METHODOLOGIES FOR TEAM WORKING IN ECO-OUTWARDS RESEARCH

Grant Agreement: 101178320

D1.1 Data Management Plan

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Project description

Acronym	METEOR
Title	**Methodologies for Team Working in Eco-Outwards Research**
Coordinator	CASE – Center for Social and Economic Research in Warsaw
Type	Coordination and Support Action (CSA)
Programme	Horizon Europe (HORIZON)
Topic	CL2-2024-TRANSFORMATION
Duration	12/2024 to 11/2027
Website	www.meteorhorizon.eu
Consortium	**CASE – Center for Social and Economic Research, Poland (Coordinator)**
	Nord Universitet, Norway
	The Open University, United Kingdom
	Universita Degli Studi Di Verona, Italy
	European University Cyprus, Cyprus
	Jyvaskylan Yliopisto, Finland
	Kastamonu Universitesi, Türkiye
	Ilia State University, Georgia
	Asociacion Para La Gestion Del Centro Europeo, Spain
	Hacettepe Universitesi, Türkiye
	Roskilde Universitet, Denmark
	SYNYO GmbH, Austria
	Universidade Do Estado Da Bahia, Brazil (Associate)

Deliverable

Deliverable number	**D1.1**
Deliverable title	Data Management Plan
Deliverable version	1.0
Lead beneficiary	**CASE**
Work package number	WP1
Work package title	Management
Due date of delivery	28.02.2025
Actual date of delivery	28.02.2025
Dissemination level	Public
Type	**DMP**
Rights	METEOR Consortium
Authors	**Magdalena Wiśniewska (CASE)**
	Kacper Banaszewski (CASE)
Reviewers	Jan Bazyli Klakla (CASE)
	Martyna Gliniecka (CASE)
	Izabela Chałupka-Moszczyńska (CASE)
	Terhi Nokkala (JVY)
	Ale Okada (OU)
	Toril Irene Kringen (NO)
	Sagnik Sengupta (NO)
	Loucas Louca (EUC),

Document history

Version	Date	Beneficiary	Description
0.1	06.02.2024	CASE	First draft
0.2	14.02.2024	CASE	Second draft
0.3	19.02.2024	CASE	Third draft
1.0	28.02.2024	CASE	Final editing

Executive Summary

The METEOR (Methodologies for Teamworking in Eco-Outwards Research) project is a HORIZON Coordination and Support Action aimed at advancing data management practices within interdisciplinary ecological research. This Data Management Plan (DMP) provides a structured framework for collecting, processing, storing, and sharing research data in accordance with FAIR (Findable, Accessible, Interoperable, and Reusable) principles in accordance with the Horizon Europe Open Research Data pilot, GDPR (General Data Protection Regulation).The key objectives of this DMP include:

- Establishing guidelines for data acquisition, storage, security, and usage, including but not limited to specify conditions of data collection;
- Ensuring legal and ethical compliance, particularly concerning personal and sensitive data;
- Defining resource allocation for data management throughout the 36-month project duration;
- Promoting open science through public accessibility of non-sensitive research outputs.

Data collection and management under METEOR will adhere to standardized naming conventions, metadata structures, and interoperability protocols. The project will utilize EUDAT B2SHARE for metadata documentation and licensing, ensuring structured data governance and long-term accessibility.

The data security strategy emphasizes encryption, access controls, regular backups, and proactive monitoring to mitigate risks such as unauthorized access, data breaches, or cyber threats.

Ethical considerations have been integrated into the project, ensuring transparency, accountability, and compliance with open-access principles and gender equality.

This DMP will undergo continuous updates to reflect emerging requirements, evolving regulations, and best practices in data stewardship and research collaboration. The METEOR consortium remains committed to fostering a sustainable, ethical, and innovative research environment through effective data management.

Disclaimer of warranties

This project has received funding from the European Union's Horizon Europe HORIZON under Grant Agreement no. 101178320. This Data Management Plan (DMP) has been prepared or approved by METEOR project partners as an account of work carried out within EC-GA no. 101178320.

This document is provided without any guarantees or warranties of any kind, whether expressed or implied. The authors and the METEOR Project Consortium working on account of EG-CA no. 101178320 disclaim any and all liability for any direct, indirect, incidental, consequential, or other damages that may arise from the use, reliance on, or application of this document.

The authors and the METEOR Project Consortium bear no responsibility for any misinterpretation, modification, or distribution of this document. Furthermore, the content of this DMP does not necessarily reflect the views, policies, or opinions of the authors or the METEOR Project Consortium.

To the fullest extent permitted by law, the authors and the METEOR Project Consortium disclaim any liability for:

- Any damages or losses arising from the use or reliance on the DMP, including but not limited to data loss, financial loss, reputational damage, or legal liabilities.
- Any consequences of decisions made based on the DMP, including but not limited to misinterpretations or misapplications of the guidance provided.
- Any third-party distribution, modification, or use of this document.
- Any changes in applicable laws, regulations, or policies that may affect the relevance, compliance, or validity of the DMP.
- Any perceived or actual endorsement, recommendation, or representation derived from the document by any third party.

Users of this document are solely responsible for ensuring their compliance with applicable legal, ethical, and regulatory requirements. It is strongly recommended that users seek independent professional advice before implementing any provisions outlined in the DMP.

Contents

Tables:

Table 1 List of abbreviations and nomenclature

Symbol/Shortname	Deliverable
DMP	Data Management Plan
FAIR	Findable, Accessible, Interoperable and Reusable data management and sharing policy
GDPR	General Data Protection Regulation
EC-GA	European Commission Grant Agreement

1 Introduction

This document is the Data Management Plan (DMP) for METEOR. The DMP is the official document for the METEOR project, stating the currently foreseen ways of acquiring, storing, using and sharing data and the legal and ethical principles surrounding the technical aspect of the project, while also serving as an indicative plan as to what kind of data the project beneficiaries expect to generate during the project and how these data will be managed. This DMP is primarily designed for project partners to ensure the application of standardized procedures and best practices in data management. The outlined guidelines enhance operational efficiency, regulatory compliance, and risk mitigation, ensuring structured data governance, improved interoperability, and strengthened security measures.

The DMP outlines what and how data will be collected, processed and analyzed, which methodology and standards will be applied, whether data will be shared/made open access and how data will be curated and preserved during and after the end of the project.

GDPR compliance mandates personal data processing to be lawful, fair, transparent, and limited to specified purposes. This includes i.a. enforcing data minimization, informational obligations, integrity controls, and access restrictions.

The FAIR principles facilitate systematic data structuring, metadata integration, and machine-readability for interoperability while maintaining security constraints.

2 Data Collection and other processing under METEOR

WP1 Management

Data collected and produced in WP1 Management relates mainly to the user accounts and profile information that is needed for the project's internal administrative purposes along with financial reporting data. This encompasses personal data of Meteor partner personnel and Advisory Group members. The contact information comprise information such as name, organization, email address, role, etc. The information shall be stored in an internal restricted repository (currently utilising MS Teams platform and One Drive) under the regime of data protection and privacy. This information is only shared within the partnership and will not be made openly available.

WP2 Evidence

What follows applies to data collected as part of Tasks from T2.1 to T2.5.

T2.1	Producing research protocol and plan D2.1, summarizing relevant national documentation.
T2.2	Documentary data analysis. In this task, ISU will analyze available reports, journal articles and other literature collected in T2.1 regarding PhD training and related processes, to enable METEOR to demonstrate the need for its program and tailor its outputs appropriately.
T2.3	All partners except SY to carry out interviews and/or focus groups with PhD students, supervisors, doctorate holders and policy actors in their countries. Target:15 participants per country, min. 150 in total.
T2.4	Qualitative data analysis. In Task 2.4 ISU will collect the qualitative material from T2.3
T2.5	Preparation of D2.2: this task is editorial in nature and involves bringing together the document analysis and qualitative studies into a concise report on the state of the art in doctoral education in Europe and elsewhere. We anticipate a report of c.100 pages to encompass a sufficient range of sources.

In the following tasks, primarily existing data will be used: Tasks T2.1, T2.2, and T2.5. The work on the tasks involves analysis of qualitative and available quantitative data related to the functioning of PhD programs and outputs of PhD training in the countries covered by the study. Examples of data used: legal acts, available reports, journal articles, and other literature.

Data will come from publicly available sources - open Internet resources and libraries - as well as from scientific databases accessed by the partners involved (examples: EU OpenAIRE, Google Scholar, JSTOR, ResearchGate, SSRN: Social Science Research Network, EBSCO Academic Search Complete, Scopus, SpringerLink).

Complementary data will be collected through expert interviews conducted with interviews and/or focus groups with PhD students, supervisors, doctorate holders, and policy actors in the countries covered by the study (Task 2.3). The interview scripts have been prepared in such a way as to avoid collection of sensitive personal data. The following data are envisaged to be collected during the interviews or surveys: surname, first name, organization, gender, age/age range, nationality, special educational needs, full-time or part-time employment, email address, field of expertise, datetime of interview, responses to interview questions, type of interview (online or face to face), interviewer. Given the specifics of interviews, researchers may not fully foresee what kinds and scope of information specific persons will intend to share with them. However, it cannot be ruled out that this will include sensitive information, e.g., about health

or mental condition. Therefore, interviews shall be reviewed to check if they include sensitive personal information.

In Task 2.4, ISU will collect the qualitative material from T2.3 to be analyzed using software tools such as NVivo. The personal data collected by each partner will be processed only by this partner and not shared with other consortium members. Each partner will conduct, record, and transcribe the interviews locally, in a local language. Neither voice recording nor raw text of the interviews will be shared with other partners. Instead, partners will develop analytical notes summarizing each of the interviews, which will be the material shared with WP2 Lead and analyzed further. The analytical notes prepared based on the interview transcription will ensure the anonymity of respondents as no identifiable data will be associated with them.

The collected data extracted from the above-mentioned sources will be aggregated to the level of an analytical report describing the functioning of the doctoral education system in Europe (T2.5).

It is envisaged that the interviews conducted by a specific partner will be stored by this partner locally. Should the interviews include personal data of sensitive nature, the partner who collected them is responsible for implementing all technical measures that may be necessary, such as file encryption, if required by the applicable law or regulations binding the partner. Analytical notes are envisaged to be kept on OneDrive with access granted only to individuals directly engaged in the project.

WP3 Training Development

What follows applies to data collected as part of Tasks from T.3.1 to T3.12

T3.1	Develop a training resource (TR) template, D3.1.
T3.2	Develop proposal writing template D3.2, based on extant national and EU templates, and following the widely used three-part structure (Excellence-Impact-Implementation) but simplified to reduce burden on participants whilst maintaining rigor.
T3.3	Develop the METEOR introductory course, Transformative Research TR3a, setting out the aim and objectives of METEOR its procedures, and its relation to the UN SDGs.
T3.4	Develop Intercultural Competence and Inclusion resource TR3b.
T3.5	Develop Collaboration and Teamwork Training Resource TR3c.
T3.6	Develop Supervision and Mentoring Training Resource TR3d
T3.7	Develop Research Proposal Evaluation Training Resource TR3e
T3.8	Develop Research and Innovation Project Design Training Resource TR3f.

T3.9	Develop Impact and Behavioural Change Training Resource TR3g.
T3.10	Develop Project Management and Implementation Training Resource TR3h.
T3.11	Develop Entrepreneurship, Exploitation and Career Development Training Resource TR3i
T3.12	Develop Communication and Dissemination Training Resource TR3j.

Primarily existing data will be used. These will be qualitative data and available quantitative data related to education and included in training materials and relevant academic literature on course developments and transversal skills (intercultural competences and inclusion, collaboration and teamwork training, supervision and mentoring, research proposal evaluation, research and innovation project design, impact and behavioural change, project management and implementation, entrepreneurship, exploitation and career development, communication and dissemination).

Examples of data used: legal acts, training materials, industry studies, policy analysis, and journalistic texts, scientific studies, online courses on transversal skills.

Data will come from publicly available sources - open Internet resources and libraries - as well as from scientific databases accessed by the partners involved (examples: EU OpenAIRE, Google Scholar, JSTOR, ResearchGate, SSRN: Social Science Research Network, EBSCO Academic Search Complete, Scopus, SpringerLink).

The developed training course catalogues will be publicly available and published online on the METEOR website. Access will be given to users after signing up and logging in with a password.

This work package envisages also pilot testing with local students and responses to feedback, as well as providing people with access to training courses. However, these activities envisage that only basic, not sensitive, data will be collected; we envisage it will be name, surname, and e-mail address.

WP 4 Implementation

What follows applies to data collected as part of Tasks T4.1, T4.2, T4.11.

T4.1	Preparation of recruitment and training plan (D4.1), including ethical requirements and data handling protocol based on the DMP from WP1, and introductory material for prospective participants.
T4.2	Recruitment and Induction of participants, using TR3.1a as an introductory resource containing details of expectations and timings. Completed by M9.

T4.11	Preparation of METEOR proposal catalogue, D4.4, including all completed proposals and their evaluations. The ISBN-numbered catalogue will act as a showcase for project ideas and although it will be available on an online, open access basis, participants will retain their IPR should they wish to further develop and exploit their ideas. This task is allocated 34 PD at KU.

The main objective of this work package is preparing 2 summer schools and arranging online participation, as well as reporting on events and evaluating the proposals. The data will be processed mainly for the purpose of tasks T4.1 and T4.2. Each partner will collect the data from its students for recruitment purposes. The following data will be processed: first name, surname, e-mail address, nationality, school name/university, city, program, mode of participation (stationary or remote), passport number, datetime.

In task T4.11, the database of the proposals developed by students as part of summer schools will be created. The intellectual property rights to the proposals written during summer schools will belong to the participants.

The data such as name, surname, e-mail address, school name/university, city, program, mode of participation (stationary or remote), and datetime will be transferred between consortium members, including the partners outside the EU (Georgia, Türkiye, Norway, and the United Kingdom), in order to organise summer schools and support an inclusive and engaging environment for all the participants. Passport number is not expected to be transferred out of the student's country; it shall be used only by the local partner responsible for organizing the student's transport to a summer school.

Data such as passport number, restricted for the given partners, will be stored on OneDrives of those partners. The rest of the data (ordinary personal data) will be stored on the shared OneDrive.

WP5 Policy and Impact

What follows applies to data collected as part of Tasks from T5.2 to T5.10.

T5.2	Participate in project clustering events
T5.3	Design and administer user questionnaires
T5.4	Compile automatically generated data (e.g. statistics, logfile data)
T5.5	Run focus groups at local level
T5.6	Collate evaluation data and document findings, including feedback from partners, to feed into D.5.2 and D5.3

T5.7	Organize participatory, reflective, and deliberative consultation of policy stakeholders in the form of participatory policy workshops (F2F or online). These National workshops will be organized in all partner countries, starting from M19, with preliminary online meetings taking place with stakeholders at earlier stages to ensure commitment and dialogue during the process
T5.8	Organize the first international workshop, which will take place after Summer School One.
T5.9	Using the learning from the first international workshop, the second international workshop will be organized to garner the expertise of policy-makers and stakeholders at European level;
T5.10	Analyse findings from the evaluation of training activities (5.1) and results from the participatory policy workshops (T5.2/ 5.3) to draft the METEOR manifesto and policy recommendations (D5.3)

For the purpose of participation in different online meetings and workshops, the METEOR consortium expects only the basic, not sensitive data to be collected: username, university name, city, datetime needed for registration.

Task T.5.3 will require designing and administering questionnaires/surveys for participants of the workshops/meetings. In this case, also only basic data (name, surname, e-mail address) are expected to be collected. Partners will be responsible for storing their national data and only anonymised data will be shared with the WP5 lead responsible for analysis.

For the purposes of creating project policy briefs, final recommendations, etc., only the primarily existing data and data gained during the earlier stages of the project will be used.

WP 6 Communication, Dissemination, Exploitation (CDE)

Two types of data come under WP6:

1. Personal data of external users for providing functionality (newsletters, event invitations, etc.) and external dissemination, communication, and exploitation activities. The datasets comprise information like surname, first name, organization, email address, role, datetime, etc., that is for the most part collected from the respective users through direct input when registering at the respective websites and confirmed with double opt-in. The datasets shall be stored in an internal restricted repository under the regime of data protection and privacy and will not be made openly available.
2. Statistics related to the performance of communication and dissemination activities, e.g., number of website visits, number of events attended, number of press articles referring to METEOR, number of participants in METEOR events. These statistics will be made available to the Work Package Leaders Group for assessing progress on Dissemination &

Communications actions, published in the updated version of the Dissemination & Communications Plan, and published in the project's final report Deliverable D6.7.

The summary of the personal data processing in specific work packages is included in Annex 1.

3 Data Summary

This section describes specifics of data acquisition, usage and analyses and how data will be made Findable, Accessible, Interoperable and Reusable (FAIR) where possible. Open Science is a major concern of METEOR and will ensure open access to data, being subject to GDPR. All results will be reported as public-level deliverables through METEOR website and through institutional repositories. Scientific publications will be targeted in full open-access journals. All articles about FAIR are publicly available on go-fair.com website. All data generated in METEOR is expected to be readable through generally available tools, such as spreadsheet software, PDF readers and other common office software, preferably open source. Project participants will reuse data (but not personal data) to be able to continue the research after the project is concluded. The raw data will be in text format, while higher level analysis will be saved in .docx and .pptx formats. The data will be generated within the research group and its size will be limited, not exceeding 512 GB.

3.1 Metadata

Metadata describing the data being collected throughout the METEOR project is needed for facilitating open access to the data, making it possible for it to be searched and accessed through adequate search engines. The EUDAT B2SHARE tool has been established as the preferred tool for facilitating adequate licenses for research data. While the final metadata classifiers have not yet been identified, the following propositions are to be reviewed and edited: Scope/subject, Date of dataset generation, Conditions, Parameters, Data type, Variable names, Data version.

Metadata for this project includes file title, short description (i.e., analytical summary about doctoral education), and researchers' ORCID. To align with Open Science and FAIR principles, metadata should include: Author(s)/Data creator(s), Title of the dataset, DOI or persistent identifier (if available), Repository location. README files will be prepared for all the folders. Metadata files will be available in XML format. Metadata will follow DDI standards. Metadata will be shared on an online repository, such as Zenodo or an organization repository. Metadata

will follow conceptual vocabulary from the European Language Social Science Thesaurus (ELSST).

Once data is generated, the list of proposed and used metadata will most likely be adapted in further versions of the DMP..

3.2 Naming conventions

To manage the created number of documents, common rules for file names need to be followed. File names need to comply with the following rules.

Project deliverables are assigned a unique identifier METEOR_[number of Deliverable][date of submission].

All files made publicly available reference METEOR in their name, with the recommendation that the convention METEOR_xxxxxxx[date], where xxxxxxx is a meaningful short description of the file. Files will be named consistently.

File names will be short (< 25 characters); without spaces, using underscores, hyphens, or camel case instead; and avoiding characters like \ / ? : * ” > < | : # % ” { } | ^ [ ] ` ~ æÆ øØ åÅ äÄ öÖ … The international date convention YYYY-MM-DD (e.g. 2017-10-25) will be used.

3.3 Personal or sensitive data

Each partner of the METEOR consortium shall be fully responsible:

- to ensure compliance with the GDPR as well as all laws and regulations applicable to them as it regards personal data processing;
- to implement the appropriate technical and organisational measures in order to secure the accuracy, integrity, and confidentiality of the personal data.

It is expected that personal data will be collected mostly through interviews or surveys (in the Research Part) or during the organisation of the events (in other work packages). Data collected in the Research Part shall then be analyzed and either pseudonymized or anonymized. In case of pseudonymization, encryption should be utilized when it is necessary to separate pseudonym keys from pseudonymized data (e.g., to separate pseudonym lists from transcriptions when both are stored in OneDrive).

All personal data collected by a given project partner shall be stored by this partner using its infrastructure or services compliant with the GDPR and all applicable laws and regulations on personal data processing. All partners use Microsoft OneDrive. As for the Research Part, no

personal data shall be transferred between European Economic Area (EEA) countries and non-EEA countries unless the partners further decide otherwise and provided it is in full compliance with the GDPR and other applicable laws.

As for the other parts of the project, only identification and contact data necessary to complete a given task (e.g., to organise a Summer or Winter school or workshops/meetings/events) should be transferred between the EEA and non-EEA countries, provided the legal requirements have been met (there is an informed consent of a data subject for the transfer of data unless another legal basis for the transfer applies).

No personal, particularly sensitive data is planned to be generated as part of the results (conclusions, analysis) of the METEOR project. Conclusions and analyses coming from the Research Part will be separated from the raw materials. Transcripts will be either pseudonymized or anonymized and in any case will not be shared with other partners. Files with recordings will not be associated with interviewees' personal details, as the interviewee will be assigned a respondent code used in the file name and interview grid. The respondent codebook will be available only to the local partners and not shared with all consortium members. If a partner’s institution or state regulations require encryption, partners will adhere. It is envisaged that the codebook will be stored for at least 5 full years after the conclusion of the project.

Should there be no other applicable legal basis for personal data processing in the non-Research part of the project (or if there is a justified need for consent as a legal basis for personal data processing), the partners should:

ask data subjects to fill out adequate consent forms in conformity with the GDPR and other applicable laws and regulations;

fulfill the informational obligation towards the data subjects under common data protection laws.

All personal data shall be collected and otherwise processed in compliance with the GDPR and all other applicable laws and regulations, including but not limited to the rules of lawfulness, fairness, transparency, purpose limitation, accuracy, minimisation, integrity, and confidentiality.

Any personal data that is going to be shared with another party shall be shared securely if necessary (e.g., this can be done by sharing the data encrypted through OneDrive and sharing the encryption key separately, e.g., via secure email).

3.4 Dataset Summary

The following table summarizes the datasets to be collected, processed, and shared throughout the project's lifecycle. The following table includes only such datasets that do not include personal data. This is a first version of the datasets to be used, but a more extensive list may be developed at later phases of the project.

Datasets including personal data are described in Annex 1.

Table 2 List of datasets

No.	Dataset Name	Source of data	Ownership*	Access Rights
1	EU, national and regional research training policies and PhD programmes Data: curricula designers, legal acts, popular science texts, industry studies, scientific texts, policy analysis, and journalistic texts.	METEOR partner who provides the relevant information	No	Yes
		Other Stakeholders	No	Yes
		Citizens & the Wider Public	No	Yes
2	Open Internet resources and institutional libraries Data: Miscellaneous	METEOR partner personnel	No	Yes
		Citizens & the Wider Public	No	Yes
3	Training courses Data: legal acts, popular science texts, industry studies, scientific texts, policy analysis, and journalistic texts, scientific studies, online training materials.	METEOR Partner	No	Yes
		Wider public	No	Yes
4	Data from Dissemination Activities Data: number of website visits, number of events attended, number of press articles referring to METEOR, number of participants in METEOR events	Work Package Leaders Group	Yes	Yes
		Other METEOR partners & wider public	No	Yes

Open Science principles of transparency and accountability: The author(s)/creator(s) of a dataset are the individuals who collected, curated, or generated the data.

Authors deserve academic credit and should be cited when the dataset is used. Owners (often institutions, funders, or organizations) can set terms for access, sharing, and licensing (e.g., Creative Commons, proprietary restrictions).

3.5 FAIR

3.5.1 Making Data Findable

All data will have an associated metadata document defined by R1 article of FAIR principles available on the aforementioned website; described metadata will be adequately extensive, indexed or registered, and searchable. Metadata will follow DDI standard. Data will be assigned with DOI while using a repository such as Zenodo or organisation repository. Data are subject to individual evaluation to determine their suitability for public access for interested parties outside the project after its completion.

3.5.2 Making data Accessible; Access management

All metadata will be retrievable by their DOI identifier and accessible even after the predicted duration of data availability has expired through a trusted repository. No tracking of people accessing the data is planned, although access to the METEOR project's virtual internet drive and repositories will be provided individually for each user, applying adequately strict encryption if required, policy of access, and backup schedule, which will be overseen by designated project participants. For encryption, standard in-build Microsoft software or other GDPR-compliant software or services may be used.

3.5.3 Making data Interoperable

Data and metadata will use a formal, accessible, and applicable language for knowledge representation, including usage of adequate vocabulary and qualified references to other metadata. Documents will be written in English and will be using established standard terminologies; variables and value names will be constructed following general data processing conventions adequate to the subject researched. Research data can be exported into different file types which will be defined once known which data will be available. While knowing that not every dataset collected/generated during the project duration will be public, many datasets

will be kept confidential and will not be available for access or interoperability. Datasets intended to be public shall use non-proprietary data file formats to ensure interoperability.

3.5.4 Making data reusable; Data expiration date

Metadata will be described with accurate and relevant attributes to enable their easier retrieval and usage, will be released with clear data usage license, and will be meeting domain-relevant community standards. The predicted expiration date for data access is set to 5 years from the publication date. Data will be properly archived after the duration of the project, ensuring its persistence regardless of cloud hosting services. Ownership of datasets will belong to the project consortium after the project completion. Suitable CC license will be used for secondary data and CC0 for open data. These relevant attributes will be informed for partners to be able to complete their datasets accordingly.

3.5.5 Data Security Guidelines

METEOR Partners are responsible for the data regarding conducting research concerned by EC-GA and will ensure best practice concerning the storage, transfer and distribution of data, included but not limited to:

1. Usage of strong passwords and access keys for access to project platforms;
2. Usage of encryption and up-to-date security protocols and software for project work;
3. Maintaining awareness of phishing, extortion attempts and other malpractice;
4. Refraining from using public networks for project work;
5. Maintaining regular backups of project research and other data;
6. Reporting eventual data breaches to adequate bodies;
7. Monitoring data logs in case of detecting unusual and possibly dangerous activity;
8. Ensuring compliance with data protection law.

4 Allocation of Resources

4.1 Cost for making data FAIR

Monetary cost for making data FAIR is estimated to be zero, and the personnel time costs are included in the workstreams for the project. Consortium partners will use their own budgets as necessary to archive personal data in their own repositories.

4.2 Responsibilities for data management

The data management coordinator is the project leader - CASE. The data management coordinator will be responsible for any updates to the DMP during the life cycle of the project. The Project Coordinator is co-responsible for overall coordination and supervision. Furthermore, consortium partners have the responsibility to make sure their activities are in line with all applicable local, national government, and international laws.

5 Ethical Aspects

In the data collection process, special attention will be given to thoroughly informing the participants and providing them a fair chance to deliberate whether they want to participate in providing data for the research activities. The participants will be given a chance to opt out of the process. The involvement of vulnerable participants in the data collection process is currently not foreseen; this will be a pre-requisite for the partners not to interview these people. The strategy for handling unintended findings that may have serious consequences will be discussed within the Consortium and will be handled with maximum care.

Ethical approvals, if required, have to be in place before data collection begins.

The ethics issues are defined in point 4 (p. 37) of the METEOR application included in the Grant Agreement.

6 Secure storage of data practices by METEOR partners

This section summarizes the data storage practices of METEOR partners. Most of them contribute to more than one WP, so this section provides an overview while minimizing repetition. CASE uses One Drive as part of Microsoft 365 (plan for educational institutions). The One Drive for Business service is provided by Microsoft, which is a recognized provider of software and cloud services for office work, remote communication, and data storage. Microsoft declares that it supports compliance with the GDPR requirements as well as helps customers ensure privacy and security. In the case of any project (including METEOR), team members access ODcloud through their institutional emails that are password protected. Protection of the data is then ensured by the external service. The data is stored in two centres; if one collapses, it is replaced by the other. In the event of system failure, lost data from the

previous two weeks can be restored, while data going back three months can be restored if it was deleted individually.

Other partners also use One Drive as part of Microsoft 365 (plan for educational institutions). In case any of the partners uses other infrastructure or software as a service (SaaS) than mentioned above, they should notify the rest of consortium members to verify if such infrastructure or SaaS meet all the criteria under GDPR and other applicable laws and regulations. In some cases (special categories of personal data or confidential information), storage of data may require encryption with encryption software, e.g., with Cryptomator, or otherwise, data should be stored in a sufficiently secure service. In some cases, voice and video recordings may be performed only with designated tools and software that comply with GDPR requirements, ensuring appropriate security measures and lawful processing. Anonymized data, after verification that re-identification is not possible, is treated as open data. Pseudonymous data is personal data.

The partners shall notify each other at due time and with proper advance about any specific requirements they are obliged to follow under their local legislation or regulations concerning personal data. The partners should consult and make mutual decisions about any issues, including but not limited to the selection of technical and organisational means of personal data processing, that may appear during their cooperation.

Annex 1: Overview of envisaged personal data processing at the level of the individual work packages

WP number	requiring	Data type	Data specifics	subjects / who	Personal Data			Who	processes	data collected? (By		the	the personal data?	
					data	*personal*	*categories*			*EEA*	*EEA*		*Inside EEA*	*EEA*
1	communication	mails, other),	name,	personnel and	–	☑	–	members	members	☑	☑	members	☑	☑
2	interviews*	transcripts	name,	students and	–	☑	interview	members	Meteor	☑	collected by	infrastructur	–	–
note /	conducted by	analytical notes		will not include	☑	–	–	members	members	notes will be	notes will be	notes may	Meteor	Meteor
	pilot testing	analytics	name,	students /	–	☑	–	members	Meteor	☑	–	infrastructur	Meteor	–
3	training courses	analytics	name,	students /	–	☑	–	members	Meteor	☑	–	infrastructur	Meteor	–
4	summer schools	documents	surname, e-mail	participants	–	☑	–	members	members	☑	☑	personal	☑	☑
5	ngs and	documents	university name,	gs participants	–	☑	–	members	Meteor	☑	–	infrastructur	☑	–
	project website	analytical data	surname, e-mail	website who use	-	☑	-	members	member in	☑	-	infrastructur	☑	-
	newsletters	documents	address	participants	–	☑	–	members	member in	☑	–	infrastructur	☑	–
	event invitations	documents	address	participants	-	☑	–	members	Meteor	☑	–	infrastructur	☑	member
6	dissemination,	documents	e-mail address	Meteor members	-	☑	–	members	members	☑	☑	containing	☑	☑