ORIENTING

D7.4

Data Management Plan (updated)

WP n° and title	**WP7 – Project Management and Coordination**
Responsible Author(s)	**TEC**
Contributor(s)	**GHE, VTT, FHG, ECE, PRE, EIF, UCA, ECA, LAV, ECR, ACL, BAS, TER, STO, SOL, LEI**
Dissemination level	**PUBLIC**
Version	**V4**
Keywords	**Data management policy, Data security, Project research data, Open data, Open Science.**

www.orienting.eu **@orienting_eu** **info@orienting.eu**

Disclaimer: This Deliverable reflects only the author's views and the Agency is not responsible for any use that may be made of the information contained therein.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 958231.

DOCUMENT INFORMATION

Grant Agreement Number	**958231**
Project Title	**ORIENTING: Operational Life Cycle Sustainability Assessment Methodology Supporting Decisions Towards a Circular Economy**
Status (F: final; D: draft; RD: revised draft):	**F**
Planned delivery date	**30/04/2022 (M18)**
Actual delivery date	**26/05/2022 (M18)**
Dissemination level: (PU = Public; PP = Restricted to other program participants; RE = Restricted to a group specified by the consortium; CO = Confidential, only for members of the consortium)	**PU**

DOCUMENT HISTORY

Version	Date (MM/DD/YYYY)	Description of changes	Contributors
01	**04/21/2021**	**First version - draft**	**TEC**
02	**04/28/2021**	**Comments from partners**	**All**
03	**04/30/2021**	**First version - final**	**TEC**
03	**20/05/2022**	**First updated version - draft**	**TEC**
04	**24/05/2022**	**Comments from partners**	**All**
05	**26/05/2022**	**Updated version - final**	**TEC**

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

Tables

Figures

No table of figures entries found.

Acronyms

CA	**Consortium Agreement**
DMP	**Data Management Plan**
EC	**European Commission**
GA	**Grant Agreement with the EC**
GDPR	**General Data Protection Regulation**
IPR	**Intellectual Property Rights**
ISO	**International Organization for Standardization**
LCA	**Life Cycle Assessment**
LCC	**Life Cycle Costing**
S-LCA	**Social Life Cycle Assessment**
LCSA	**Life Cycle Sustainability Assessment**
MT	**Management Team**
PMP	**Project Management Plan**
PO	**Project Officer**
QAP	**Quality Assurance Plan**
TL	**Task Leader**
WP	**Work Package**
WPL	**Work Package Leader**

Executive summary

The H2020 **project ORIENTING** (Operational Life Cycle Sustainability Assessment Methodology Supporting Decisions Towards a Circular Economy) aims to develop a robust, operational methodology for product Life Cycle Sustainability Assessment (LCSA). The main value of the project is to provide a holistic and practical life-cycle approach for the integrated assessment of environmental, social and economic impacts of products and services, taking into consideration circularity and criticality aspects as well.

WP7 of ORIENTING covers all tasks related to the overall project management (e.g. administrative, financial and legal issues) to ensure the accuracy, quality and timeliness of the work undertaken in the project.

The **first version of the D7.3 Data Management Plan (DMP)** for the project was submitted in M6. The DMP is a dynamic document evolving during the lifespan of the project. In this sense, Deliverable D7.4 "Updated Data Management Plan" is published on M19 (one month later than originally planned) to update the data management policy within the project.

The Consortium strongly believes in the concepts of open science, and in the benefits that the European innovation ecosystem and its economy can draw from allowing the reuse of data at a larger scale. The purpose of the Data Management Plan (DMP) is to provide an analysis of the main elements of the data management policy that will be used by the Consortium, with a specific focus on project research data.

The DMP covers the complete research data life cycle. It describes the types of research data that will be generated or collected during the project, the standards that will be used, how the research data will be stored and what parts of the datasets[1] will be shared for verification, reuse or other uses. It also reflects the current state of the Consortium agreements on data management and is consistent with exploitation and IPR requirements.

Research data linked to exploitable results will not be put into the open domain if they compromise its commercialisation prospects, have inadequate protection, or in case of confidentiality issues. The rest of research data will be made public through an open access repository.

The expected types of research data that will be collected or generated along the project deal with the integration and operationalization of life cycle sustainability assessment and lie in the following categories:

1. LCSA methods, models, indicators, data (for topics addressed in ORIENTING), also including "LCSA-supporting tools" (e.g. spreadsheets and templates that guide goal and scope definition, materiality assessment and selection of indicators).
2. Data and software specifications.
3. LCSA integration tool.
4. Procedures and guidance documents (guidelines for consistent LCSA application, training material).
5. Technical-scientific outputs (e.g., reports, scientific articles, contributions to conferences, input for standards).

[1] A dataset is defined in this context as a collection of data (see also https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm)

1. Introduction

This document describes the Data Management Plan (DMP) for ORIENTING, a project funded by the European Union's H2020 Programme under Grant Agreement #958231. The DMP was initially presented on Month 6 as Deliverable 7.3 of the project and its updated version was planned on Month 18, as Deliverable 7.4 Data Management Plan (updated).

This DMP follows the guidelines provided by the EU H2020 programmes.[2] The DMP is, according to the European Commission (EC), a key element of good data management. A DMP describes the data management life cycle for the data to be collected, processed and/or generated by the project. As part of making research data findable, accessible, interoperable and re-usable (FAIR), a DMP should include 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/made open access.
- how data will be handled and stored (including after the end of the project).

A questionnaire has been designed and distributed to collect data management information from the consortium partners (see *Annex A*). Replies obtained on Months 6 and 18 have been checked and updated to refine the DMP.

2. Data summary

2.1. Purpose of data collection and generation

The purpose of data collection and generation in ORIENTING is to produce know-how. The results and the conclusions from analysing all those data collected and generated will help achieve the goal of the project, i.e. the development of an operational life cycle sustainability assessment methodology.

2.2. Data collection and generation

Most of the data will be generated from the tasks carried out from work package WP1 to WP5, but WP6, which combines exploitation and dissemination activities, will be key for data management since it will ensure that ORIENTING's outputs and data are properly managed and exploited.

A preliminary identification of ORIENTING's products was done as part of WP6 activities, which was updated in M18. This has resulted in the following categorization of the data to produce in the framework of the project:

1) LCSA methods, models, indicators, data (for topics addressed in ORIENTING), also including "LCSA-supporting tools" (e.g. spreadsheets and templates that guide goal and scope definition, materiality assessment and selection of indicators).
2) Data and software specifications.
3) LCSA integration tool.
4) Procedures and guidance documents (guidelines for consistent LCSA application, training material).

[2] European Comission. (2016). Data management - H2020 Online Manual. Retrieved October 9, 2020, from https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

5) Technical-scientific outputs (e.g., reports, scientific articles, contributions to conferences, input for standards).

A detailed description of products will be generated per WP during the ORIENTING project and compiled in the excel file "**https://tecnalia365.sharepoint.com/:x:/r/sites/PLANNMBP-42/Documentos%20compartidos/WP7-Project%20Management%20and%20Coordination/Products/List%20of%20products%20of%20ORIENTING.xlsx?d=w7856ccd1b32945578bd6a8a41addc750&csf=1&web=1&e=WoeO4n**".

Table 1. Dataset information template (applicable to any category identified)

Work Package	**Which WP and deliverable the dataset is related to**
Type of product	Types could be report, paper, interview, expert or organization contact details, video, audio, presentation, or note
Dataset Name	The name of the dataset/product should be easily to search and find
Version number	To keep track of changes to the dataset/product
Link	Provide link used in Teams
Description	Brief description of the dataset/product
Responsible partners	The lead partners responsible for the dataset generation/collection
Purpose	The purpose of the data collection/generation and its relation to the objectives of the project
Digital format	Data formats could be XLSX, DOC, PDF, PPT, JPEG, OPJ, TIFF, PBIX, other (specify)
Digital size	The size of the dataset (units: GB/MB) and the number of files
Sources	The origin of the data
IPR Owner	Which project participant(s) own the intellectual property right (IPR)
Re-use existing Data	Identification if any existing data being reused and how they are used
Beneficiary	To whom the data may be useful
Keywords	The keywords associated with the dataset to make it easier to search and find

3. FAIR data

ORIENTING will make the datasets generated in the project comply to European Commission's FAIR data policy – "Findable, Accessible, Interoperable, Reusable".

3.1. Making data findable, including provisions for metadata

A file naming system has been set in D7.1 Quality Assurance Plan for easy identification of files stored in the project internal collaborative platform (Microsoft Teams). The naming convention includes a short description of the document that is aligned with the "dataset name" and "keywords" of each dataset. Besides, it has also a version number.

Naming conventions: ORIENTING_<WPX>_<D/TX.Y>_<Title>_<Beneficiary>_<Date>_<Version>.<ext>

Where:

<WPX> Work Package identifier, for example “WP1”. Omit when not applicable

<D/TX.Y> Deliverable or task number, for example “D2.3” for Deliverable 2.3. or T5.2 for Task 5.2. Omit when not applicable

<Title> Short description of document.

<Beneficiary> i) Beneficiary acronym when presenting individual activities and the deliverables / milestones by the lead beneficiary;
ii) WPL when the leader is reporting as Work Package leader.

<Date> Date in “ddmmyyyy” format.

<Version> Version identifier: ‘v1’, ‘v2’…‘vfinal’

<Beneficiary> and <Date> are optional. When the task is identifiable with the name of the deliverable, <WPX> field can also be optional to avoid repetitions.

Example: ORIENTING_D7.1_Quality Assurance Plan_v1.docx.

It has also been set a common naming system (e.g. ORIENTING#TEAMS/WP1/Meetings) for data findability, as well as keywords in the datasets/deliverables.

For published articles, a Digital Object Identifier (DOI) is assigned by journals as a unique and permanent code to identify the article. For contribution to conferences, bibliographic references will be provided.

Partners have been asked via questionnaire (see Annex A) if they are satisfied with the common naming system proposed to make data findable. **Partners are generally satisfied with the procedure** put on place.

3.2. Making data openly accessible

Research data generated in the ORIENTING project will comply with all requirement of the GA. In fact, article 27.1 of the GA states the obligation to protect the results and article 28.1 the obligation to exploit those results. An elaborated exploitation plan will be submitted as deliverable D6.9 in month 36.

However, article 29.1 of the GA states that “Unless it goes against their legitimate interests, each beneficiary must — as soon as possible — ‘disseminate’ its results by disclosing them to the public by appropriate means (other than those resulting from protecting or exploiting the results), including in scientific publications (in any medium).” In this regard, it is important to note that **if a partner intends to disseminate its results, “must give advance notice to the other beneficiaries of — unless agreed otherwise — at least 45 days, together with sufficient information on the results it will disseminate**. Any other beneficiary may object within — unless agreed otherwise — 30 days of receiving notification, if it can show that its legitimate interests in relation to the results or background would be significantly harmed. In such cases, the dissemination may not take place unless appropriate steps are taken to safeguard these legitimate interests.”

Furthermore, article 29.2 of the GA specifies that “**each beneficiary must ensure open access (free of charge online access for any user) to all peer-reviewed scientific publications relating to its results**.” This is already taken into account and, after surveying the partners, the goal of submitting at least 5 articles to peer reviewed journals has been confirmed (see also section 4 on allocation of resources).

Internally, the Consortium is using Microsoft Teams as intranet to store project related data and documentation. A webpage was also created (https://orienting.eu/) to grant external access to public deliverables, and for other communication purposes.

In their replies to the questionnaire, most partners say that project **data is stored in their cloud and/or server, giving specific access permissions** to those team members working on the project.

Some partners made also explicit that accessibility rights are assigned based on the confidentiality of the data (partly making use of non-disclosure agreements).

Others mentioned that procedures for data accessibility (including authentication and authorization) are implemented.

Furthermore, it was suggested to discuss at Consortium level on the possibility of publishing key data underlying scientific publications, to ensure validation of results. In principle, data could be archived in a common and open data repository, if not restricted by IPR or other confidentiality issues.

3.3. Making data interoperable

The Consortium aims to collect and document the data in a standardized way to ensure the datasets would be easy to understand, reuse and interoperate among different parties who are interested in utilizing them. Standard technical terminology will also be used to facilitate inter-disciplinary interoperability.

Partners have been asked how to make data interoperable. Feedback generally converges towards the need of using of a **standard vocabulary** explaining terms (incl. acronyms) and definitions relating to Life Cycle Sustainability Assessment. Shared definitions and a new LCSA ontology to use in ORIENTING is being set up during the project, mainly through activities of WP2 and WP3.

Partners have also been asked if they are going to generate data in a **non-standard format** for which special software is needed, and if so, which measures will be taken to make that data accessible to all partners. The only comment in this respect relates to the ".pbix" format, which however will not pose any issue for project partners. The .pbix is the data format for documents generated in Power-BI (a software tool within Microsoft environment and its cloud services, which is used for the development of the user-friendly hands-on integration tool). Some partners, involved in the development and debugging of the tool, will have premium access to the Power-BI development environment and will have the possibility to edit files in .pbix format allowing them modifying internal tool specifications, graphics and metrics if required. Users of the integration tool will not be affected in any case, since they will have access only to their results through a web interface, which will be running using a common web-browser for all users and will contain the results by means of an embedded dashboard generated in Power-BI.

3.4. Increase data re-use (through clarifying licenses)

Data reusability means the easiness to re-use the data for further researches or other purposes. In the ORIENTING project, most datasets have high reusability because no special methods or software is required to re-use the data. When formats will be not standard, the information will be converted into standard formats such as .doc, .xlsx, .pdf, .jpeg or .ppt.

Partners have been asked what they intend to do with the data after the project is finished. Apart from storing relevant data for potential uses in future, partners are generally willing to communicate, disseminate and exploit key results. Partners may also use them for internal development purposes. Agreements to publish data created in the project should be taken at Consortium level.

The quality assurance of the data is part of the general Quality Assurance Plan (D7.1). All deliverables will be internally peer-reviewed by consortium members: WP Leaders will be in charge of reviewing technical deliverables of their WP. The

Project Coordinator will be responsible for final review, validation and submission to the EC. The articles published in scientific journals will be externally peer-reviewed.

Partners have been asked which specific procedures should be implemented to ensure quality. A reference to general quality standards for companies (e.g. ISO 9001) and data quality ratings was made. Furthermore, it was highlighted that publication of research results lead to searchable resource, and that contracts define the usage rights of products and data. A recommendation was made of using Creative Commons licence CC-BY-SA or CC-BY for any opened datasets, unless there are compelling reasons to select more restricted type of CC-licence. Creative commons licences by default also include a disclaimer of liability for the re-use of opened data. Additionally, attention should be paid for the quality of metadata.

4. Allocation of resources

The open accessibility of research data generated in the context of the H2020 Programme implies costs for the consortium. Such costs are eligible for reimbursement during the project lifetime if compliant with the GA conditions.

The planned budget dedicated to data management is shown in Table 2. Partners have confirmed the allocation of resources described in the GA.

Table 2. Allocation of resources

Partner Name	Descriptions
TEC	1 open access publication fee (1 paper) (3 000€)
GHE	1 open access publication fee (1 paper) (3 000€)
VTT	1 open access publication fee (1 paper) (3 000€)
FhG	1 open access publication fee (1 paper) (3 000€)
ECE	1 open access publication fee (1 paper) (3 000€)
EIF	1 open access publication fee (1 paper) (3 000€)
UCA	1 open access publication fee (1 paper) (3 000€)

As for long-term preservation of the datasets, different internal policies of each partners are noted in table 3.

Table 3. Long-term policies for data preservation

Partner Name	Decision Maker for Data Preservation	Preservation timeframe after the end of the project
TEC	Project Coordinator and Manager of ORIENTING	5 years
GHE	Prof. Dr. ir. Jo Dewulf	5 years
VTT	Principal investigator of the project	20 years (unless agreed otherwise)
FHG	Project Manager and Head of Department	Minimum 5 years, depending also on legally required periods
ECE	Scientific Director and CEO	5 years
PRE	Standard retention policies	5 years
EIF	Project manager	10 years, min. legally required period, up to
UCA	Director of The Centre for Sustainable Design (CfSD)	10 years

ECA	Project manager and Ecoinvent management	5 years
LAV	Project Manager	Unless specified by the client or project's contract, data will be stored indefinitely.
ECR	Executive Director	For an unlimited period of time
ACL	Project manager	5 years
BAS	Project manager	5-10 years, minimum 5 years, depending also on legally required periods
TER	Project manager	10 years
STO	Stora Enso Packaging Materials Sustainability team	minimum 5 years, depending also on legally required periods
SOL	CEO	10 Years
LEI	Project manager	>5 years

5. Data security

Currently, the ORIENTING project is using Microsoft Teams as collaborative platform to share, store and edit data and documents related to the project. The platform is only accessible to members, which are invited by Project Manager or Project Coordinator. The data and communication safety and privacy within the collaborative platform is guaranteed by Microsoft:

- Microsoft "Teams enforces team-wide and organization-wide two-factor authentication, single sign-on through Active Directory, and encryption of data in transit and at rest. Files are stored in SharePoint and are backed by SharePoint encryption."[3]
- "Network communications in Teams are encrypted by default. By requiring all servers to use certificates and by using OAUTH, TLS, Secure Real-Time Transport Protocol (SRTP), and other industry-standard encryption techniques, including 256-bit Advanced Encryption Standard (AES) encryption, all Teams data is protected on the network."[4]
- Microsoft guarantees that the information is stored on servers located in the European Union[5].

Besides, most of the consortium partners have their own provisions in place for data security (as listed in Table 4).

[3] Microsoft (2022) Security and compliance in Microsoft Teams. Retrieved on May 24th, 2022 from https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview#:~:text=Teams%20enforces%20team%2Dwide%20and,are%20backed%20by%20SharePoint%20encryption.

[4] Microsoft (2022) Security and Microsoft Teams. Retrieved on May 24th, 2022 from https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide

[5] https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?geo=All&view=o365-worldwide

Table 4. Data security provisions within partner's organisation

Partner Name	Data Security Provisions
TEC	Data access: Every worker in TECNALIA has his/her own password-protected user account to access the systems (MFA or double factor identification). The access to networks folders and programs where information is stored/managed depends on user permissions. Backup: TECNALIA has two-level backup for the information kept within its local infrastructure. The first level is the system "previous versions" service that allows a user to recover a copy of the work (5 copies a day, two weeks period). Moreover, every day TECNALIA makes full backup of the working information. There are daily, weekly, monthly and yearly copies. The recover from this backup requires a formal procedure. Transfer of data: To transfer information TECNALIA uses platforms that require security protocols, such as OneDrive and SharePoint, and information protection tools such as Veracrypt.
GHE	Ghent University provide documentation on how to secure data, as described in a summarized way in the text that follows: "1. Use a trustworthy device (desktop, laptop, notebook, tablet, smartphone,…) which is sufficiently secure. (…) 2. Within the buildings of Ghent University, you work on a trusted network that is adequately protected (…) 3. Protect your Ghent University account and the associated login data (username and password) (…) 4. Be fully aware of common risks and hazards (…) 5. Use the central disk space/storage (personal disk space and shares) offered by DICT instead of storing files locally on your own IT resources (hard disk of desktop or laptop, USB stick, external hard disk,…) (…) 6. Preferably work with the applications offered on Athena.UGent.be (Citrix technology) 7. Install as few additional applications as possible on your devices, and certainly nothing that is downloaded from the internet without any security guarantees or sent via e-mail. This reduces the risk of infections with malware. 8. Do not use external cloud services to store personal data or confidential information unless you encrypt this data in a secure and reliable manner using cryptographic tools. (…) 9. You carry responsibility for working with information in a secure manner. (…) 10. Inform the DICT Helpdesk as soon as possible if you suspect a data leak, as a result of which confidential information might have ended up in the wrong hands, or if you notice any other information security incident. (…)."
VTT	Data collected or acquired within the project will be stored in a secure IT environment behind a firewall at VTT's premises or in secure cloud environment provided by VTT's selected IT service providers. Access to all VTT's IT systems need registration and authentication. Principal Investigator checks applications for the use of data. Where access is granted to research data, this will be provided through secured telecommunications channels. According to VTT's safety policy, data and IT systems can only be accessed via devices acquired from VTT's IT administration, and in which necessary safety updates are made regularly. VTT adheres to requirements set in GDPR regulations if/when handling personal data.
FHG	In addition to the German Data Protection Regulation (DSGVO), the German Federal Data Protection Act (BDSG), and a large number of other laws containing data protection regulations, provisions contained in central works agreements and company agreements as well as the IT Security Manual are of particular importance to Fraunhofer-Gesellschaft employees in their employment.
ECE	The security is ensured by: authentication procedures explained above; quality system 9001 for data management; GDPR for the management of personal data. In addition, all the sensitive data and models are saved in double copy, also into an external hard disk. Moreover, every day Ecoinnovazione makes full backup of the working information.
PRE	ISO certified for Information Security for the development of their software and apply these general policies and procedures also for consultancy projects
EIF	The security is ensured by: authentication procedures for computers; by default, GDPR for the management of personal data. In addition, all data and models are saved locally on the

	computers of the project contributors, on institute data storage and internal back-up system on tape and external back-up (e.g. at the Karlsruhe Institute of Technology).
UCA	GDPR policies at the level of the university and a related plan for The Centre for Sustainable Design (CfSD). UCA-CfSD retains physical records as required by the EC.
ECA	Data security provisions include: regularly updated software and trustworthy employee devices, data encryption, password management best practices, role-based access control, off-site backups and audit logging.
LAV	Regarding the equipment, every employee in Anthesis Lavola has his/her own password-protected user account to access the systems. There are two systems of data management depending on the type of data: Microsoft Sharepoint is used for project documentation, and Oracle Netsuite is used for project management. Netsuite also contains the clients and supplier's data. With Sharepoint, documentation of the project is stored in a folder indefinitely unless specified otherwise. This folder can be either accessed by everyone at the organization or, if specified, can be protected with restricted access to certain users. Sharepoint access is protected with password, which is also verified/double-checked with the Authenticator system via mobile phone. Sharepoint documents are stored in the cloud, it counts with Microsoft's own backup system plus it allows to store up to 500 changes so that older versions of a file can be restored. Regarding Netsuite, economic, clients and supplier's data of a project is stored directly within Netsuite's web platform. Access to Netsuite is protected with password, security questions and verification with mobile, and it has restricted access and actions allowed depending on the role of the user. Netsuite has its own backup system. There is also the policy of not sharing data outside the organisation unless it is made through Sharepoint. Training on data security have been provided to all employees, and special training for data managers too.
ECR	Common data security protocols and tools for online and offline data storage and transmission.
ACL	Data security procedures to ensure GDRP compliance for data storage and transmission
BASF	NDA and internal data security procedures managed by a central department.
TER	Internal procedures for Digital Data Security - ISO 9001
STO	Data access: Every worker in Stora Enso has his/her own password-protected user account to access the systems. The access to networks folders and programs where information is stored/managed depends on user permissions. All data and models are saved on the internal network drive with access limited to only Sustainability team members.
SOL	Data security procedure, protocols and tools in order to avoid data leakage and ensure compliance with GDPR for online and offline data storage and transmission.
LEI	As defined per ISO 9001, as well as firewall and training.

6. Ethical aspects

The partners of the ORIENTING project will comply with article 34 of the GA concerning ethics and research integrity.

Partners cannot share (confidential) information externally unless agreed.

Privacy of data subjects must be ensured and handled according the European GDPR regulation. Confidentiality of data (e.g. in exchanges with AB members, or data collected and used in case studies) must be bilaterally discussed between involved parties, and an NDA signed when necessary. This may imply that some data cannot be shared with the entire consortium.

Furthermore, while promoting data sharing, partners highlighted the need to **comply with**

- other European and National Data Protection Laws (e.g. data storage outside Europe is not considered adequate).

- Antitrust disclaimers and requirements.

7. Personal data management

ORIENTING project, and specially WP5 activities, has the aim to create a network of stakeholders from many different sectors and countries. In this context, data protection and management policy are crucial. The Data Management procedures described here update those presented in D5.1 "Stakeholder's engagement Plan".

7.1. Compliance with national and EU legislation

ORIENTING will comply with ethical principles and with applicable international, EU and national law. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), effective from 25 May 2018, describes ethical considerations for the use and security of personal data that shall be taken into account within ORIENTING.

The consortium will not ask for any kind of personal sensitive data (health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction). As there is no sensitive personal data to be collected and stored at all by any of the partners in the ORIENTING project, there are no additional permissions from competent local/national ethic/legal bodies required. All partners are committed to thoroughly implement the data protection policy.

7.2. Procedure to contact stakeholders

This procedure updates the one described in D5.1 "Stakeholders' Engagement Plan" (Chapter 3.4 "Data management policy"). To contact and invite stakeholders to participate in the activities of ORIENTING (e.g. questionnaires, workshops, subscription to newsletter, social networks), the following procedure is established in accordance to the general principles of the GDPR (EU General Data Protection Regulation 2016/679):

1. A preliminary ORIENTING contacts' database excel file was created to collect the following general information (no personal data included): Stakeholder category | Subcategory |Organization | Department or Area| Website
2. Ecoinnovazione and Tecnalia checked this database to detect possible omissions.
3. Each partner contacted directly their own contacts, to suggest or invite them to participate in the project and updated the database.
4. Only those contacts that had previously been involved in a similar project or topic were contacted, otherwise it could be considered as commercial activity. In accordance with Directive 2000/31/EC (Directive on electronic commerce), if a company (i.e. any partner) is going to advertise or offer products or services via e-mail (the ORIENTING project can be seen as a service), it can only do so when the commercial communication meets the following requirements:
   I. It is **addressed to** a company or natural person who is a **client or collaborator**, that is, with whom there has been a previous relationship with. The communication must refer to products or services similar to those previous relationship, we should never address clients or stakeholders to offer them something in which they have not shown prior interest or collaboration.
   II. If it is **not addressed to a client or collaborator**, the communication would be only possible if the person it is addressed to, has previously requested it or expressly authorized.
5. ECE-TEC provided a draft common presentation text (see **ANNEX B**. Email presentation proposal for contacts).

Once this first contact was done, the stakeholders interested in participating in different activities (e.g. workshops) were requested to register in the website. In doing so, they filled a contact form and gave the required authorization (in

accordance with all Legal requirements of Data Protection) to share personal data and feedback in the context of the ORIENTING project. All data collection is centralized through the website, where data controllers of personal data are clearly identified and also the purpose and legal basis for processing those data (see **ANNEX C**).
ORIENTING website gives also the chance to readers to subscribe to the newsletter using Mailchimp services. The subscription form for this purpose asks for email address, first name, last name, and authorization checkbox ("I accept to receive Communications from ORIENTING project"). The Data Protection policy for this subscription is clearly made available to the reader. Furthermore, to functional mailbox have been created for interactions with stakeholders: info@orienting.eu and events@orienting.eu.

7.3. Scope of personal data to be collected

No sensitive personal data will be collected. Personal data will be collected and stored only when necessary to identify an expert or stakeholder in his/her official or professional role, as well as to maintain a balance between different stakeholders:

- Identification and contact details (name, surname, email address, country).
- Personal information: gender.
- Professional/employment-related details (organization, role, type of organization, sector of operation).
- Codes and keys that identify registered user of the website (password).
- Internet browsing data (e.g. IP address, website visits, Wi-Fi network connections, location).

Only ECE, LAV and TEC will have access to these files. Furthermore, pictures and recordings of activities and events organised by the consortium are taken only after agreement of all participants.

7.4. Data management procedures

Questions included in stakeholders' consultations will only cover real needs for the development of the ORIENTING project. Answers will be gathered and treated confidentially in relevant deliverables (e.g. D5.4 "Document on comments and replies from the online consultation"). Anonymized records, reviewed to highlight common stakeholder needs, will be integrated in the following public deliverables:

- D5.2 "Report on users' needs and wishes".
- D5.3 "Report on the outcomes of Stakeholders' engagement".

7.4.1. Data collection

Data will be collected for specified, explicit and legitimate purposes. The data collection process will allow the data subjects to give their consent. The purpose of data collection will be explicitly determined at the time of the collection. In case of statistical purposes, the result of processing is aggregate data and not personal.

If a consortium partner is the creator of data (e.g. by performing interviews, or performing surveys), then the partner is responsible for proper storage, processing and sharing of that data, and ensuring that personal data is purged before further dissemination to the consortium.

If a consortium partner wishes to use relevant information for ORIENTING activities but is not the creator (e.g. by acquiring relevant datasets or relevant documentation), then the partner is responsible for determining the source of the data and assessing the data sharing policies and if the dataset contains personal or otherwise privacy-compromising data. If that is the case, it is the responsibility of the consortium partner to purge personal data from that dataset and prepare it for further dissemination in a proper admissible form.

7.4.2. Data storage

The storage period will be reasonable with respect to the processing purposes. The data will not be stored more than necessary and solely for the purposes for which they were collected. In case of any detected data loss, the data subject will be informed without delay.

Information collected by ORIENTING that is not already in the public domain will be fully anonymized. This involves partners removing the link between data and identifiable individuals.

All data shared and processed by the consortium will be stored in secure environments at the locations of consortium partners with access privileges restricted to the relevant project partners.

7.4.3. Data protection

The key principles that apply to personal data protection are detailed here:

- Data processing will be authorized (see **ANNEX C**) and executed fairly and lawfully. In case of any detected alteration or unauthorized disclosure, the data subject will be informed without delay.
- Although the ORIENTING project will not be collecting such data, it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
- The data subject will have the right to remove consent, on legitimate grounds, to the processing of data relating to him/her. He/she will also have the right to remove consent, on request and free of charge.
- When organizing online workshops/webinars, the registered participants’ names and personal information will be kept confidential among the co-controllers (as stated in ANNEX C). The only information that can be provided to other organizations is the list of organizations that participated in the workshop/webinar.

7.4.4. Data retention

Personal data facilitated by stakeholders (by giving authorization through the website) will be retained until 6 months after the completion of the project. The data controller will facilitate the data subject to access, rectify their data, and practice his/her 'right to be forgotten' (GDPR, Article 17). In addition, the controller will not hinder any attempt of the data subject to transfer the collected data to another controller (GDPR, Article 20).

7.4.5. Data transfer

If processed data is to be transferred from one partner to another, care has to be taken to do so in a secure manner, for example via a secure data channel, in an encrypted mode, or via secure physical transfer. If processed data is transferred from one partner to another, the Coordinator (TEC) will be informed.

7.4.6. Data destruction

The data controller will evaluate the risks of accidental or unlawful data destruction. In case of any detected destruction the data subject will be informed without delay.

7.4.7. Procedure for informed consent

Informed consent is a key principle of ethical research, ensuring that research participants are adequately informed of the risks of taking part in experimental studies, that their participation is voluntary, and that the information about them gathered remains under their control. The two key principles of informed consent, taken here from the *Economic and Social Research Council* (ESRC) Framework for Research Ethics (http://www.ethicsguidebook.ac.uk/consent-72), can be defined as:

- Principle 1: Research subjects must be informed fully about the purpose, methods and intended possible uses of the research, what their participation in the research entails and what risks, if any, are involved.
- Principle 2: Research participants must participate in a voluntary way, free from any coercion.

This data management policy will be presented to the public on the project website for free download (Annex C). Each of the contacted stakeholders will be provided with an electronic copy (email) or a printout of this data management policy upon his or her request. Each potential research participant will be contacted and asked if they would be interested in participating in the project. Participation will be entirely voluntary. Participants can refuse, interrupt, deny responding to any questions and withdrawing from the consultation at any time with no consequences.

Without any prior written consent, these data will not be stored. Stored data will be only used for the purpose of this project and exchanged only between the partners as far as this is necessary for the implementation of this project. Data exchange will be aggregated and anonymous, removing all personal identification data.

7.4.8. Use of pre-existing data

During the course of the research, it is possible that the ORIENTING team will gain access to data that was collected before the start of the project, by an organization who is not a member of the Consortium. In this event, the ORIENTING partner who receives this data must ensure that there is no information contained in the data that could be used to identify individual citizens. Furthermore, the ORIENTING partner must be mindful of the risks of linking this data, or conclusions resulting from this data with data or conclusions from other data sources.

In a similar way as when interacting with human participants, informed consent must be obtained when acquiring pre-existing data from external sources. Data exchange will be aggregated and anonymous, removing all personal identification data will be removed in the exchange. This procedure is not necessary when data has been explicitly released to the public domain or released under clearly stated conditions that include the intended usage within the ORIENTING project.

8. Other issues

At current stage, all consortium partners have reported no obligation to comply with additional specific national, funder, sectorial, departmental, or institutional data management policies or procedures.

9. Annexes

9.1. Annex A. Questionnaire for Data Management Plan

The aim of this questionnaire is to gather information on data generation, collection and management procedures carried out by ORIENTING partners within their organizations. This information will be used within Deliverable 7.3. Data Management Plan.

Section 1: FAIR Data

FAIR data are data which meet principles of findability, accessibility, interoperability, and reusability[6]

1.1 Data findability

In the project, we will use the common naming system (e.g. ORIENTING#TEAMS/WP1/Meetings) for data findability, as well as keywords in the datasets/deliverables.

a. Are you happy with this and/or do you have improvements to suggest?

Click or tap here to enter text.

b. Does your organization have further identifiers for tracking generated data?

Click or tap here to enter text.

1.2 Data accessibility

a. Does your organization have any procedures for data accessibility (including authentication and authorization) that could be applied to ORIENTING?

Click or tap here to enter text.

1.3 Data interoperability

a. Data collected within ORIENTING project should be interoperable, this is, understandable and usable by all members. Will you use standard vocabulary to allow inter-disciplinary interoperability? If technical terms are used, how will you ensure the understandability?

Click or tap here to enter text.

b. Are you going to generate data in a non-standard format for which special software is needed? If so, how do you plan to make data accessible to other partners?

Click or tap here to enter text.

1.4 Data re-usability

a. What are you planning to do with the data produced once the project is completed (license, publish, store …)?

[6] Wilkinson, Mark D.; Dumontier, Michel; Aalbersberg, IJsbrand Jan; Appleton, Gabrielle; et al. (15 March 2016). "The FAIR Guiding Principles for scientific data management and stewardship". *Scientific Data*. **3**: 160018. doi:10.1038/sdata.2016.18. OCLC 961158301. PMC 4792175. PMID 26978244.

Click or tap here to enter text.

b. Do you have any specific quality control procedures for re-usability in place to ensure the quality of the generated data (e.g. accessible data usage license, procedure to register or index data in searchable resources.)?

Click or tap here to enter text.

1.5 Any other aspect related to FAIR data

a. Do you have any other aspect related to FAIR data that you would like to point out?

Click or tap here to enter text.

Section 2: Allocation of Resources

2.1 There is a certain budget allocated for data accessibility (such as publication fees in open access journals) in the GA. Do you agree with it or do you think that modifications are needed?

Click or tap here to enter text.

The planned budget dedicated to open access publications already foreseen in the GA is shown here:

Partner Name	Descriptions
TEC	1 open access publication fee (1 paper) (3 000€)
GHE	1 open access publication fee (1 paper) (3 000€)
VTT	1 open access publication fee (1 paper) (3 000€)
FhG	1 open access publication fee (1 paper) (3 000€)
ECE	1 open access publication fee (1 paper) (3 000€)
EIF	1 open access publication fee (1 paper) (3 000€)
UCA	1 open access publication fee (1 paper) (3 000€)

2.2 Long-term preservation of the data:

a) Did you allocate economic resources for long-term preservation of data, even after the end of the project?
Yes ☐ No ☐

b) For which resources?

Click or tap here to enter text.

c) Who will decide which data to keep?

Click or tap here to enter text.

d) For how long?

Click or tap here to enter text.

Section 3: Data Security

3.1 What provisions are in place for data security within your organization?

Click or tap here to enter text.

Section 4: Ethics

4.1 Are there any ethical or legal issues that can have an impact on data sharing?

Click or tap here to enter text.

Section 5: Other management procedures

5.1 Do you make use of other procedures for data management?

Yes ☐ No ☐

5.2 If yes, which ones? Click or tap here to enter text.

Section 6: Data Summary (Products identification)

Please fill in this excel file stored in "https://tecnalia365.sharepoint.com/:x:/r/sites/PLANNMBP-42/Documentos%20compartidos/WP7-Project%20Management%20and%20Coordination/Products/List%20of%20products%20of%20ORIENTING.xlsx?d=w7856ccd1b32945578bd6a8a41addc750&csf=1&web=1&e=WoeO4n" with information for all potential products/datasets your organization might generate or collect during the project (e.g. guidelines, software specifications, tool, scientific paper). Information to be compiled are reported below, please note that must be inserted in the excel file in transposed format.

Work Package	WP Choose an item. , Deliverable Click or tap here to enter text.
Type of product	**What types of data/product will be collected/generated?** Click or tap here to enter text.
Dataset Name	Click or tap here to enter text.
Version number	**Will you provide clear version number to keep track of changes to the dataset/product?** Yes ☐ No ☐
Link	Provide link used in Teams
Description	**Please write a brief description of the dataset/product.** Click or tap here to enter text.
Responsible partners	**Who are the lead partners responsible for the dataset generation/collection?** Click or tap here to enter text.
Purpose	**What is the purpose of the data collection/generation and its relation to the objectives of the project?** Click or tap here to enter text.
Format	XLSX ☐ DOC ☐ PDF ☐ PPT ☐ JPEG ☐ OPJ ☐ TIFF ☐ PBIX ☐ Other ☐ Click or tap here to enter text.
Size	Expected Size: Click or tap here to enter text. GB☐ MB☐ Number of files: Click or tap here to enter text.
Source	**What is the origin of the data? How the dataset is generated/collected?** Click or tap here to enter text.
IPR Owner	Click or tap here to enter text.
Re-use existing data	**Will you re-use any existing data?** Yes ☐ No ☐ **If yes, how will you use?** Click or tap here to enter text.
Beneficiary	**To whom will the data be useful?** Click or tap here to enter text.
Keywords	**The keywords associated with the dataset.** Click or tap here to enter text.

9.2. Annex B. Email proposal for contacts

Subject: Invitation to register as stakeholder of the EU-funded ORIENTING project on Life Cycle Sustainability Assessment

Dear Mr./Ms. XXX

With this message we would like to inform you about the EU-funded ORIENTING project, as we consider it may be of interest to you.

The ORIENTING project ("Operational Life Cycle Sustainability Assessment Methodology Supporting Decisions Towards a Circular Economy") is developing a comprehensive and operational methodology for the life cycle sustainability assessment (LCSA) of products and services. The innovation of this approach lies in the integration of environmental, social and economic impacts: the aim is to evaluate the products produced under both linear and circular business models, enabling professionals to understand and manage the possible alternatives.

The partners of the project are TECNALIA (coordinator), UGENT, VTT, FRAUNHOFER, ECOINNOVAZIONE, PRE, EIFER, UCA, ECOINVENT, ANTHESIS-LAVOLA, ECOPRENEUR.EU, ACLIMA, BASF, TERNUA, STORA ENSO, SOLANA and LEIBLEIN.

ORIENTING aims to contribute to the development of a future Product Sustainability Footprint at European level, evolving existing PEF and designing new indicators for the evaluation of material criticality and product circularity. New tools will be developed to support and simplify the methodology application in business and policy development. Tools include guidance and training materials, data and software specifications and a hands-on LCSA IT tool. The methodology and support tools will be applied in five industrial case studies that will serve as demonstrators.

The project outcomes will enable informed business decisions and contribute to the development of a levelled playing field – a single market – for products based on robust (i.e. transparent and verifiable) sustainability information. In order to ensure the applicability of the outcomes of the project, the consortium aims to work in close cooperation with various stakeholders (industry associations and clusters, SMEs, consumer organisations, as well as governmental and standardisation bodies) through engagement and dissemination events.

Since we consider your participation in the project of mutual interest, we would like to invite you to register as a stakeholder in the following link, as well as to follow our social networks profiles LinkedIN & Twitter. By registering as stakeholder, you will be regularly updated about the progress of the project and may be invited to engagement and dissemination events.

Best regards,
Your signature

This project has received funding from the European Union’s Horizon 2020 Research and Innovation programme under grant agreement No 958231.

We inform you that the ORIENTING processes your personal data contained in this communication in order to inform you of the activities and services offered by this entity. The legal basis that enables us to process your data is your consent or, failing that, the legitimate interest in response to the relationship we have with you to date. You can exercise your rights of access, rectification and deletion of your data, limit its treatment and opposition to its processing, as well as your right to portability at any time by sending a written communication to the email address info@orienting.eu (Data Controller)

If you do not wish to receive new communications regarding the activities and services offered by this entity, please communicate it to the following email address: info@orienting.eu (Data Controller)

9.3. Annex C. Website Privacy Policy

Summary of the Privacy Policy presented at www.orienting.eu website.

Who is the data controller for your personal data?

The personal data that you provide to us herein and in other communications with us shall be processed by the following CO-CONTROLLERS:

Name: Anthesis Lavola
Address: Rambla de Catalunya, 6, planta 2, 08007 Barcelona, Spain
Tel: 938 51 50 55
Tax ID Code (CIF): VAT number: ESA58635269
Email address: info@lavola.com

Name: Ecoinnovazione
Address: Via Massimo D'Azeglio 51,
c/o Studio Mele, 40123 Bologna, Italy
Email address: eco@ecoinnovazione.it
Tel: +39 328 9870 609
Tax ID Code (CIF): VAT number: IT04669840284

Name: Tecnalia Research & Innovation
Address: Parque Científico y Tecnológico de Bizkaia
Astondo Bidea, Edificio 700 E-48160 Derio (Bizkaia)
Tel: 902 760 000
Tax ID Code (CIF): G48975767
Email address: dpo@tecnalia.com

How have we obtained your data?

The data we process have been provided by you via the different forms you filled out while browsing the WEBSITE and/or via other channels (e.g. registering as a user of the WEBSITE).

If the personal data you provided pertain to a third party, you hereby guarantee that you have informed said third party of this PRIVACY POLICY and have obtained their authorisation to provide their data to the CO-CONTROLLERS for the purposes specified below.

Where indicated (in the fields marked with an " * "), the personal data requested are mandatory. If you do not provide them, or the data you provide are incorrect, it will not be possible to process your request and/or provide the services requested.

The CO-CONTROLLERS are not responsible for ensuring the veracity of the data provided by the users. Under all circumstances, the users themselves are responsible for ensuring the accuracy and authenticity of the personal data they provide. The user undertakes to provide information that is complete and correct. The CO-CONTROLLERS shall not be held in any way liable for any damage or detriment that may derive from the use of said information.

However, the CO-CONTROLLERS shall be held liable for the veracity of the information that they themselves produce, and reserve the right to update, modify or remove the information contained on the WEBSITE and even to limit or refuse access to said information. The CO-CONTROLLERS shall be exempted from any and all liability with regard to any damage or detriment that the user may suffer as a result of any errors, defects or omissions in the information provided by the CO-CONTROLLERS, where such information originates from outside or public sources.

What personal data do we collect?

The data processed by the CO-CONTROLLERS are data that you have provided to us while you were browsing the WEBSITE, via the relevant forms that we use to formalise our contact with you, and/or via email.

In particular, we process the following categories of data:

- Identification and contact details (e.g. name, surname, email address, telephone number, country, date of birth, etc.).
- Personal information: gender.
- Professional/employment-related details (e.g. company and position).
- Images recorded during the activities and events organised by TECNALIA and in which you have taken part.
- Codes and keys that identify you as a registered user of the WEBSITE.
- Internet browsing data (e.g. IP address, website visits, Wi-Fi network connections, location, etc.).

What is our purpose and legal basis for processing your data?

Your personal data is processed pursuant to development of the PROJECT and to manage the involvement of the interested parties in same; and to promote and raise awareness of the development of the PROJECT and its content. More specifically:

- To manage and process your registration as a user of the WEBSITE.
- To manage your access to and use of the content and services that the CO-CONTROLLERS make available to you via the WEBSITE.
- To process and manage any requests for information, suggestions and queries you may submit via the WEBSITE or via email, including queries regarding privacy and/or the exercising of your rights with regard to data protection.
- To send you communications related to the Orienting project, via different means including electronic channels, provided you have given your consent.
- To manage your subscription to our newsletter service and the sending of the corresponding electronic communications, provided you have given your consent.
- To manage and raise awareness of the activities and events organised by the CO-CONTROLLERS, in cases where you have given your consent to same.

Under no circumstances shall the data collected be used to create profiles or make automated decisions.

In accordance with the applicable regulations, the processing of your personal data by the CO-CONTROLLERS is based on the following, as applicable: (i) your consent, which is given at the moment we collect the personal data you voluntarily provide to us via the mechanisms provided for this purpose on the WEBSITE; (ii) the legal relationship you have established with us; and (iii) compliance with legal obligations.

We hereby remind you that, for cases in which processing is based on your consent, you may freely revoke this consent at any time and without charge, under the terms specified in the section on Rights.

To whom do we disclose your data?

We hereby inform you that your personal data may be disclosed to the following third parties:

- The public administrations, authorities and bodies to which the CO-CONTROLLERS may be legally obliged to disclose your data.
- Other organisations that, together with the CO-CONTROLLERS, form part of the Consortium created to carry out the activities of the Orienting project (and are duly identified in the following link), for the purpose of dealing with your requests and queries and/or sending you communications related to the project.

Additionally, we also inform you that your personal data may be disclosed to third parties that provide services to the CO-CONTROLLERS in their capacity as data processors. Some of these data processors have data-processing centres located outside the European Economic Area; consequently, your data may be subject to international transfer, in accordance with the applicable legal guarantees. In particular, LAVOLA uses a third-party technology service (Mailchimp) located in the United States to manage the sending of commercial communications via electronic channels. The corresponding international data transfers are carried out under the aegis of standard contractual clauses for the transferring of personal data to data processors located in third-party countries approved by the European Commission. No other international data transfers are envisaged.

How long will we keep your data?

As a general rule, personal data shall be kept while they remain necessary with regard to the purpose for which they were collected, or until you revoke your consent or request the erasure of your data (if this should occur beforehand). We shall also keep your data for the additional amount of time required to comply with any legal obligations that the CO-CONTROLLERS may be required to observe.

Notwithstanding the above, we hereby inform you that the CO-CONTROLLERS have put in place internal data scrubbing policies designed to regulate the amount of time they keep the personal data they control, so that the data can be deleted when they are no longer necessary and/or suitable for the purpose for which they were collected.

What rights do you have and how can you exercise them?

The applicable regulations on data protection afford you a series of rights in relation to your personal data, which you may exercise while your data are being processed. These rights are detailed below:

- Accessing your data: you have the right to access your data in order to find out which of your personal data we are processing.
- Requesting the rectification or erasure of your data: under certain circumstances, you have the right to rectify inaccurate personal data that pertains to you and which we are processing, and even to request that we erase your data when, among other reasons, the data are no longer necessary for the purposes for which they were collected.
- Requesting the limitation of the processing of your data: under certain circumstances, you have the right to request that we limit the processing of your data, in which case we inform you that we shall only keep your data for the purposes of making or defending against any claims that may arise, as provided for in the applicable regulations on data protection.
- Data portability: under certain circumstances, you have the right to obtain a copy of the personal data you have provided to us, in a structured, machine-readable, commonly used format, and to transfer said data to another controller.
- Objecting to the processing of your data: under certain circumstances, and for reasons related to your personal situation, you have the right to object to the processing of your personal data; in which case, we shall cease to process them, unless they must be kept for overriding and lawful reasons or for the purposes of making or defending against any claims that may arise.

Likewise, you also have the right to withdraw your consent at any time; however, this shall not affect the lawfulness of the processing that was carried out based on the consent that was given prior to the withdrawal.

You may exercise these rights by sending a written request to any of the CO-CONTROLLERS at the postal address specified in the section titled “Who is the data controller for your personal data?”, or by sending an email to info@orienting.eu.

Lastly, you are hereby informed that you may also file a claim with the competent supervisory authority.

Security measures

At all times, the CO-CONTROLLERS shall ensure that your data is processed under conditions of absolute confidentiality and in line with the obligation of secrecy, in accordance with the stipulations of the applicable data protection regulations. To this end, we shall adopt the necessary technical and organisational measures to ensure the security of your data and prevent them from being altered, lost, processed or accessed without authorisation, taking into account the state of technology, the nature of the data stored and the risks to which they are exposed.

Cookie Policy

Additionally, we hereby inform you that the WEBSITE has a Cookie Policy, which can be accessed via the following link. Cookie Policy