to their personal data collection or processing procedures, including changes in plans for the types of personal data to collect;
- Flagging any concerns about personal data protection as soon as possible so that the issues can be appropriately addressed; and
- Supporting TRI with the periodic updates of this report in a timely manner.

RE4GREEN partners will be regularly reminded of the personal data protection measures in place, including during project meetings. All researchers should have the opportunity to raise questions to gain further information, should it be required. Personal data protection will also form a standing item on the agenda of regular project meetings.

Conclusion

This deliverable presented the RE4GREEN consortium's plan to manage the production, collection and processing of its research data, results and scientific publications. It will be updated and reviewed by the consortium during the course of the project and updated in advance of the project's interim review and final review meeting. Updates will be made to consider new data, changes in consortium policies, and changes in consortium composition and external factors (e.g., new consortium members joining or old members leaving). Each project partner handling and responsible for data collected, stored, or used in RE4GREEN is responsible for ensuring compliance with the strategy outlined in this document.

References

- ALLEA (All European Academies) 2017, 'European Code of Conduct for Research Integrity, Revised Edition', May. <http://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf>
- European Commission Directorate-General for Research & Innovation (EC) n. d., 'Open access and Data Management'. https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm
- European Commission Directorate-General for Research & Innovation (EC) 2018a, 'Ethics and data protection', 14 November. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
- European Commission Directorate-General for Research & Innovation (EC) 2018b, 'Ethics in Social Science and Humanities', October. https://ec.europa.eu/info/sites/default/files/6_h2020_ethics-soc-science-humanities_en.pdf
- European Commission Directorate-General for Research & Innovation (EC) 2017, 'H2020 Programme Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020', Version 3.2, 21 March. http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf
- European Commission Directorate-General for Research & Innovation, 2016, 'H2020 Programme Guidelines on FAIR Data Management in Horizon 2020', Version 3.0, 26 July. http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf
- European Commission (EC) 2022, 'Horizon Europe Programme Guide', Version 2.0, 11 April. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf
- European Parliament and the Council of the European Union, 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), OJ L, 4 May 2016, pp. 1-88.

Appendix I

Legitimate Interest Assessment (LIA)

Legitimate Interest Assessment (LIA) for the creation and use of contact lists for stakeholder database

Prepared 22/03/2024

Introduction

This document provides the legal basis for the processing of personal data in the RE4GREEN project for the purpose of compiling and using a contact list of stakeholders, whom we will contact periodically by means of an e-mail, in order to provide them with information about RE4GREEN and invite them to participate in social labs.

The RE4GREEN contact list contains the names, titles, organisations and e-mail addresses of stakeholders whom we believe might be interested in being involved in the social labs or who have asked to be added to our contact list.

Article 6 of the General Data Protection Regulation (GDPR) provides for several possible legal bases for the processing of personal data. In the following sections, we discuss how and when they – informed consent and legitimate interest – might apply to the outlined data processing operations.

Processing under Art. 6(1)(f) of the GDPR

Art. 6(1)(f) provides that processing of personal data is lawful where “processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

Data processing in the RE4GREEN project includes collecting contact details as well as sending information to contacts. These activities are necessary for the project to complete its purpose and deliverables and to ensure that relevant stakeholders are recruited for the social labs to provide insight on ethical issues in I&R and green transition. Hence, identifying and recruiting the relevant stakeholders has a larger social purpose than simply benefiting the consortium partners (“the beneficiaries” in the EC’s terminology).

Our legitimate interest in conducting such communications is enshrined in the RE4GREEN Grant Agreement, Article 15.2 of which states that processing of personal data is done “lawfully, fairly, and in a transparent manner” and also that data is “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”. Furthermore, Article 17 of the Grant Agreement clearly indicates that the RE4GREEN consortium is obliged to disseminate its results to multiple audiences, which implies the need to compile a contact list targeted at multiple audiences in a strategic and effective manner, i.e., not just a random list of people who visit the project’s website and ask to be put on the contact list. It has to be a *targeted* and

strategic contact list. Hence, we consider that the GA serves as a valuable justification for the RE4GREEN consortium to process personal data for this purpose, to inform stakeholders and process data for recruitment in the social labs as part of its commitment to deliver WP2 deliverables.

Following Art.6(1)(f) GDPR, after a legitimate interest has been identified, a balancing exercise must be conducted between the interest in question and the interests of the data subjects concerned, in order to ascertain whether the latter are not overriding the former. For this balancing exercise, Tri IE consulted the website of the Information Commissioner's Office (ICO), the UK data protection authority, which offers detailed guidance on how to conduct such a balancing exercise and on which the following is adapted.

The ICO says that there are three elements to the legitimate interest basis. We must:

1. *identify a legitimate interest* – As stated above, we have a legitimate interest, under Article 17, to process personal contact details, as mentioned above, in order to create impact for our EU-funded project.
2. *show that the processing is necessary to achieve it* – 'Necessary' means that the processing must be a targeted and proportionate way of achieving our purpose. We must collect the contact details for stakeholders across the EU in order to inform them about how our project results could help promote demand response. The processing is necessary as we could not reasonably achieve the same result in another way; we have chosen the least invasive and socially accepted method of communication.
3. *balance it against the individual's interests, rights and freedoms* – see below, where we have done a balancing test, and are confident that the consortium's legitimate interests do not override the individual's interests or fundamental rights.

As noted below, our processing of personal data will not cause harm any more than any other e-mail to our stakeholders. We are not using people's data in ways they would find intrusive or which could cause them harm. We will always offer stakeholders an option to unsubscribe from our contact list.

As we wish to rely on legitimate interests as the basis for processing data on our contact list, we have conducted this legitimate interest assessment (LIA) before we start the processing. According to the ICO, an LIA is a type of light-touch risk assessment based on the specific context and circumstances. It helps ensure that processing is lawful. Recording our LIA also helps to demonstrate compliance in line with our accountability obligations under Articles 5(2) and 24 of the GDPR.

The ICO posits the following questions as part of its LIA exercise. Opposite each question in the left-hand column, we give our response in the right-hand column.

First, identify the legitimate interest(s)

Question	Response
Why do you want to process the data – what are you trying to achieve?	We are conducting publicly funded (European Commission 101131706) research on climate and environmental ethics issues associated with R&I. The data collected are to ensure that the experts and stakeholders included in the research are strategically selected, based on publicly available information on e.g., their organization web-pages. Strategic in this case means being able to speak directly, from a position of expertise and experience, to the questions of climate and environmental ethics issues. We wish to invite these targeted stakeholders to participate in the social labs.
Who benefits from the processing? In what way?	The European Commission benefits by being assured that the research is conducted with the correct and appropriate experts and stakeholders. The benefit is of legitimate and quality results. The experts and stakeholders benefit from being included in a network of participants with shared interest in enhancing the climate and environmental ethics integrity aspects of their work. Research Ethics Committees also benefit from guidelines developed through a high-quality research process that involves the right experts and stakeholders. Additionally, the consortium partners benefit from the processing because the social labs are an integral part of the project and identifying relevant stakeholders to provide insights on ethical issues for D2.2 and D2.3 and to be used later in WP3.
Are there any wider public benefits to the processing?	To the extent that research findings are taken up by the European Commission; Research Ethics Committees; and researchers and stakeholders, and that these findings support actions to reduce climate and environmental harms from R&I, the public benefits, as the project results will be available publicly.
How important are those benefits?	These benefits are vital. Current climate and environmental impacts of research, innovation, development and industrialization are unsustainable and contributing to pollution, biodiversity loss, and climate change. The importance is also highlighted in R&I in the context of the green transition.

<p>What would the impact be if you couldn't go ahead?</p>	<p>The robustness of the research would be negatively affected and the project results run the risk of being soiled and not representative of the wider research community, if stakeholder engagement cannot be carried out. The project would thus be in a position of having to change / breach its contract with the European Commission, imposing financial and reputational harm on more than 30 researchers involved in the project. Not proceeding would also undermine the European Commissions request for services regarding reducing the climate and environmental harms of R&I. As such, RE4GREEN's contribution and impact in examining and abating climate and environmental harms of R&I will not be done effectively.</p>
<p>Would your use of the data be unethical or unlawful in any way?</p>	<p>No. Data will be only collected either through publicly available sources and/or with explicit consent from individuals -- e.g., name, email, organization sector, area of expertise, gender, geography. The data will only be used to keep track of participations in the project (as required by the Commission); invite participants to research activities, with their consent (approved by ethics committees); and share the results of the research activities back to participants. We will follow good data protection practices and follow established legal interpretations of the GDPR, together with relevant ethical guidelines</p>

Second, apply the necessity test

Question	Response
<p>Does this processing actually help to further that interest?</p>	<p>Yes. Data use for strategic recruitment of participants to the project is strategic and proportionate, to fulfil our obligations in WP2</p>
<p>Is it a reasonable way to go about it?</p>	<p>Yes. Information shared by the individual experts and stakeholders we contact will be from public sources only, and already uploaded to the Internet with their consent (e.g., as employees of their organizations; as corresponding authors of publications; as publicly listed authors in reports or on advisory boards according to Europe Commission Comitology rules). This is also the only way to enter into direct contact with them, as contacting them through email is the least intrusive method of approaching them.</p>

Is there another less intrusive way to achieve the same result?	No. This method is considered to be the least intrusive. There is no less intrusive way to achieve the same result.
---	---

Third, apply the balancing test

By applying the balancing test (based on the questions below), we consider the impact of our processing and whether it overrides the interest we have identified

Question	Response
What is the nature of your relationship with the individual?	In most cases, there will be no prior relationship to the individual and they are approached on the basis of their professional role and/or expertise. In rare cases, researchers in the RE4GREEN project will contact colleagues and peers with whom they already have a direct personal connection.
Is any of the data particularly sensitive or private?	No. All data will be from publicly available sources.
Would people expect you to use their data in this way?	Yes. As the data are from public sources (e.g., as employees of their organizations; as corresponding authors of publications; as publicly listed authors in reports or on advisory boards according to Europe Commission Comitology rules), there is an expectation of the possibility of being contacted with requests for information etc.
Are you happy to explain it to them?	Yes. We will inform our contacts about the mission of our project and how its results could support them. We will also inform them about the project's privacy policy. We will always inform contacts that they can opt-out of further communications by simply clicking on the "unsubscribe" button or performing a similar, non-burdensome action.
Are some people likely to object or find it intrusive?	No, no more than any other email from an unexpected source. Indeed, as all messages from RE4GREEN will be personalised to the expertise of the individual, contact from RE4GREEN will likely be less objectionable or intrusive.
What is the possible impact on the individual?	No more than on any other email. We expect only a positive impact, in the sense that stakeholders will become aware of our project and would be willing to offer their insight on ethics and integrity issues in environmental and climate I&R.
How big an impact might it have on them?	As above.

Are you processing children's data?	No.
Are any of the individuals vulnerable in any other way?	Not that we are aware of
Can you adopt any safeguards to minimise the impact?	We want to maximise the (positive) impact of our project. However, as noted above, we are implementing safeguards to protect our contact list – notably, our contact list file is securely stored, password-protected, and only a few individuals have access to the file.
Can you offer an opt-out?	Yes. If individuals invited to participate in the Social Labs do not wish to participate, they will not be included in the Social Labs. Only their name (no contact information) will be kept for a period of 2 years (the duration of the Social Lab) to ensure they are not contacted again. In addition, if individuals wish to cease participation in the lab at any time, they are free to do so. Their information (except name for 2 years to ensure they are not contacted again) will be removed from the database.

The decision on legitimate interest

Based on the foregoing, we conclude that whenever the ground from Art.6(1)(a) GDPR does not apply, legitimate interest (as set out in Article 6(1)(f) of the GDPR), is an appropriate basis for our processing of personal data for the discussed purposes. We are confident that our legitimate interests are not overridden by any risks to the data subject.

Safeguards

Even though we believe there are no significant risks to the data subjects of their being on our contact list and sending them relevant news, we have considered safeguards to reduce any further risks, as follows: RE4GREEN commits to keeping its contact list in a secure, password-protected file to which only a limited number of individuals will have access on a need-to-know basis.

Next steps

We understand that if we want to process the personal data for a new purpose, we may be able to continue processing under the legitimate interest provision as long as our new purpose is compatible with our original purpose. If necessary or useful, we will adhere to Art. 6(4) of the GDPR and conduct a new LIA to demonstrate compliance with the legislation.

We will keep this record of our legitimate interest assessment (LIA) on file in order to demonstrate compliance with legislation, if required. We will keep our LIA under review and repeat it if circumstances change.

Appendix II

Overview of RE4GREEN Data Table

WPI: Analyse, Identify, Assess

T1.1: 1 Identify key concepts and issues in environmental and climate ethics for R&I [Lead: UT; Contributors: TRI IE, AIT, AU, UAB, UCT, WECF, UTokyo]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none">• Developed by: task lead, with contributions from task contributors.• Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners.• Format: MSWord, Excel, PowerPoint, and PDF documents.• Processing: reviewed and updated as necessary.• Dissemination: Internal, to task partners.
Corpus of Academic literature for systematic review	<ul style="list-style-type: none">• Developed by: all task contributors.• Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners.• Format: RIS format results stored in password-protected Zotero library; PDF documents.• Processing: title, abstract, and full-text screening will take place in password-protected file on Covidence (under licence with the UT), which will be reviewed and updated as necessary.• Dissemination: Internal, to task partners.
Codebook based on relevant information from the literature	<ul style="list-style-type: none">• Developed by: all task contributors.• Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners.• Format: MSWord, Excel, PowerPoint, and PDF documents.• Processing: publication titles and abstracts will be screened based on inclusion and exclusion criteria: each abstract will be assessed by two reviewers, and any disagreements regarding inclusion and exclusion will be discussed in team meetings. This process will lead to an elaborated set or criteria that will be used for the full text screening.• Dissemination: internal, to task partners.
Metadata from reviewed literature	<ul style="list-style-type: none">• Developed by: all task contributors.• Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners.• Format: MSWord, Excel, PowerPoint, and PDF documents.• Processing: reviewed and updated as necessary.



This document is shared under a CC BY 4.0 license.

	<ul style="list-style-type: none"> • Dissemination: internal, to task partners.
D1.1 Mapping of environmental and climate ethics in the context of the sustainability transition	<ul style="list-style-type: none"> • Developed by: all task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: MSWord, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary. • Dissemination: submission to an appropriate journal for publication, and made available to the public on the RE4GREEN website and published on Zenodo and submitted to the EC.

T1.2: Analyse research ethics and integrity challenges of technologies and policies supporting the Green Transition [Lead: UBO; Contributors: UT; AIT, TRI IE, UCT, WECF]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: MSWord, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP1. • Dissemination: internal, to task partners.
Scientific information (technologies, environmental impact, innovation trends) compiled from R&I landscape analysis	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors, building on key concepts identified in T1.1 and insights collected in the Social Labs in WP2. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP1. • Dissemination: internal to consortium partners.
D1.2 Draft manuscript journal article reviewing environmental and climate ethics in the context of the	<ul style="list-style-type: none"> • Developed by: T1.1 and T1.2 contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word.

sustainability transition	<ul style="list-style-type: none"> • Processing: reviewed and updated as necessary, until the submission of D1.2. • Dissemination: submission to an appropriate journal for publication, and made available to the public on the RE4GREEN website and published on Zenodo and submitted to the EC.
---------------------------	--

T1.3: Identify gaps in existing training materials/programmes [Lead: VUMC; Contributors: ECSA; EUREC]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary, until finalisation of D1.3. • Dissemination: internal, to task partners. The protocol will be made available on Zenodo.
Corpus of training material collected for gap analysis	<ul style="list-style-type: none"> • Developed by: task lead with contribution from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Website links, text, videos and PDF documents, Excel. • Processing: quantitative (descriptive statistics) and qualitative (thematic content) data analysis. Reviewed and updated as necessary, until finalisation of D1.3. • Dissemination: internal, to task partners. Data extraction files will be made available on Zenodo.
Publicly available personal data of training course coordinators	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Excel. • Processing: publicly available names and email addresses of training course coordinators will be gathered from university websites, in accordance with GDPR legislation and will be recorded in data extraction files. This will form the basis of a contact list for potential experts who could be invited to participate in T4.1. This will be reviewed and updated as necessary.

	<ul style="list-style-type: none"> • Dissemination: internal, to task partners.
--	---

T1.4: Review existing research ethics and integrity frameworks/guidelines [Lead: TRI I&E; Contributors: EUREC]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from EUREC. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of TRI and EUREC. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary, until finalisation of D1.3. • Dissemination: internal, to task partners.
Corpus of existing ethical frameworks and guidelines for gap analysis	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from EUREC. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word, Excel, and PDF documents. • Processing: gap analysis, to inform D1.3. • Dissemination: internal, to consortium partners.
D1.3 Gap analysis of research ethics and integrity resources for R&I in general and new climate and environmental technologies in particular	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: Password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PDF documents, content analysis files (e.g., MAXQDA). • Processing: reviewed and updated as necessary, until finalisation of D1.3. • Dissemination: internal, to task partners. Content analysis files and draft manuscript will be made available on Zenodo and submitted to the EC.

WP2: Engage, Learn from, and Co-create through Social Labs

T2.1: Design common methodology for RE4GREEN social labs [Lead: AIT ; Contributors: ECSA, UBO, AU, UAB, UCT, EARMA, UTokyo]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal, to the consortium partners.
D2.1 Social Lab Methodology	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of Task partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal, to the consortium partners, and to the EC. A version will be published to Zenodo and the project website in M36.

T2.2: Recruit and interview participants [Lead: AIT; Contributors: AU, EARMA, TRI IE, UBO, ECSA, UCT, EUREC, UAB, KU, UTokyo, UT, WECF]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of Task partners. • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal, to the consortium partners.

Stakeholders' contact details and correspondence	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the protected drives of task partners (one contact table for each task partner). One common version without contact details or correspondence details will be securely stored on password-protected project cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, Excel, and PDF documents. • Processing: partners will source contacts from public webpages. Names, emails, gender, geography, expertise, and organisation type will be recorded. Emails will only be kept by partners on secured protected drives. Common public information (no emails) will be stored in a common sheet on a protected drive shared by partners. Contacts will be reviewed and updated as necessary as AIT and partners interact with stakeholders. Contact information will be kept until five years after the end of the project and then deleted. • Dissemination: internal to the consortium partners (never with contact details); for reporting to the European Commission on stakeholder participation (aggregate participation information; no contact details or names).
Audio, video and transcription of recordings of interviews	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the protected drives of task partners. Deleted upon completion of transcription. • Format: video and audio files, Word, Excel, and PDF documents. • Processing: transcription; development of anonymised interview summaries. • Dissemination: none for primary data. For processed anonymised data, internal to consortium partners.

T2.3: Dialogue and exchange on ethics and integrity issues [Lead: AIT; Contributors: AU, EARMA, TRI IE, UBO, ECSA, UCT, UT, UAB, KU, UAB, VUMC, WECF, UTokyo]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, and PDF documents; MURAL online web tool with AIT or licenses of task partners.

	<ul style="list-style-type: none"> • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal to the consortium partners.
Contact details of participants and correspondence	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the protected drives of task partners (one contact table for each task partner). One common version without contact details or correspondence details will be securely stored on password-protected project cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, Contact information will be kept until five years after the end of the project and then deleted. • Dissemination: internal to the consortium partners (never with contact details); for reporting to the European Commission on stakeholder participation (aggregate participation information; no contact details or names).
Online Social Lab meeting results	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint; MURAL online web tool with AIT or licenses of Task partners; PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP2. Results in terms of participant perspectives on climate and environmental ethics issues and possible responses will take the form of anonymised summaries filed in the Social Lab Report template. • Dissemination: internal, to the consortium partners.
D.2.2 Social Lab Implementation Report I: environment and climate ethical issues in the context of R&I and for the green transition	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of D2.2 and European Commission approval of deliverable. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC.

T2.4: Elaboration and validation of strategies and guidelines [Lead: AIT; Contributors: AU, EARMA, TRI IE, UBO, ECSA, UCT, KU, UAB, VUMC, WECF, UTokyo]
TYPE OF DATA: DATA LIFECYCLE AND HANDLING:

Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, and PDF documents; MURAL online web tool with AIT or licenses of task partners. • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal, to the consortium partners.
Online Social Lab meeting results	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of Task partners. • Format: Word, Excel, PowerPoint; MURAL online web tool with AIT or licenses of Task partners; PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal, to the consortium partners.
In-person Social Lab meeting results	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password protected drive of task partners. • Format: Word, Excel, PowerPoint; PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP2. Qualitative analysis of trends and themes. Results in terms of participant perspectives on climate and environmental ethics issues and possible responses will take the form of anonymised summaries filed in the UBO REC approved Social Lab Report template. • Dissemination: internal, to the consortium partners.
Contact details of participants and correspondence	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the protected drives of task partners (one contact table for each task partner). One common version without contact details or correspondence details will be securely stored on password-protected project cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, Excel, and PDF documents.

	<ul style="list-style-type: none"> • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal to the consortium partners (never with contact details); for reporting to the European Commission on stakeholder participation (aggregate participation information; no contact details or names).
D.2.3 Social Lab Implementation Report 2: strategies for responding to environment and climate ethical issues in the context of R&I and for the green transition	<ul style="list-style-type: none"> • Developed by: AIT, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of D2.3 and European Commission approval of deliverable. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC.

T2.5: 5 Packaging Social Lab learnings for exploitation and training support [Lead: AIT; Contributors: ECSA, UCT, UBO, AU, EARMA, NTUA, UAB, UTokyo, VUMC, KU]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, and PDF documents; MURAL online web tool with AIT or licenses of task partners. • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal, to the consortium partners.
D.2.4 Draft manuscript on environmental and climate ethical issues and response strategies	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of deliverable 2.4 and European Commission approval of deliverable. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC.

WP3: Produce and/or adapt Guidelines and Develop Policy Recommendations

T3.1: Incorporate the objectives of the “do no significant harm” principle [Lead: AIT; Contributors: UT; UAB; UTokyo, KU]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, and PDF documents; MURAL online web tool with AIT or licenses of task partners. • Processing: reviewed and updated as necessary, until the finalisation of WP2. • Dissemination: internal, to the consortium partners.
Stakeholder contact details and correspondence	<ul style="list-style-type: none"> • Developed by: task lead, with contribution from all task partners. • Storage: password-protected and securely stored on the protected drives of task partners (one contact table for each task partner). One common version without contact details or correspondence details will be securely stored on password-protected project cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of WP3. • Dissemination: internal to the consortium partners (never with contact details); for reporting to the European Commission on stakeholder participation (aggregate participation information; no contact details or names).
Audio, video and transcription of recordings of interviews	<ul style="list-style-type: none"> • Developed by: task lead, with contribution from all task partners. • Storage: password-protected and securely stored on the protected drives of task partners. Deleted upon completion of transcription. • Format: audio and video files, Word, Excel, and PDF documents. • Processing: transcription; development of anonymised interview summaries. • Dissemination: none for primary data. For processed anonymised data, internal to consortium partners.

D.3.1 Guidance report on incorporating the objectives of the "do no significant harm" principle in R&I	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of D2.4 and European Commission approval of deliverable. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC.
--	--

T3.2: Produce and/or adapt operational ethics and integrity guidelines [Lead: TRI I&E; Contributors: EUREC, AIT, ECSA, AU, UT, VUMC, UAB, EARMA, WECF

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: TRI with contribution from all task partners, based on analysis and findings of WPI and WP2. • Storage: password protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password protected drive of task partners. • Format: Word, Excel, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of D3.2. • Dissemination: internal, to the consortium partners.
D3.2 Research ethics and integrity guidelines for R&I in the Green Transition	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all partners, building on key concepts identified in WPI and insights collected in Social Labs in WP2. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word and PDF documents. • Processing: drafting, internal quality review, submission to EC. • Dissemination: submitted to the EC, distributed to target audiences, and made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC..

T3.3: Develop recommendations on environmental risk assessments [Lead: UBO; Contributors: NTUA, AIT, EARMA]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of D3.3. • Dissemination: internal, to consortium partners.
Material related to normative risk assessment	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, and PDF documents. • Processing: Compilation of concepts, methods and practices from scientific literature, reviewed and updated as necessary, until the finalisation of D3.3. • Dissemination: internal, to task partners.
Experiences with ethical risk assessment practices and protocols	<ul style="list-style-type: none"> • Developed by: task lead, task partners, partners' networks, and Social Lab participants. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, and PDF documents. • Processing: observations and feedback collection via literature review (internal desktop research) and practice reports (from Social Lab participants), benchmark analysis, reviewed and updated as necessary, until the finalisation of D3.3. • Dissemination: internal, to task and consortium partners and to Social Lab participants.
D.3.3 Recommendations on environmental and	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task partners.

climate ethics amendment of risk assessment strategies	<ul style="list-style-type: none"> • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word and PDF documents. • Processing: drafting, internal quality review, submission to EC. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC.
--	---

T3.4: Develop and disseminate policy recommendations on R&I governance [Lead: TRI I&E; Contributors: AIT, EUREC, NTUA, AU, WECF, EARMA]

TYPE OF DATA: DATA LIFECYCLE AND HANDLING:

Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task partners. • Storage: password-protected and securely stored on project drive and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint and PDF documents. • Processing: reviewed and updated as necessary, until the finalisation of D3.4. • Dissemination: internal to task and consortium partners.
Contact details and correspondence with relevant stakeholders, decision-makers and policymakers	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task partners, building partners' networks and on stakeholders identified in WP2. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Excel, Word, email exchanges. • Processing: collected in the stakeholder database, updated throughout the lifetime of the project. • Dissemination: internal, to task partners.
Recordings and transcription of consultations	<ul style="list-style-type: none"> • Developed by: task lead, with contribution from task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word, Excel, and PDF documents and a manual coding of the transcriptions. • Processing: transcribed, coded, and analysed for recommendations for D3.4 and D3.5.

	<ul style="list-style-type: none"> • Dissemination: internal, to task partners.
D.3.4 Policy brief 1	<ul style="list-style-type: none"> • Developed by: task partners, based on analysis built on WPI, WP2, and consultations. • Storage: password-protected and securely stored on project drive and in the internal password-protected drive of partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: drafting, internal quality review, submission to EC. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC.
D.3.5 Policy brief 2	<ul style="list-style-type: none"> • Developed by: task partners, built on T1.2, T2.4, and consultations. • Storage: password-protected and securely stored on project drive and in the internal password-protected drive of partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: drafting, internal quality review, submission to EC. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC.

WP4: Develop and Implement Training Programmes

T4.1: Develop training materials [Lead: VUMC; Contributors: AIT, ECSA, NTUA, TRI IE]	
TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: Reviewed and updated as necessary, until finalisation of D4.1. • Dissemination: internal, to task partners. Protocol will be made available on Zenodo.
Corpus of training material	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners.

	<ul style="list-style-type: none"> • Format: Word, Excel, PowerPoint, and PDF documents; H5P interactive files; MP3 and MP4 files. • Processing: quantitative (descriptive statistics) and qualitative (thematic content) data analysis. Reviewed and updated as necessary, until finalisation of D4.1. • Dissemination: internal, to task partners.
Delphi study survey responses	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: personal data and Delphi responses will be password-protected and securely stored in the internal password-protected drive of task leads. Delphi responses will be gathered using GDPR-compliant Lime Survey. • Format: Word, Excel, and PDF documents. • Processing: Quantitative (descriptive statistics) data analysis will be used for demographic data, and quantitative and qualitative (thematic content) data analysis will be used for survey responses. Reviewed and updated as necessary, until finalisation of D4.1. • Dissemination: Personal data will not be disseminated unless Delphi participants consent to being named as experts, in which case their names will be mentioned in the acknowledgements section of the draft manuscript made available on Zenodo and submitted to an appropriate journal for publication.
D.4.1 Micromodules	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF documents; H5P interactive files; MP3 and MP4 files. • Processing: reviewed and updated as necessary, until finalisation of D4.1. • Dissemination: internal, to task partners. Submitted to EC. Final micromodules will be made available on the Embassy of Good Science (CC by 4.0 licensing) and ENERI classroom. Draft manuscript will be made available on Zenodo and the RE4GREEN website and submitted to an appropriate journal for publication.

T4.2: Pilot, evaluate and refine training pathways [Lead: VUMC; Contributors: ECSA, NTUA, KU]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary, until finalisation of D4.2. • Dissemination: internal, to task partners.
Personal data and informed consent of participants involved in piloting study	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: personal data (contact list, demographic data i.e. gender, area of expertise, survey responses) will only be gathered after informed consent is given and will only be available to task leads. It will be password-protected and securely stored in the internal password-protected drive of task leads. • Format: Excel files. • Processing: Quantitative (descriptive statistics) data analysis will be used for demographic data, and quantitative and qualitative (thematic content) data analysis will be used for survey responses. Reviewed and updated as necessary, until finalisation of D4.2. • Dissemination: personal data will not be disseminated.
D.4.2 Training programmes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF documents; H5P interactive files; MP3 and MP4 files. • Processing: reviewed and updated as necessary, until finalisation of D4.2. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC. Final training programmes will be made available on the Embassy of Good Science (CC by 4.0 licensing) and ENERI classroom.

T4.3 Implementation and dissemination [Lead VUMC; Contributors: EUREC, ECSA, NTUA, TRI IE, WECF, KU]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: reviewed and updated as necessary, until finalisation of WP4. • Dissemination: internal, to task partners.
Tools, methods, and materials for dissemination of trainings	<ul style="list-style-type: none"> • Developed by: task lead, with contribution from task contributors. • Storage: Password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password protected drive of task partners. Training programmes will also be available on the Embassy of Good Science and ENERI classroom. • Format: Word, Excel, PowerPoint, and PDF documents; H5P interactive content files; MP3 and MP4 files. • Processing: reviewed and updated as necessary, until finalisation of WP4. • Dissemination: internal, to task partners. Final training programmes will be made available on the Embassy of Good Science (CC by 4.0 licensing) and ENERI classroom.

WP5: Make Impact and Ensure Sustainability

T5.1: Augment the Plan for Dissemination, Communication and Exploitation [Lead: NTUA]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: Password-protected desktop computers at NTUA. • Format: Word files. • Processing: reviewed and updated as necessary. • Dissemination: internal, to task contributors.

RE4GREEN press kit (logo, colours, posters, and other items related to the visual identity)	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: Password-protected desktop computers at NTUA and RE4GREEN SharePoint. • Format: Word, PowerPoint, PDF, png, and jpeg files. • Processing: reviewed and updated if formatting issues arise. • Dissemination: through all RE4GREEN dissemination and communication channels.
D.5.1 Project's branding: logo, aesthetics, website design, and social media presence	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected desktop computers at NTUA and in password-protected project cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word, PowerPoint, PDF, png, and jpeg files. • Processing: reviewed and updated if formatting issues arise. • Dissemination: to be made available to the public on the RE4GREEN website, published on Zenodo and submitted to the EC.

T5.2: Project website and Social Media presence [Lead: NTUA; Contributors: UBO]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: Password-protected desktop computers at NTUA. • Format: Word files. • Processing: continuously reviewed and updated. • Dissemination: If needed with relevant partners for planning joint activities
Online presence (Twitter, Instagram, project website)	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task contributors. • Storage: created content to be stored on NTUA servers (RE4GREEN website). • Format: WordPress output files. • Processing: continuously reviewed and updated. • Dissemination: through all RE4GREEN dissemination and communication channels.
D.5.2 Plan for dissemination, communication and exploitation	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all partners • Storage: password-protected desktop computers at NTUA, in password-protected project cloud-based drive (SharePoint, managed by the project coordinator). • Format: Word and PDF files. • Processing: reviewed and updated as necessary.

	<ul style="list-style-type: none"> • Dissemination: on the RE4GREEN website (NTUA servers), on Zenodo and submitted to the EC.
--	--

T5.3: Implement the Dissemination and Communication Plan [Lead: NTUA; Contributors: all]	
TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected desktop computers at NTUA. • Format: Word files. • Processing: reviewed and updated as necessary. • Dissemination: internal, to consortium partners.
Information on monitoring partners' dissemination and communication activities	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: Password-protected tabletop computers at NTUA, in password-protected project cloud-based drive (SharePoint, managed by the project coordinator), and on EC portal (continuous reporting section). • Format: Word files. • Processing: continuously reviewed and updated. • Dissemination: internal, to consortium partners, and the EC.
Names and email addresses for those who wish to receive the project's newsletter	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: Password-protected desktop computers at NTUA. • Format: Excel files. • Processing: continuously reviewed and updated. • Dissemination: no dissemination – all measures will be taken for GDPR-compliance to be safeguarded.

WP6: Coordination and Management

T6.1: Project coordination, administrative and financial management [Lead: UBO; Contributors: all]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes, administrative and financial documents	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. Sensitive financial documents are stored locally on GDPR-compliant servers at UBO, • Format: Word, Excel, PowerPoint, and PDF documents. • Processing: updated by partners as needed over the project's lifetime. • Dissemination: shared internally, with project partners, and with the EC.

T5.4: Implement exploitation, uptake and sustainability activities, M5-M36 [Lead: NTUA; Contributors: AIT, EARMA; EUREC, UBO, TRI IE]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected desktop computers at NTUA. • Format: Word files. • Processing: reviewed and updated as necessary. • Dissemination: internal, to task contributors.
Monitoring system and tools for dissemination activities	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected desktop computers at NTUA, in password-protected project cloud-based drive (SharePoint, managed by the project coordinator), on EC portal (continuous reporting section). • Format: Word files. • Processing: continuously reviewed and updated. • Dissemination: internal, to task contributors, and to the EC.

T6.2: Data management and open science [Lead: TRI IE; Contributors: all]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from all partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word, PowerPoint, and PDF files. • Processing: updated by partners as relevant over the project's lifetime, at a minimum in time with the project's interim review. • Dissemination: internal, to consortium partners.
D.6.2 Data management plan and Open Science	<ul style="list-style-type: none"> • Developed by: task lead, with contributions of all consortium partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word and PDF files. • Processing: drafting, internal quality review, updated throughout the project at a minimum in time with the project's interim review. • Dissemination: public document, submitted to the EC and shared with project partners, published on project website and Zenodo.

T6.3: Capacity building on gender expertise [Lead: WECF; Contributors: UBO, TRI IE]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word and PDF files.

	<ul style="list-style-type: none"> • Processing: reviewed and updated as necessary. • Dissemination: internal, to task contributors.
Corpus of training material,	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word, Excel, PowerPoint, and PDF files. • Processing: reviewed and updated as necessary. • Dissemination: internal, to the consortium partners.
Recommendations, guidelines and publications	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word, PowerPoint, and PDF files. • Processing: reviewed and updated as necessary. • Dissemination: internal, to consortium partners.
D.6.4 Training Methodology and Plan	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word and PDF files. • Processing: reviewed and updated as necessary prior to deliverable submission. • Dissemination: public document, submitted to the EC and shared with project partners, published on project website and Zenodo.
D6.5 Checklists, factsheets and gender glossary	<ul style="list-style-type: none"> • Developed by: task lead. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word and PDF files. • Processing: reviewed and updated as necessary prior to deliverable submission. • Dissemination: public document, submitted to the EC and shared with project partners, published on project website and Zenodo.

T6.4: Stakeholder and advisory board management [Lead: EUREC; Contributors: UBO, EARMA]

TYPE OF DATA:	DATA LIFECYCLE AND HANDLING:
Work Plan, internal notes	<ul style="list-style-type: none"> • Developed by: task lead, with contribution from task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of EUREC and task partners. • Format: Word, Excel, PowerPoint, and PDF files. • Processing: reviewed and updated as necessary. • Dissemination: internal, to task contributors.
Contact details of board members, informed consent, and correspondence	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of task partners. • Format: Word, Excel, PowerPoint, and PDF files. • Processing: reviewed and updated as necessary. • Dissemination: internal, to consortium partners.
Stakeholder database	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from consortium partners. • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint, managed by the project coordinator) and in the internal password-protected drive of EUREC. • Format: Word, Excel, PowerPoint, and PDF files. • Processing: reviewed and updated as necessary. • Dissemination: internal, to consortium partners.
Transcriptions and recordings of SAB meetings	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task partners. • Storage: password-protected and securely stored on the protected drives of task partners. • Format: Word, Excel, PowerPoint, and PDF files. • Processing: processed following the meetings and deleted upon completion of transcription. • Dissemination: no dissemination of primary data. Processed and anonymised data will be disseminated internally, to consortium partners.
D.6.3 Report on the activities of the	<ul style="list-style-type: none"> • Developed by: task lead, with contributions from task partners.

<p>stakeholder advisory board</p>	<ul style="list-style-type: none"> • Storage: password-protected and securely stored on the project's cloud-based drive (SharePoint managed by the project coordinator) and in the internal password-protected drive of partners. • Format: Word, Excel, PowerPoint, and PDF files. • Processing: reviewed and updated as necessary until submission of deliverable. • Dissemination: public document, submitted to the EC and shared with project partners, published on project website and Zenodo.
-----------------------------------	---

Table 3: Overview of RE4GREEN data

Appendix III

Personal Data Protection Table

	Partners	Collection and Processing of Personal Data
1.	UBO	<ul style="list-style-type: none"> Name, affiliation, position, expertise, professional title, gender, country, and contact details (email address) of participants in the UBO Social Lab. Data that will be collected from the individuals themselves (with their consent) in WP2. Upon contact, individuals are reassured of their right to withdraw from the database. Access: UBO staff and restricted to the partners leading the relevant activity. Stored on UBO's secure and password-protected GDPR-compliant institutional cloud server. Data will be shared with partners if needed, in line with the German Reference Center for Ethics in the Life Sciences' (DRZE) privacy policy and in compliance with the GDPR.
2.	EUREC	<ul style="list-style-type: none"> Name, affiliation, position, expertise, professional title, gender, country, and contact details (email address) of stakeholders for WP6. Data that will be collected from the individuals themselves (with their consent) and from publicly available data. Upon contact, individuals are reassured of their right to withdraw from the database. Access: EUREC's staff and restricted to the partners leading the relevant activity. Stored on EUREC's password-protected, GDPR-compliant SharePoint. Data will be shared with partners if needed, in line with EUREC's privacy policy and in compliance with GDPR.
3.	TRI IE	<ul style="list-style-type: none"> Name, affiliation, professional title, gender, and contact details (email address, phone number) of policy-makers and stakeholders for WP3, engagement and exploitation of research results. Data that will be collected from the individuals themselves (with their consent), data gathered in WPI and WP2. Upon contact, individuals are reassured of their right to withdraw from the database. Access: TRI's staff and restricted to the partners leading the relevant activity. Stored on TRI's secure and password-protected, GDPR-compliant SharePoint.

		<ul style="list-style-type: none"> Data will be shared with partners if needed, in line with TRI privacy policy and in compliance with GDPR.
4.	UT	UT will not be collecting personal data.
5.	AIT	<ul style="list-style-type: none"> Name, affiliation, position, expertise, professional title, gender, country, and contact details (email address) of participants in the AIT Social Lab. Personal data collected will be pseudonymised, and only pseudonymised data will be shared across Social Lab partners. Personal data will be collected from the individuals themselves (with their consent) in WP2, and data subjects will be assured that they can withdraw from the Social Labs at any point. Upon contact, individuals are reassured of their right to withdraw from the database. Access: AIT staff, and restricted to the partners leading the relevant activity. Stored on AIT secure, password-protected, GDPR-compliant institutional cloud server and SharePoint. Data will be shared with partners if needed, and contact details only if strictly necessary, in line with the AIT privacy policy and the GDPR.
6.	AU	<ul style="list-style-type: none"> Interviews and workshop meetings in WP2 will be recorded. Recordings, data, and signed informed consent forms will be stored securely. A secure folder at AU has been set up for this purpose. Only AU research team members will have access to this folder. Only pseudonymised data will be shared with other RE4GREEN partners. The data will be pseudonymised when reported, i.e., only non-identifying information will be shared in reporting (e.g., "one biodiversity researcher from a university; one policymaker working on the Green Transition"). Only pseudonymised information will be reported in participation statistics (e.g., gender, geography, sector, research field, Social Lab number), unless participants formally indicate otherwise.
7.	NTUA	<ul style="list-style-type: none"> Names and email addresses of those who wish to receive the project's newsletter. Storage and format: the team stores data in NTUA's secure server with a single- or double-encryption protocol and this procedure is GDPR compliant. During the process of raw data, it is stored temporarily on a password-protected desktop computer. Processing: only by task leader.

		<ul style="list-style-type: none"> Dissemination: no dissemination - all measures will be taken to uphold GDPR compliance.
8.	EARMA	<ul style="list-style-type: none"> Name, affiliation, position, expertise, professional title, gender, country, and contact details (email address) of participants in the EARMA Social Lab. The data will be pseudonymised before sharing with other partners. Recordings, data, and signed informed consent forms will be stored securely, in a dedicated and restricted folder. Access: EARMA's EU project's team. Stored on a secured and password-protected, GDPR-compliant institutional cloud server. Only pseudonymised data will be shared with other RE4GREEN partners, unless participants give permission otherwise.
9.	ECSA	<ul style="list-style-type: none"> Name, affiliation, position, expertise, professional title, gender, country, and contact details (email address) of participants in the ECSA Social Lab. The data will be pseudonymised before sharing with other partners. Data that will be collected from the individuals themselves (with their consent) in WP2. Upon contact, individuals are reassured of their right to withdraw from the database and the project. Access: ECSA staff, restricted to the partners leading the relevant activity. Recordings, data, and signed informed consent forms will be stored securely, in a dedicated and restricted folder. Stored on a secured and password-protected, GDPR-compliant institutional cloud server. Only pseudonymised data will be shared with other RE4GREEN partners, unless participants give permission otherwise.
10.	KU	<ul style="list-style-type: none"> Name, affiliation, position, expertise, professional title, gender, country, and contact details (email address) of participants in the Social Labs. Data will be pseudonymised before sharing with other partners. Data that will be collected from the individuals themselves (with their consent) in WP2 and WP4. Upon contact, individuals are reassured of their right to withdraw from the database. Access: KU staff, restricted to the partners leading the relevant activity.

11.	UAB	<ul style="list-style-type: none"> • The UAB validated the ENS National Cybersecurity Governance (cni.es) certification, equivalent to the Security Framework ISO 27,001 or the European NIS directive), in April 2024. • Regarding the RE4GREEN project, recordings of Social Labs and interviews conducted in WP2 will be stored in UAB's internal GDPR-compliant, password-protected SharePoint. • These recordings will be transcribed. Summaries of these transcriptions will be anonymised before being shared with the WP lead for analysis. The list of participants' contact details will be deleted after the completion of the project.
12.	UCT	<ul style="list-style-type: none"> • In the Social Labs, recordings will be made of the recruitment interviews as well as the three online workshops. For each of the interviews and the online Social Lab sessions, participants will be asked to fill out and sign informed consent forms. • The consent forms, personal data, and recordings will be safely stored in UCT's internal GDPR-compliant, password-protected cloud-based drive. • Only UCT RE4GREEN project staff will have access to the folder. • The recordings will be transcribed, and summaries of the transcriptions will be pseudonymised before being shared with the WP lead for analysis. • In reporting on the Social Labs, the data will be pseudonymised, including reporting of statistics related to Social Lab participation. • UCT subscribes to Microsoft's OneDrive Cloud Storage, which has been approved by the University's Information Security team for the storage of research data. The recording of data on electronic equipment during the interviews and Social Labs (audio recordings) shall be encrypted and password-protected. Devices containing personal data will be protected by whole-disc encryption. Identifiable data (including consent forms) will be stored on the UCT servers and will be held in accordance with its data management policy which is informed by the FAIR open data principles https://uct.ac.za/sites/default/files/content_migration/uct_ac_za/39/files/TGO_Policy_Research_Data_Management_2018.pdf • Any data transfer will be done securely and with a similar level of data protection as required under South African law.
13.	VUMC	<ul style="list-style-type: none"> • Name, affiliation, professional title, area of expertise, country, gender, and contact details (email address) of Delphi and piloting participants for WP4 (development of training materials). Delphi questionnaire responses will be gathered in T4.1. Publicly available names and email addresses of training course coordinators will also be gathered in T1.3.

		<ul style="list-style-type: none"> • For WP4, data will be collected from the individuals themselves (with their informed consent). • Upon contact, individuals are reassured of their right to withdraw from the database and the project. • Access: task leads. • Stored on VUMC's secure, password-protected, and GDPR-compliant SharePoint. • Data will be shared with partners if needed, in line with VUMC privacy policy and in compliance with GDPR. Only pseudonymised Delphi data (T4.1) will be shared amongst the Delphi participants, amongst the project partners, and in the final article as outlined in the information letter provided to participants.
14.	WECF	<ul style="list-style-type: none"> • Name, affiliation, professional title, gender, and contact details (email address, phone number) of stakeholders for WP6. • Data that will be collected from the individuals themselves (with their consent), data gathered in WP6. • Upon contact, individuals are reassured of their right to withdraw from the database. • Access: WE CF's staff working on RE4GREEN and restricted to the partners leading the relevant activity. • Stored on WE CF's password-protected, GDPR-compliant SharePoint. • Data will be shared with partners if needed, in line with WE CF privacy policy and in compliance with GDPR.
15.	UTokyo	<ul style="list-style-type: none"> • Recordings of SLs and interviews conducted in WP2 will be stored in UTokyo's internal GDPR-compliant, password-protected SharePoint. • These recordings will be transcribed. Summaries of these transcriptions will be pseudonymised before being shared with WP lead for analysis.

Table 4: Personal data

Appendix IV

Data Security Table

	Partners	Technical and organisational measures
1.	UBO	<ul style="list-style-type: none"> The DRZE's institutional policies and procedures are specified in its internal Privacy Policy. UBO follows the GDPR in relation to any project work undertaken, which involves data collection, storage, and transfer. All data are either stored locally on a password-protected laptop or desktop or on a secure, institutional, GDPR-compliant server maintained by UBO. Access to the documents is granted by invitation only and is limited to internal users at UBO. The DRZE's DPO is Dr. Jörg Hartmann (joerg.hartmann@uni-bonn.de).
2.	EUREC	<ul style="list-style-type: none"> EUREC's institutional policies and procedures are specified in its internal Privacy Policy. EUREC follows the EU's GDPR in relation to any project work undertaken, which involves data collection, storage, and transfer. Any personal data collected are stored on a secure, private, cloud-based server that is maintained on a routine basis. All access to cloud-based server files is granted by invitation only; there is a log register and related licences for each person on the cloud ensuring that only authorised staff may access the shared network environment and assets on the network. EUREC project members store their laptops (and any other device used for RE4GREEN) securely when unattended (at home or during travel), encrypt home office network access, and install and regularly update anti-virus software.
3.	TRI IE	<ul style="list-style-type: none"> Trilateral Research's institutional policies and procedures are specified in its internal Policies and Procedures document and its Data Protection Policy. Trilateral follows established guidelines in relation to any project work undertaken, which involves data collection, storage, and transfer. Regulation (EU) 2016/679 (General Data Protection Regulation – "GDPR") and the British and Irish Data Protection Acts of 2018 (the Acts) govern the processing of personal data. Any personal data collected are stored on a secure, private, cloud-based server that is maintained on a routine basis. All access to cloud-based server files is granted by invitation only; there is a log register and related licences for each person on the cloud. Trilateral encrypts access to the network via state-of-the-art network management tools, ensuring that only authorised Trilateral staff may access the shared network environment and assets on the network.

		<ul style="list-style-type: none"> • Trilateral project members store their laptops (and any other device used for RE4GREEN) securely when unattended (at home or during travel), encrypt home office network access, and install and regularly update anti-virus software. Any transfer of sensitive data only takes place over encrypted connections, using password protection and access controls in the case of uploads and downloads to and from repositories. • Trilateral Research is accredited under the UK government Cyber Essentials scheme.
4.	UT	<ul style="list-style-type: none"> • The University of Twente's institutional policies and procedures are specified in its internal Privacy Policy (this is managed by LISA). UT complies with the GDPR in relation to any project work undertaken, which involves data collection, storage, and transfer. • All data are either stored locally on a password-protected laptop or desktop or on a secure, institutional, GDPR-compliant server maintained by UT. Access to the documents is granted by invitation only and is limited to internal users at UT. • The UT DPO can be contacted at the following address: dpo@utwente.nl.
5.	AIT	<ul style="list-style-type: none"> • AIT institutional policies and procedures are specified in its internal Policies and Procedures document and its Data Protection Policy. • AIT follows established guidelines in relation to any project work undertaken, which involves data collection, storage, and transfer in compliance with the GDPR. • AIT operates a network access control system to control access to the LAN and WLAN. • AIT-managed devices (Windows and Linux) are authenticated by means of computer certificates, which are rolled out via Active Directory (AD) group policies or the Linux management system. The configuration of the 802.1x supplicant is also managed and rolled out centrally. • Authorisation (assignment to the authorised VLANs) is carried out via AD groups using LDAP queries for Windows systems or MAC address groups for Linux systems. • All other devices are authenticated via their MAC addresses and assigned to the corresponding VLANs. • Access is controlled by segmenting and separating the VLANs by means of LAN firewalls. Special project networks that require higher security standards are either protected by a project specific firewall or operated by means of their own internet breakouts (stand-alone solutions). • All of AIT's network infrastructure systems are monitored via a monitoring tool. Remote access for employees is via a dedicated VPN client software in connection with a central VPN gateway. • Authentication takes place via 2FA. • To ensure that the client is a valid AIT system, specific client parameters will be checked by a host checker when the connection is established.

		<ul style="list-style-type: none"> • Bitlocker hard disk encryption and pre-boot authentication are implemented on AIT notebooks running the Microsoft Windows 10 operating system. The purpose of this is to increase access security for Windows-based mobile devices (laptops). • AIT Servers are continuously provided with updates by the system administrator. Monthly updates are installed immediately after a patch is released by operating system manufacturers. Urgent updates announced by the manufacturers, or the CERTs are promptly coordinated and implemented in service operations in close collaboration between system administrators, ITC and ITO, who will also notify those affected by a service interruption. • The AIT DPO can be reached at dpo@ait.ac.at
6.	AU	<ul style="list-style-type: none"> • AU's institutional policies and procedures are specified in its internal Privacy Policy: https://international.au.dk/about/profile/privacy-policy AU follows the European Union's General Data Protection Regulation (GDPR) in relation to any project work undertaken, which involves data collection, storage, and transfer. • All data are stored on a secure, institutional, GDPR-compliant server maintained by AU. Access to the documents is granted by invitation only and is limited to the AU RE4GREEN research team. • AU's DPO can be contacted at dpo@au.dk.
7.	NTUA	<ul style="list-style-type: none"> • The NTUA team stores data in NTUA's secure server with a single- or double-encryption protocol, and this procedure is compliant with the GDPR. • While raw data are being processed, they are stored temporarily on a password-protected desktop computer.
8.	EARMA	<ul style="list-style-type: none"> • EARMA's institutional policies and procedures are specified in the Privacy Statement, available on its website: https://earma.org/privacy-statement/#:~:text=We%20publish%20photographic%20and%20visual,EARMA%20members%20with%20EARMA%20members • EARMA follows the GDPR in relation to any project work undertaken, which involves data collection, storage, and transfer. • Any personal data collected is stored on a secure, private, cloud-based server that is maintained on a routine basis. All access to cloud-based server files is granted by invitation only. • The EARMA DPO is Ms Emma Lythgoe, Executive Director (emma.lythgoe@earma.org).
9.	ECSA	<ul style="list-style-type: none"> • ECSA follows the European Union's General Data Protection Regulation (GDPR) in relation to any project work undertaken, which involves data collection, storage, and transfer.

		<ul style="list-style-type: none"> • Any personal data collected are stored on a secure, private, cloud-based server that is maintained on a routine basis. All access to cloud-based server files is granted by invitation only. • ECSA project members store their laptops (and any other device used for RE4GREEN) securely when unattended (at home or during travel), encrypt home office network access, and install and regularly update anti-virus software.
10.	KU	<ul style="list-style-type: none"> • The KU institutional policies and procedures are specified in its internal Information on Security Regulations (정보보안규정, 3-1-68) • All data are either stored locally on a password-protected laptop or desktop or on a secure, institutional server. The KU contact for Information Security Management System is yerlsim@korea.ac.kr.
11.	UAB	<ul style="list-style-type: none"> • The UAB implements the GDPR's recommendations on security measures, and those contained in Spanish Royal Decree 1720/2007, of 21 December, which enacts the Regulation implementing the Organic Law on the protection of personal data (LOPD): • Procedure for backing up and recovering data. • Procedure for confirming the identity of authorised users. • Access controls. • Access register. • Limit to repeated unauthorised access attempts. • Procedure for assigning and managing passwords, and expiry periods. • Unintelligible storage of active passwords. • Management of storage media. • Designation of a person in charge of coordinating and monitoring the security measures. • Audits. • Security procedures in the transmission of data. • Regarding breaches on security, the GDPR requires the supervisory authority and the data subjects to be notified of security breaches that present, or could present, a major risk to the rights and liberties of natural persons, whether these are the owners of the data or third parties. This notification must be made within 72 hours of the breach occurring or of becoming aware it. • To eliminate or minimise the risks or the consequences of security breaches, the UAB must adopts the necessary technical and organisational measures, which include the following. • Pseudonymisation or encryption of personal data.

		<ul style="list-style-type: none"> • Procedures to guarantee the confidentiality, integrity, availability and permanent resilience of the processing systems and services. • Ability to restore availability and access to the personal data quickly in the event of a physical or technical incident. • Procedure for verifying and assessing technical and organisational measures.
12.	UCT	<ul style="list-style-type: none"> • UCT subscribes to Microsoft's OneDrive Cloud Storage which has been approved by the University's Information Security team for the storage of research data. • The recording of data on electronic equipment during the interviews and SLs (audio recorders or photographic cameras) shall be encrypted and password protected. Devices containing personal data will be protected by whole disc encryption. Identifiable data (including consent forms) will be stored on the UCT servers and will be held in accordance with its data management policy which is informed by the FAIR open data principles (data should be 'Findable, Accessible, Interoperable and Reusable') https://uct.ac.za/sites/default/files/content_migration/uct_ac_za/39/files/TGO_Policy_Research_Data_Management_2018.pdf • Research data will be stored for the number of years as agreed in the grant agreement after publication or public release of the work. • Any data transfer will be done securely and with a similar level of data protection as required under South African law.
13.	VUMC	<ul style="list-style-type: none"> • VUMC's institutional policies and procedures are specified in the Privacy statement of Amsterdam UMC. VUMC follows the European Union's General Data Protection Regulation (GDPR) in relation to any project work undertaken, which involves data collection, storage, and transfer. • Any personal data collected is stored on a secure, private, cloud-based server that is maintained on a routine basis. All access to cloud-based server files is granted by invitation only; there is a log register and related licences for each person on the cloud ensuring that only authorised staff may access the shared network environment and assets on the network • VUMC project members store their laptops (and any other device used for RE4GREEN) securely when unattended (at home or during travel), encrypt home office network access, and install and regularly update anti-virus software
14.	WECF	<ul style="list-style-type: none"> • WECF uses a state-of-the-art SharePoint provided by Microsoft that follows the security standards, especially an access control via password and is GDPR compliant • Use of strong passwords

		<ul style="list-style-type: none"> • Raising employee awareness in dealing with personal data, especially via data protection and security training, as well as refresher training for such • Automatic locking of devices after a certain period of inactivity if manual locking cannot be guaranteed when leaving the area of influence.
15.	UTokyo	<ul style="list-style-type: none"> • UTokyo's institutional policies and procedures are specified in its internal Privacy Policy. UTokyo also follows the European Union's General Data Protection Regulation (GDPR) in relation to any project work undertaken, which involves data collection, storage, and transfer. • Any personal data collected are stored on a secure, private, cloud-based server that is maintained on a routine basis. All access to cloud-based server files is granted by invitation only; there is a log register and related licences for each person on the cloud ensuring that only authorised staff may access the shared network environment and assets on the network. • UTokyo project members store their laptops (and any other device used for RE4GREEN) securely when unattended (at home or during travel), encrypt home office network access, and install and regularly update anti-virus software.

Table 5: Data security

Appendix V

ICT Tools and GDPR Compliance Table

Tool used	Information on GDPR Compliance	How the tool is used in RE4GREEN
MS Teams	https://privacy.microsoft.com/en-gb/privacystatement	RE4GREEN consortium uses Teams for its meetings with partners.
LinkedIn	https://privacy.linkedin.com/gdpr	RE4GREEN uses LinkedIn to post news about the project and related to the topics covered by the project, to an audience that consists of institutions, organisations, EU projects and individuals that work/are involved in related fields.
X	https://gdpr.twitter.com/en.html	RE4GREEN partners use Twitter to share and post news about the project and topics covered by the project. Re4GREEN follows institutions, organisations, EU projects and individuals that work/are involved in related fields.
Zoom	https://zoom.us/privacy	RE4GREEN project currently uses Zoom for online meetings, workshops, and events. Each participant joins the meeting using their name and email address. Personal data will not be re-used in any way. No information is stored locally (unless required for audit) and no copies are made unless there is a need for recording in which case we will seek a consent of participants.
Lime Survey	https://www.limesurvey.org/	RE4GREEN will use this service to assist with Delphi questionnaire for task 4.1
One Drive	https://onedrive.live.com/	RE4GREEN will use this service to assist to store research material for individuals on the cloud, not to be shared with other partners
Zotero	https://www.zotero.org/	RE4GREEN will use this service to assist with citation management for tasks 1.3 and WP4
MAXQDA	Is my data safe when using MAXQDA Transcription? - MAXQDA	RE4GREEN will use this service to assist with qualitative data analysis for tasks 1.3 and WP4
R	R: The R Project for Statistical Computing (r-project.org)	RE4GREEN will use this service to assist with quantitative data analysis for tasks 1.3 and 4.1

Website	RE4GREEN	RE4GREEN will use this service to assist with publication of RE4GREEN findings and promotion of the project
Whisper	GDPR-compliant transcription tool	RE4GREEN will use this service to assist with WP2 transcriptions at AU

Table 6: ICT Tools and GDPR compliance

