



RESKILLING

Deliverable D1.3 Data Management Plan

Grant Agreement no.: 101147328
Project acronym: RESKILLING
Project title: Research initiative for Enhancing and Adapting Workforce SKILLs for Implementing TraNsport Automation with Employment Growth
Project coordinator name and organisation:
Matina Loukea, Centre for Research and Technology Hellas (CERTH)



Funded by
the European Union

This project has received funding from the European Commission under the European Union's Horizon Europe research and innovation programme under grant agreement No. 101147328

This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI) for the Swiss partners

Document Details	
Document identifier	Data Management Plan
Due Date of Delivery	30 June 2025
Actual Date of Delivery to EC	30 June 2025
Task Number	Task 1.4
Dissemination level	Public

Contributors
Ingrid Skogsmo (VTI, Sweden), Matina Loukea (CERTH, Greece), Katerina Toulou (CERTH, Greece), Fabienne-Agnes Baumann (VDI/VDE, Germany), Giuseppe Garofalo (ECTRI, Belgium), Maja Fojud (EURNEX, Germany)

Reviewers
Evangelos Beckiaris (CERTH, Greece), Manon Coyne (POLIS, Belgium), Teresa De la Cruz Eiriz (ZLC, Spain), Evy Rombaut (VUB, Belgium), Caroline Alm��ras (ECTRI, Belgium). Marc Zinkel (Beceptum, Germany).

Disclaimer

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission European Climate, Infrastructure and Environment Executive Agency (CINEA). The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use, which may be made of the information contained therein.

Control Sheet			
Version	Date	Editor	Summary
1.0	30/06/2025	Ingrid Skogsmo (VTI, Sweden)	First submission of deliverable

List of Acronyms	
Acronym	Definition
CCAM	Cooperative, Connected, Automated Mobility
CO	Confidential (Level of confidentiality)
D	Deliverable
DMP	Data Management Plan
DPO	Data Protection Officer
DPIA	Data Privacy Impact Assessment
FAIR	Findable, Accessible, Interoperable, Reusable
FP7	Framework Programme 7 (Horizon 2020)
GDPR	General Data Privacy Regulation
M	Month
PU	Public (Level of confidentiality)
RE	Restricted (Level of confidentiality)
WP	Work Package

Table of Contents

Executive Summary	6
1. Introduction	7
1.1. Purpose of the document	7
1.2. Intended Audience	8
1.3. Interrelations	8
2. Data in RESKILLING - Generation and Use	9
2.1. Types of data.....	9
2.2. Data description	13
2.2.1. Metadata	14
2.3. FAIR Data	15
2.4. Open Access principle	16
3. Data sharing and access	18
3.1. Confidentiality.....	18
3.2. Data storage.....	18
3.3. Data ownership	18
3.4. Data Sharing and Re-use.....	19
3.5. Data/meta-data repository (RESKILLING databases)	19
3.6. Data Preservation.....	20
3.7. Data Security.....	20
3.8. Internal record keeping	22
4. Data management obligations	24
4.1. Research consent	24
4.2. Privacy by design	24
5. Data Privacy Impact Assessment	25
6. Conclusions and next steps	26
Annex 1 Data processing - record keeping template	27
Annex 2 Data Privacy Impact Assessment (DPIA) template	30
Annex 3 Privacy Policy for project website	34

List of Figures

Figure 1. Schematic view of data in the RESKILLING project 12

List of Tables

Table 1 Examples of data that will be collected, used, generated in RESKILLING WPs10
Table 2: Dataset Description Template 13
Table 3 Data documentation matrix 14
Table 4 Dissemination levels of RESKILLING project data..... 18

Executive Summary

This deliverable is the first version of the Data Management Plan (DMP) elaborated within the RESKILLING project, referring to what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved.

The RESKILLING Data Management Plan refers to the latest EC DMP guidelines. Data that will be produced within the project lifecycle shall be Findable, Accessible, Interoperable and Reusable (FAIR). It outlines the types of data that will be collected, processed or generated, the methodologies and standards to be applied, the conditions under which the data will be shared and/or made openly accessible, and the measures for data curation and long-term preservation.

It should be noted that the DMP – 1st version, is a Deliverable in M6 (Month 6) of the project and will be a living document and it will evolve during the project lifespan according to the progress of project activities, capable to capture and reflect the evolution in the form of dataset updates and/or changes in Consortium policies to be reflected in Deliverables D1.4 DMP – update (M18), and D1.5 – final update (M36).

1. Introduction

The Horizon Europe project RESKILLING entails multiple data collection streams to support its multi-layered implementation, validation, and evaluation activities. These streams include, but are not limited to, the organisation of surveys, interviews, and workshops, the execution of project-related case studies, and the analysis and assessment of project outcomes. In several instances, the collection and processing of personal data will be necessary to fulfil the research objectives.

All personal data processing activities will strictly adhere to established anonymisation and data protection principles and will comply with the relevant legal and ethical frameworks, including:

- a) the **General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679**,
- b) the **Universal Declaration of Human Rights** and the **Council of Europe Convention 108** for the Protection of Individuals with regard to Automatic Processing of Personal Data, and
- c) all **applicable national legislation** implementing these frameworks, particularly in relation to informed consent procedures and lawful processing grounds.

Moreover, the project is committed to the **open science principles** promoted by Horizon Europe. Research data collected and/or generated during the course of RESKILLING will, in principle, be made openly accessible via **certified open repositories**, unless restrictions apply due to privacy, confidentiality, or security concerns. Appropriate metadata will accompany all datasets to ensure discoverability, reuse, and long-term preservation.

1.1. Purpose of the document

The purpose of the present deliverable D1.3 Data Management Plan, first version (“DMP” in the following) is to provide a comprehensive overview of the data-related activities within the project. Specifically, detailing the main dimensions and characteristics of the data the project will collect, process and generate, including details on the content, type, format, and expected volume of the data.

Furthermore, the DMP describes the standards and methodologies will be applied for data collection, processing, documentation, and long-term management, addressing also how the project will ensure that all data is managed (exploited, shared, and preserved beyond the project’s lifetime) in accordance with the **FAIR principles—Findability, Accessibility, Interoperability, and Reusability..** In addition, this deliverable sets out the project’s approach to data protection and privacy, including compliance with relevant legal and ethical frameworks, particularly the **General Data Protection Regulation (GDPR)**.

It furthermore identifies open-access features of the project’s data and specifies the security measures that will be implemented to prevent unauthorized access to both personal data and data-processing infrastructure. It details the application of anonymisation and pseudonymisation techniques and outlines the informed consent procedures that will be followed for data processing in compliance with the GDPR and relevant national legislation.

It also includes provisions for storage, maintenance and management of access to data, ensuring both the integrity and availability of data during and after the project’s implementation.

1.2. Intended Audience

The intended audience of the RESKILLING project's DMP includes both internal and external stakeholders involved in or impacted by the project's activities. Internally, the DMP is primarily addressed to the project partners to guide them in the responsible handling of data throughout the project's lifecycle.

Externally, the DMP targets participants and stakeholders involved in project activities, including, but not being limited to operators, municipalities, authorities, users of mobility ("citizens"), agencies and organisations dealing with employment, labour market, growth and innovation; persons working in the transportation and digital sectors, educators, "job providers" (industry, SME), policymakers, citizens, mobility service users etc.

Moreover, the DMP is designed to serve the scientific community (research and academia) with an emphasis on researchers in the areas of training and skills development, labour economics and inclusive growth, intelligent transport systems, urban and transport planning, and automotive engineering, and standardisation.

By providing transparent information on the project's data governance, the DMP contributes to knowledge sharing, reproducibility, and alignment with open science principles.

1.3. Interrelations

Data of various types will be generated, collected, and processed across all Work Packages (WP) of the RESKILLING project, with each contributing to and relying on specific datasets to fulfil its objectives.. Several partners will be directly involved in data gathering activities, while others will process and utilise data outputs from preceding or parallel WPs.

In particular, WP2 will conduct stakeholder mapping, generating datasets that will inform the design and implementation of activities in WPs 3 to 6. These data will serve as key input in the development of the project's use cases, as well as in the assessment of effects and socio-economic impacts in WP3.

Within WP3, reviews and analyses of surveys will be performed and existing data in literature and online will provide input to development of training modules, the creation of scenarios, the setup of the RESKILLING's CCAM Employment & Skills Observatory and the definition of project's case studies in WP4.

WP4 in turn leads the development of the Business Model ToolKit and of the CCAM Employment & Skills Observatory, making use of data outputs from WPs 2, 3 and 5. WP4 will also involve iterative creation and testing of content, requiring structured data capture at different phases.

WP5 will use and analyse data from WP2 and outcomes from WPs3 and 4, in order to formulate evidence-based policy recommendations and a strategic roadmap for supporting the socio-economic transition to CCAM.

WP6 relies on input and actions from all other WPs to create content and make use of it for dissemination, communication, stakeholder engagement, and exploitation, ensuring coherent and impact-driven outreach activities. Throughout the development phase of project outputs — -such as tools, models, trainings, use cases, scenarios, recommendations and case studies - data

from the WPs will be generated and iteratively refined at different stages, including data produced in the case studies and user feedback loops, all of which will be systematically documented and governed in alignment with the project's data management and FAIR principles.

2.Data in RESKILLING - Generation and Use

For RESKILLING to achieve its mission and to meet its objectives, a series of data is required to be collected, created, processed, used and managed. Data collection and processing in RESKILLING adheres to the respective European regulations, encompassing a) the General Data Privacy Regulation (GDPR) (EU) 2016/679), b) the Universal Declaration of Human Rights and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and c) the national laws applying its provisions, including those governing the acquisition of valid consent.

The following sections provide a detailed overview of the types of data to be collected, generated, and processed within the RESKILLING project, along with the corresponding methodologies for their handling.

2.1. Types of data

RESKILLING's activities will collect, generate, use and manage various types of data, which may be generalised into four main categories:

- **Management data:** i.e. data related to the management of the project and project related events. This includes e.g. reporting data and budget figures.

Personal data: Individuals play a key role to RESKILLING activities, and will be involved across various activities and phases, including participation in the Stakeholder Community, the Advisory Board, the co-creation activities, case studies, and as end-users of different tools being developed within the project (e.g. the CCAM Employment & Skills Observatory).

Personal data to be collected or processed may include, but is not limited to:

- **Contact details** (e.g., name, email address, professional affiliation, phone number)
- **Demographic information** (e.g., age group, gender, occupation, region)
- **Professional profiles and roles** (e.g., expertise area, employment status, sectoral affiliation)
- **Recorded opinions and feedback** provided during surveys, interviews, focus groups, or interactive sessions

In addition, personal data also pertains to project partner staff, primarily for internal coordination purposes. This may include information shared through mailing lists, communication tools, project management platforms, and attendance logs for project meetings and events.

- **“Research Data” or “Content”:** Work undertaken in the WPs will not only use data as input to support the development of key outcomes but will also **generate new datasets** as part of the results..

For example, WP2 and WP3 undertake stakeholder and contextual mappings, which involve identifying, collecting, analysing, and enriching data from various primary and secondary sources. The final outputs of these activities—structured mappings and analytical frameworks—will themselves be considered project-generated datasets.

Comparable processes will occur in WPs 4 to 6, where data will be both used and produced through the development of training content, business models, scenario analyses, case studies, and communication outputs. These outputs will contribute to the broader project knowledge base and, where appropriate, be shared openly in accordance with the project's **Open Science** and **FAIR data** principles.

- **Data generated when using RESKILLING outputs:** RESKILLING “outputs” here signifies project results such as Training modules, developed in WP4, or the CCAM Employment & Skills Observatory. When applying these outputs, the users will generate results for their own further use. That use of a certain output may also generate some subjective user feedbacks, e.g. usefulness and handling. Furthermore, data that can be used to assess the output’s functionality is also generated.

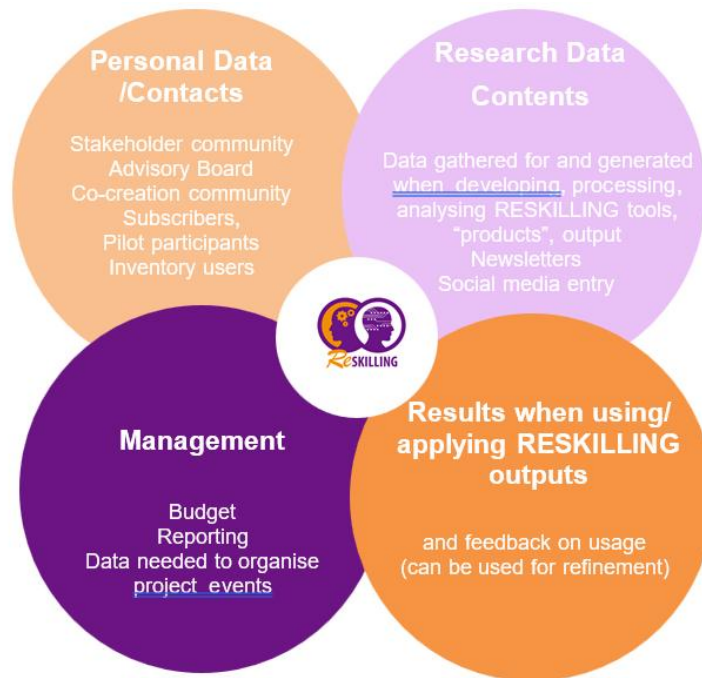
Indicative examples of data that will be collected, used and generated in all RESKILLING WP’s are shown in Table 1, that will be updated and revised as needed in the DMP iterations (D1.4 at M18 and D1.5 at M36) . Figure 1 provides a schematic overview of the data categories.

Table 1 Examples of data that will be collected, used, generated in RESKILLING WPs

	Management data	Personal / Contact data, Subjective data	Research data / Content	Data generated when using RESKILLING outputs tools
WP1 Project management	Budget, Reporting, Administrative data	Internal mailing lists		
WP2 Stakeholder community		Stakeholders, Advisory Board	Mapping, Engagement activity (e.g. survey) processing and results	
WP3 Employment & Socioeconomic effects of CCAM			Mapping, Developing, analysing, processing, Results	
WP4 Towards job creation, growth and innovation		Co-creation community Pilot participants, stakeholders	Business models & schemes development, processing	Results from using business models and schemes
			Training modules development	Results from use of training modules
			Case studies realisation relevant information from different organisations and stakeholders., development iterations	
			Information for CCAM Employment & Skills Observatory personalised outputs,	Personalised recommendations and information on CCAM-related employment effects Feedback data

	Management data	Personal / Contact data, Subjective data	Research data / Content	Data generated when using RESKILLING outputs tools
				(for iterative enhancement)
			Interview data (transcripts, notes) Workshop documentation	
WP5 Impact Assessment & Roadmap		Co-creation community	Data gathered for developing Impact assessment, processing	
			Roadmap, Guidelines and policy recommendations	Material produced when applying guidelines and recommendations
WP6 Communication, Dissemination & Exploitation strategy		Subscribers, participants	Penetration, followers, “clicks” downloads, subscriptions etc	
Dissemination tools and events		Participants	Log of events, Log of publications	
RESKILLING inventory		Inventory users	Data gathered for development of inventory, processing	Results of using and applying inventory
Exploitation activities	Event management	Participants in activities	Evaluation data	

Figure 1. Schematic view of data in the RESKILLING project



Within the RESKILLING project, it is essential to clearly distinguish between data intended for public dissemination and data that is considered sensitive, requiring restricted access and enhanced protection measures.

- **Publicly available data (Project Outputs):** The majority of project results—such as the *RESKILLING Inventory*, the *CCAM Employment & Skills Observatory* (to a certain extent), *Training Modules* (partially), the *Business Model Toolkit*, *Guidelines and Policy Recommendations*, and the *Strategic Roadmap*—are designed to be openly accessible to stakeholders, end users, and the broader public. This approach aligns with the principles of Open Science and adheres to the FAIR data principles. Data generated for these outputs will be managed in accordance with the principle of being *as open as possible, as closed as necessary*.
- **Sensitive Personal Data (Privacy-related):** Sensitive data in terms of privacy will include all data related to contact information, which has to be registered and processed regarding the GDPR European legislation. The project contact database, containing sensitive information and will be considered “confidential” according to ISO 27001 standards on information security and will only be accessible to the RESKILLING Consortium members. The same data protection measures will also apply to sensitive data that may be generated when using and applying RESKILLING tools.
- **Output-generated and technical data (Non-Personal):** Usage of RESKILLING outputs and tools may furthermore generate non-personal data, that relates to the tools’ performance metrics, user interaction statistics, or technical logs. Although such data is not classified as personal under GDPR, it may contain **project-sensitive insights** and thus will be treated as “**restricted**”—accessible only by authorised personnel within the consortium, in alignment with ISO/IEC 27001. While this data is not intended for public dissemination, aggregated or anonymised versions may be used for evaluation or reporting purposes, where appropriate.

2.2. Data description

This section presents a preliminary description of the datasets that will be collected, generated and managed in RESKILLING. Datasets refer to the file extension of the data, and in RESKILLING the following types are foreseen to be handled:

- Reports (in the form of word or pdf documents)
- Protocols and other documentation created during workshops
- Excel files with raw data, surveys etc.
- Web, audio and video recordings
- Database

The RESKILLING project will produce different categories of datasets:

- Context data: data that describe the context of an experiment.
- Acquired and derived data: data that contain all the collected information related to an experiment.
- Subjective data: from e.g. questionnaires, surveys, personal and group interviews,
- Raw/unprocessed data: data collected directly from the source (either objective or subjective).
- Metadata: descriptions of data that will facilitate the data analysis and data pre- processing.
- Aggregated data: data summary obtained by reduction of acquired data and generally used for data analysis.

As the nature and extent of datasets can evolve during the project, the initial data descriptions presented in this deliverable will be reviewed and updated in the M18 version of the DMP (D1.4). The DMP will be a living document, continuously enriched and revised throughout the project lifecycle to reflect emerging data and updated management practices. To support this process, a draft data description template has been developed (Table 2). This template will be used to describe the different datasets, including their reference, file format, standards, methodologies and metadata and repository to be used.

Table 2: Dataset Description Template

Dataset Reference	RESKILLING_WPX_TX.X_XX Each dataset will have a reference that will be generated by the combination of the name of the project, the Work Package and Task in which it is generated
Collected / Created	
Dataset name	Name of the data/metadata/exploitable result
Dataset description	Description of the data/metadata – of the information you will collect/create including data provenance, origin and how it will be used, by whom. If re-using existing data, make reference to the data and how/from where they were retrieved.
Standards and metadata	A list of metadata attributes The used methodologies
Dataset type	(see above)
File format	All the format that defines data (file extension e.g. docx, txt, etc; or prototype)
Data size	State the expected size of the data in MB/GB
Owner	Partner name / Consortium / External stakeholder
Privacy level	Public / Consortium / Partner/ etc.
Repository during the	Provide an Open access repository / partner storage (private

Dataset Reference	RESKILLING_WPX_TX.X_XX Each dataset will have a reference that will be generated by the combination of the name of the project, the Work Package and Task in which it is generated
project (for private/public access)	cloud/private drop box)/etc.
Data Sharing	Explanation of the sharing policies related to the dataset between the next options: Open: Open for public disposal Embargo: It will become public when the embargo period applied by the publisher is over. In case it is categorized as embargo the end date of the embargo period must be written in DD/MM/YYYY format. Restricted: Only for project internal use. Each dataset must have its distribution license. Provide information about personal data and mention if the data is anonymised or not. Inform if the dataset entails personal data and how this issue is taken into account.
Back-up frequency	How often will it be made? Daily/monthly/yearly/once
Duration of preservation (in years)	Number of years
Archiving and Preservation	The preservation guarantee and the data storage during and after the project (for example : databases, institutional repositories, public repositories ...) Open access repository/partner storage (private cloud / private drop box) etc., or destroyed after end of project
Link to dataset	URL link to actual dataset with the same filename (if Open).

2.2.1. Metadata

The role of metadata is to accompany all datasets to ensure they can be accessed, understood, and effectively used by parties beyond the original data collectors. External users and analysts have to understand any underlying processes in order to understand the data and to be able to re-use them.

In RESKILLING different types of data are handled in the project activities, and therefore the level of detail in metadata can vary between “basic” and “advanced” level.

Basic: details defining the origin, the type, the creation dates and the way these data were created.

Advanced: include definitions of variables, the methods used and applied in order to gather and capture data based on common standards (incl. any procedural steps taken). A detailed and technical specification of data might be included like the variables that define the specific dataset, the units of measurements and the assumptions applied for the data collection (e.g. zero might mean no activity recorded, therefore the person is not active). The format and file types used for collecting and storing the data (and size) can be of help if external users show interest in re-using a dataset (i.e. checking compatibility with s/w they use in order to aggregate or analyse data utilise import/export functionalities).

Initial documentation details for these levels are presented in Table 3 below.

Table 3 Data documentation matrix

Basic	Source 1	Source 2	Source n	Advanced
Data name				Definition of variables
Who created/contributed to data				Vocabularies
Date created				Units of Measurement
Data modified				File format and type
Conditions				Methods used/assumptions made/analytical procedural info; description

2.3. FAIR Data

The data that will be generated within the RESKILLING project will be included in an open access repository that will be consistent with all the be 'FAIR' principles. These requirements do not affect implementation choices or necessarily suggest any specific technology, standard, or implementation solution. RESKILLING will apply the FAIR principles as follows:

Making data findable, including provisions for metadata

- The datasets will have rich metadata to facilitate the findability.
- All the datasets will have a Digital Object Identifier provided by the RESKILLING public repository (ZENODO)
- The reference used for the dataset will follow this format: RESKILLING_WPX_AX.X_XX, including clear indication of the related WP, activity and version of the dataset.
- The metadata will be defined in the "Standards and metadata" section of the dataset description Table 2.

For data to be made openly available in RESKILLING, according to the FAIR principle, special care should be applied to provide appropriate metadata for any entry to the storage of data for open access.

Making data openly accessible

- Datasets openly available are marked as "Open" in the "Data Sharing" section of the dataset description table (see Table 1).
- The repository that each dataset is stored in, including Open access datasets, is mentioned in the "Archiving and Preservation" section of the dataset description table (see Table 1).

ZENODO will be one of the considered options.

- “Data sharing” section of the dataset description table (see Table 1) will also include information with respect to the methods or software used to access the data of each dataset.
- Data and their associated metadata will be deposited either in a public repository or in an institutional repository.
- “Data sharing” section of the dataset description table (see Table 1) will outline the rules to access the data if restrictions exist.

Making data interoperable

- Metadata vocabularies, standards and methodologies will depend on the repository to be hosted (incl. public, institutional, etc.) and will be provided in the “Standards and metadata” section of the dataset description table (see Table 1).

Increase data re-use (through clarifying licenses)

- All the data producers will license their data to allow the widest reuse possible. More details about license types and rules will be provided in the final version of the DMP.
- “Data Sharing” section of the dataset description table (see Table 1) is the field where the data sharing policy of each dataset is defined. Data available for use are subsequently available for future re-use. If any constraints exist, an “embargo period” will be set or “restricting flag” will be explicitly raised in this section of Table 1.
- The data producers will make their data available for third parties within public repositories only for scientific publications validation purposes.

All datasets will be maintained for the entire duration of the project as well as for two additional years after its conclusion. After the project ends, all datasets will be stored in a centralised facility to minimise maintenance costs. Datasets with acknowledged long-term value may be kept for a longer period, as indicated in the “Archiving and preservation” section in Table 2. The long-term value of a dataset will be decided according to the exploitation plan as well as its relation to a scientific publication.

For the period in which the data will be available for open access, no restrictions will be imposed on their access. In case IPR protected or proprietary data will be generated or made available as background assets in the context of the project by one or more beneficiaries, access to this data will be treated in accordance with the rules and regulations foreseen in the project Consortium Agreement. For all this data, access will be granted only to authorised users. This access is granted by the Coordinator.

All data to be available as open data will undergo a quality assurance process. Each partner in charge follows specific procedures to assure the quality of the data and conformance to standards as referred to each dataset’s description in section 2.2. Additional peer-reviews will take place in case of publication in Journals.

2.4. Open Access principle

RESKILLING will ensure open access to all peer-reviewed scientific publications relating to its results and will provide access to the research data needed to validate the results presented in deposited scientific publications. Publications and research data made available to third parties will not contain any personal information.

The RESKILLING Consortium will make public Deliverables and publications available with Open access in ZENODO, which is a free service developed by CERN under the EU FP7 project OpenAIREplus (Grant Agreement no.283595), under a dedicated account for RESKILLING. Under the same account, all the research derived datasets that will emerge in the project and that will be decided to be **Open** for sharing by the Consortium will be shared. By the end of the project, this process will be completed. If data are shared, they will be in an easily accessible and re-usable format (e.g. csv), wherever this is feasible and possible to ensure that the data are accessed with open-access tools and software.

The following lists the minimum metadata fields that should label any RESKILLING project-generated scientific publication in a repository:

- The terms: “European Union (EU)”, “Horizon Europe”
- Name of the action (Research and Innovation Action)
- Acronym and grant number (RESKILLING, GRANT NO. 101147328)
- Publication date, name and authors
- Length of embargo period if applicable
- Persistent identifier

When referencing Open access data, RESKILLING will include as a minimum the following statement demonstrating EU support (with relevant information included into the repository metadata):

“RESKILLING is funded by the European Union within Horizon Europe research and innovation programme under grant agreement No. 101147328”.

In regards to the specific repositories available to the RESKILLING consortium, numerous project partners maintain institutional repositories that will be listed in the next DMP version (Deliverable D1.4), where project scientific publications and, in some instances, research data will be deposited. The use of a specific repository will depend primarily on the primary creator of the publication and on the data in question.

Some other project partners will not operate publically accessible institutional repositories. When depositing scientific publications they shall use either a domain specific repository or use the EU recommended service OpenAIRE (<http://www.openaire.eu>) as an initial step to finding resources to determine relevant repositories.

The RESKILLING Consortium will strive to open as many datasets as it is feasible and agreed by its Consortium members and data owners. When this is not the case, it will be justified with the note in the data sharing field of this dataset stating the reasons for the applied restrictions.

¹ http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/open-access_en.htm

3.Data sharing and access

3.1. Confidentiality

RESKILLING will produce data with different levels of confidentiality – which is summed up in **Error! Reference source not found..**

Table 4 Dissemination levels of RESKILLING project data

Level of Confidentiality	
PU	Public
RE	Restricted to a group specified by the consortium
CO	Confidential, only for members of the Consortium

3.2. Data storage

Data will be stored in secure areas (physical, network, cloud-based). Data to be shared for analysis will not include any personal or identification data. Personal data cannot be shared with external databases for further (re-)use. For example, Dropbox cannot be used.

Data collection, storing, accessing, and sharing abide to the international legislation and guidelines.

All datasets will be password protected. Each dataset will need to have one or more identified dataset owners, i.e. named individual(s), which have full access (read, write, update, delete). Other individuals who want to use/reuse the dataset will be able to read and download but not make any changes or modifications to the specific dataset.

In RESKILLING several use cases and case studies will be undertaken, leading to collection and generation of various types of data. At the start of such an activity an assessment of the datasets will be done with respect to access and storage. These details will be included in the upcoming versions of this present DMP (D1.4, M18 and D1.5 M36).

The RESKILLING SharePoint area has been put in place by the Swedish National Road and Transport Institute (VTI) and constitutes a platform for data sharing and information management within the consortium. As a general principle data will be stored on RESKILLING's Sharepoint. Material in the SharePoint area is stored in the cloud. Backup is built-in and data is retained for 120 days. VTI obtains data from the cloud on a daily basis, stores it on disk for 2 years, and makes daily backups.

3.3. Data ownership

Any data gathered during the lifetime of the project are under the ownership of the beneficiary or the beneficiaries (joint ownership) that produce them according to Art. 16, in Annex 5 of the signed Grant Agreement. The beneficiaries have the intellectual property rights of the data they collect

and re-use of data is defined by the limitation they might set in how they will make data available. This means partners decide if they make their data freely and openly available to the research community (no additional restrictions on access to data or publications) or there is an embargo period, whereby permission for accessing the data is given after a certain period of time. As datasets have not been formed yet this information will be available in the updated version of this deliverable.

3.4. Data Sharing and Re-use

All publication resulting by work performed within a project must be in open- access journals.

The target is to maximize the impact on scientific excellence through result publication in open access yet highly appreciated journals, without releasing any confidential information that could potentially violate the security nature of the project.

The RESKILLING consortium will strive to make many of the collected datasets open access. When this is not the case, the data sharing section for that particular dataset will describe why access has been restricted.

Data re-use by external researchers and other stakeholder groups will be feasible for selected datasets. The embargo period will be at least the duration of the project, as partners would like to easily manage the data whilst collection, analysis and reporting is ongoing. Sharing and-reuse will be applied in the central database according to data depositor's preferences and suggestions.

3.5. Data/meta-data repository (RESKILLING databases)

RESKILLING will use a trusted repository for its databases. Open access to the deposited data will be granted according to details in the Grant Agreement Annex 5, article 16.

Each partner creating a dataset will also be responsible for their upload to the central database to allocated space. An agreement will be reached between the administrator and the data responsible about the level of sharing between the partner (depositor) and the administrator (and the rest of the Consortium), defining the terms and conditions of use for the specific dataset. Embargo, if any, is set by the owners.

The database's requirements and specifications (e.g. s/w, standards, guidelines, etc.) are still to be decided. First, it is essential to identify and categorise any inherent restrictions in datasets because of the services or applications they are generated from. In addition, indirect restrictions might apply related to s/w developed for work to be carried out by a specific partner (e.g. in-house s/w, tools, etc.). There might be license or operating restrictions that should be considered (e.g. compatibility and access only with certain h/w or s/w).

3.6. Data Preservation

Data will be preserved in the database after the end of the project (for a period of two years) for those datasets that partners have agreed to share with other researchers.

3.7. Data Security

The data collected in RESKILLING will be stored internally in a data repository provided by VTI (Microsoft SharePoint). VTI runs a daily back-up of documents, and Sharepoint backups are stored on disk for two years. In the event of failure, full restoration is initiated from the most recent verified backup. Such recovery events are logged, and lessons learned are reviewed in periodic data management updates.

The external open data will be stored in the public repository ZENODO, hosted by CERN.

Data security for all documents uploaded to the internal data storage (on Sharepoint relies on the security measures put in place by Sharepoint.

RESKILLING will provide security mechanisms and management procedures so as to a) ensure personal (sensitive) data protection through a strict process of data collection and anonymisation, and b) guarantee data integrity and reliability, ensuring system's high performance operation through the exchange of the necessary information.

The consortium research partners will always fully comply with all applicable data protection legislation and regulation during this project, to ensure the security and protection of individuals' personal information in relation to this project.

In terms of **personal data protection**, personal data will be anonymised and strictly used for the project's purposes. Before collecting any personal data, the Local Ethics Representative (see D1.2) will be responsible for informing the involved pilot users/participants and collecting their informed consents (template annexed in D1.2) that data will be maintained and stored based on the Grant Agreement rules and European/National legislation. No personal data will be centrally stored, without anonymisation or pseudonymisation. Only one person per site or activity (the Local Ethics Representative) will have access to the informed consent form containing the personal information and only that person will be aware of the relation between the participant's unique identifier code and their personal identity, in order to administer the activity/tests. In practice, the Local Ethics Representative will collect those data required for contacting the participants, and then issue a single "Ref-ID") for each of them. This Local Ethics Representative will not participate in the evaluation and will not know how each user responded or behaved. One month before the end of the project, this reference, i.e., the reference between the Ref-ID and the real-life contact details of the participant, together with any other personal information held on the participant will be deleted, thus safeguarding full anonymisation of the results.

The stored data might refer to participant's age, gender, nationality, profession, education but this information will be safeguarded, stored and processed only in accordance with all applicable data protection laws and regulations. The stored data will not contain any other identifier apart from the Ref-ID. In no circumstances will a participant be asked for information relating to their beliefs, political or sexual preferences. User-related data will be securely and safely stored. Furthermore,

data will be scrambled where possible and abstracted to permit its use to achieve project outcomes while ensuring data integrity and security.

Any party which provides any data or information (the "Providing Party") to another party (the "Receiving Party") in connection with the project will not include any personal information relating to an identified or identifiable natural person or data subject. To this end, the Providing Party will anonymise or pseudonymise all data delivered to other parties to an extent sufficient to ensure that a person without prior knowledge of the original data and its collection cannot, from the anonymised or pseudonymised data and any other available information, deduce the personal identity of participants.

Partners supplying special data analysis tools, shall have the right on written notice and without liability to terminate the license that it has granted these tools to be used during the duration of the project, if the supplying partner knows or has reasonable cause to believe that the processing of particular data through such tools infringes the rights (including without limitation privacy, publicity, reputation and intellectual property rights) of any third party, including of any individual.

RESKILLING will undertake activities in several countries and sites. The Consortium will comply with any related European and national legislation and directives relevant to the country where the data collections are taking place. Compliance is monitored by the Ethics Board, the Coordinator and the Technical Manager of the project. Each site will have its own Ethics Committee and one person will be nominated per site as responsible for following the project's Ethics Board recommendations and data protection. Assignment of GDPR roles in RESKILLING

The RESKILLING project encompasses multiple data collection, aimed at supporting a comprehensive, multi-layered implementation and validation process. The Grant Agreement, Section 4, states that: "Personal or sensitive data will not be stored, will be only used to contribute to the identification of the transport professionals CCAM related needs and expectations, as well as for the assessment of the RESKILLING outcomes. All data processing activities will strictly adhere to anonymisation principles and comply with the following legal frameworks: a) the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), b) the Universal Declaration of Human Rights and Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and c) relevant national legislation enforcing these provisions, particularly in relation to obtaining valid consent."

According to GDPR principles, the following roles and responsibilities are identified.

1. **Data Manager** is the natural or legal person that coordinates the actions related to data management, is responsible for the actual implementation of the DMP and its successive versions and for the compliance to open research data guidelines. In RESKILLING, this role is undertaken by VTI , who is leading the DMP Deliverables in the project (D1.3, and its updates D1.4, D1.5) and the Data Protection Officer (DPO) liaison between the project and the Ethics Manager, which is CERTH.
2. **Data Controller** is the legal entity, i.e. the project partner, which, alone or jointly with others, determines the purposes and means of the processing of personal data. In RESKILLING, this role will be undertaken separately and not centrally as each activity, e.g. case study, may vary in terms of plans, data collected, and results gathered. For surveys, interviews etc, the partner who controls the data, and who decides why and how personal data are collected or processed on the respective platform, is the Data Controller

and potentially the Processor. Likewise, each partner planning to organise demonstration and/or dissemination events will be responsible for any data collected.

3. **Data Processor** is the legal entity which processes personal data on behalf of the Controller and under its guidance. The partners who lead WP2-6 are responsible for data processing particularly of personal data. Processors are also organisations that process data on behalf of a Controller — e.g., a subcontractor or a partner conducting analysis for another partner.
4. **For each case study:** the PMT will specify which particular partners are the Data Controllers for each site, and which natural person (Local Ethics Representative) has the operational role of collecting and storing the consent forms and the Ref-ID key on behalf of the partner.
5. **Data analysis, consolidation and results reporting:** Partners analysing, consolidating and reporting results are Data Processors in all 6 WPs. Individuals, such as Local Ethics Representatives, are natural persons who perform tasks on behalf of the organisation that is the Controller or Processor; in other words, they are **authorised persons**, not the actual controllers or processors themselves.

The current allocation of responsibilities will be re-visited and if needed updated in the next version of this Deliverable.

Additionally, **the Data Protection Officer (DPO)** is an enterprise security leadership role to oversee data protection strategy and implementation to ensure compliance with GDPR requirements. The DPO assists the controller or the processor in all issues relating to the protection of personal data. It is mandatory for every public authority and corporation that handles personal data in the EU to have a data protection officer. Among RESKILLING's partners this applies to VTI, where Jakob Sunesson has been designated as DPO.

A data subject 'is a natural person whose personal data is processed by a controller or processor'. In RESKILLING, those subjects are all those people participating in focus groups, surveys and other activities, and they will be referred to as **"user/participant"**, as it is more appropriate to both their involvement and role in RESKILLING.

GDPR adherence is closely related to the ethical treatment and monitoring of all human related activities, including data collection and processing. Ethics Boards/ Committees may exist at each entity/institution AND/OR on national level. All entities participating in activities that involve stakeholders and "users/participants" may need to get approval before proceeding with those activities. Ethical approvals address data privacy and ethical issues relevant to the specifications and requirements at the site where the activity takes place.

3.8. Internal record keeping

To comply with GDPR requirements on record keeping (Article 30), RESKILLING asks all Data Controllers and processors acting on behalf of the Data Controller (all acting under the auspices of the project Data Manager) to record their (personal) data processing activities in standard templates (Annex 1). These forms include fields on the contact information of the Data Controller(s) and processor(s), purpose and categories of processing, a general description of the technical and organisational security measures, etc. These are submitted to the project Data Manager and, in turn, Project Coordinator for presentation whenever need and/or requested. They are treated

as living documents and they must be updated whenever it is necessary. At the end of the project, the main processes and outcomes will be shared with the Project Core Team.

4. Data management obligations

4.1. Research consent

As a research and innovation action, RESKILLING processes personal data only for research and evaluation purposes. RESKILLING will elicit unambiguous consent from participants after giving them the appropriate information in clear and simple terms using the GDPR compliant informed consent forms in Annex 1. This will need to be obtained for the various activities where personal data may be collected or processed. Participants retain the right to withdraw their consent at any point during the study (-ies), without any impact on their rights or involvement in other activities..The Data management team (Data Manager, Ethics Manager, and DPO(s) of partners involved in the specific activity) will ensure through the Ethics and Data Privacy policies that all processes, from participants' recruitment to data reporting, are ethical and GDPR compliant.

4.2. Privacy by design

The GDPR states that “the controller shall...implement appropriate technical and organisational measures...in order to meet the requirements of this Regulation and protect the rights of data subjects”. RESKILLING's DMP details the procedures that will be followed to ensure compliance with the GDPR requirement for data processors and controllers to hold and process only the data necessary for its activities (data minimisation), as well as the limitation of access to personal data to those needing it for processing (Article 23).

5.Data Privacy Impact Assessment

The Privacy Impact Assessment is required under Article 35 of the General Data Protection Regulation (EU) 2016/679. A DPIA is a process which helps assessing privacy risks to individuals in the collection, use and disclosure of information. The focus on the DPIA is to highlight the key areas where private data might be collected/ processed, and to help identifying privacy risks, foresee problems and bringing forward solutions.

The Controller must conduct a DPIA if the processing is likely to result in a high risk to individuals. It is also good practice to do a DPIA for any other major project activity which requires the Processing of Personal Data.

In RESKILLING it is mandatory for all WPs to consider if any of its activities need a DPIA, and if yes, perform such. A template is provided in Annex 2.

In addition to the DPIA, a data privacy policy for the website has been developed. It will be continuously updated, adhering to the evolving outcome of the DPIA running in the project. The privacy disclaimer can be reached through the project's web site, and can also be found in Annex 3 of this deliverable.

6. Conclusions and next steps

This version of the Data Management Plan addresses the high-level data types, the data privacy policy, data treatment and management prerequisites according to GDPR, allocation of data related roles, and an outline for Data Privacy Impact Assessment. It also includes a Privacy Policy for the project website. The next version of the DMP (D1.4), which is scheduled for M18, will include detailed dataset descriptions as the data types from the various project sources will have been comprehensively defined in detail. The data management repository's technical, content and quality specifications for storing and communicating the datasets will be created and described in D1.4. Data owners will reach a decision upon data visibility and sharing limitations.

Additionally, the final location and format of open RESKILLING datasets will be defined.

The final DPIA report will be annexed in the final version Data Management Plan Deliverable (D1.5) in M36. A final location and format of open RESKILLING datasets will also be defined in D1.5.

In conclusion, this Deliverable is a living document. It will be referenced throughout the project, and it will be regularly updated during the lifetime of the project.

Annex 1 Data processing - record keeping template

*NOTE: The information requested here is in line with the requirement to maintain data processing records under the GDPR and **is specific to personal data**. All Data Controllers and processors must also keep records of data set descriptions according to the latest Data Management Plan and DPIA. Where applicable, this information must be verified by the organizational Data Protection Officer. These documents should be treated by responsible persons as living, which they are responsible to keep up to date and share them with the management team whenever they are requested.*

I. Data Controller's record of processing activities

1	Contact details of Data Controller
Email	
Company address	
Telephone	
2	Purpose of processing
3	Description of categories of data subjects and of the categories of personal data
4	Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations
5	Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation

6	Where possible, the envisaged time limits for erasure of the different categories of data
7	Where possible, a general description of the technical and organisational security measures for
a	the pseudonymisation and encryption of personal data;
b	the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c	the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d	a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

II. Data Processor's record of processing activities

1	Contact details of Data Processor
Email	
Company address	
Telephone	
2	Categories of processing carried out on behalf of the Controller
3	Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation
4	Where possible, a general description of the technical and organisational security measures for
a	the pseudonymisation and encryption of personal data;
b	the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c	the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d	a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

Annex 2 Data Privacy Impact Assessment (DPIA) template

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of the Local Ethic Representative person	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as relevant deliverables and other supportive documents that reside in SharePoint. Summarize why you identified the need for a DPIA.

--

Step 2: Describe the processing

Describe the nature of the processing

--

Describe the scope of the processing

--

Describe the context of the processing

--

Describe the purposes of the processing

--

Step 3: Consultation process

Consider how to consult with relevant stakeholders - describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

--

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep?

How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

--

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm (Remote, possible or probable)	Severity of harm (Minimal, significant or severe)	Overall risk (Low, Medium or High)

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk [eliminated; reduced; accepted]	Residual risk [low; medium; high]	Measure approved [Yes/No]

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		

Item	Name/position/date	Notes
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA



Research initiative for Enhancing and Adapting Workforce SKILLs for Implementing TraNsport Automation with Employment Growth

Annex 3 Privacy Policy for project website

**Research initiative for Enhancing and Adapting
Workforce SKILLs for Implementing TraNsport
Automation with Employment Growth**

ReSKILLING

Grant Agreement Number: 101147328

Privacy Policy for project website

The Centre for Research and Technology Hellas - Hellenic Institute of Transport (CERTH/HIT), as Project Coordinator and co-responsible for the content of the RESKILLING website, and the European Conference of Transport Research Institutes (ECTRI), as WP Dissemination leader and co-responsible for the content of the RESKILLING website, respect your online privacy and handles your personal data with care. We are responsible for the use of the personal information that we collect to carry out our activities and take all measures within our power to ensure the safety of that use of personal data. This Privacy Policy applies to our Website <https://reskilling-project.eu> (the "Website") and the services that we offer (the "Services"). The personal data are processed in accordance with the Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), on the basis of your consent, our legitimate interest, or legal obligations, as further described in Article 3.

When you register for certain Services, we will ask you to provide personal information. When you sign up to stay informed about our activities, you agree that ECTRI collects and registers the personal information that you transfer. If you are an employee or volunteer of one of our member organisations, based on our terms of reference we have a legitimate interest to retain your data to carry out our activities, unless otherwise indicated by you (see Article 5: Your rights).

This "Privacy Policy" regulates the processing of your personal data by the controller:

- CERTH/HIT, with registered premises at 6th Km Harilaou Thermi, 57001 Thessaloniki, Greece, Non-Profit Organisation under Private Law with statutory registration number: PD77/2000.
- ECTRI, with registered premises at Square de Meeûs 38/40, 1000 Bruxelles, Belgium, and recorded in the Crossroads Bank for Enterprises under the number <831 370 370>.

Please read through this Privacy Policy carefully, since it contains your rights vis-à-vis CERTH/HIT and ECTRI. The Privacy Policy may be reworked or updated from time to time.

Article 1 - Personal data that you communicate to us

1.1. During a visit to this Website:

- IP address
- Authentication and tracking cookies – see our Cookies Policy.

1.2. When registering for our newsletters:

- Name and Surname
- e-mail address
- Tracking data (subscriptions, bounces, opens, clicks, geographic location)

1.3. When registering to the events:

- e-mail address
- First name
- Last Name
- Organisation
- Position/Job title

Article 2 - Personal data that we collect indirectly

2.1. Public data of the principal, customer, or some other business relation.

CERTH/HIT and ECTRI sometimes process public data, e.g. data that are subject to a publication duty, such as the publication of your appointment as director of an organisation, or data that you made public yourself, such as information posted on your website, or data that are generally known in your region or that have appeared in the press.

Article 3 - Purposes of the processing

3.1. General purposes

CERTH/HIT and ECTRI will use the gathered personal data exclusively for the following purposes:

- **IP address** (see article 1.1): to look after and improve this Website by including Personal Data in anonymous statistics, from which the identity of specific persons or companies cannot be discovered, with as legal basis the legitimate interests of CERTH/HIT and ECTRI in continuously improving its Website and provision of services.
- **Name, e-mail address** (see article 1.2) when subscribing to this Website's contact Newsletter. Data processing through the Website's contact form is based on our legitimate interests of getting into touch with interested users and providing further information about the project through our Newsletter.
- **Name, e-mail address, organisation, job title** (see article 1.3): in order to be able to provide the requested services, with as legal basis the legitimate interest to carry out our activities as described in our terms of reference.
- **Photos and videos** to be used for our internal and external communications, with as legal basis your prior explicit consent.

You are not obliged to release your personal data, but you do understand that the granting of certain services becomes impossible if you refuse the processing.

• 3.2. Newsletters and Emails

The personal data will also be used for direct marketing (sending content promoting directly or indirectly our activities).

If you are already included in our mailing list for receiving informative material in electronic form, CERTH/HIT and ECTRI can use your data to send content relating to RESKILLING project and its activities.

This consent can be withdrawn at any time – free of charge and without any obligation for a justification, either via email: the.reskilling.project@gmail.com, or by post to: either CERTH/HIT, 6th Km Harilaou Thermi, 57001 Thessaloniki, Greece or ECTRI, Square de Meeûs 38/40, 1000 Brussels, Belgium – subject to including a copy of an official form of identification.

• 3.3. Transfer to third parties

CERTH/HIT and ECTRI will never pass on your personal data to third parties, with the exception of RESKILLING partners supporting us and technical service providers who handle technical support in so far as this is necessary for the technical provision of services and/or if they are obliged to do so on the basis of a statutory provision or a judicial ruling. The data transfer is based on our legitimate interest of efficiently organising and allocating our tasks and duties.

Furthermore, we use the following instruction-bound processors:

- [Google Analytics](#)
- [Mailchimp](#)

CERTH/HIT and ECTRI will not sell your personal data, rent them out, share them or otherwise make them commercially available to third parties.

• 3.4. Legal requirements

In rare cases, it is possible that CERTH/HIT and ECTRI are obliged to reveal your personal data subject to a court order or in order to comply with other compelling laws or regulations. CERTH/HIT and ECTRI shall make reasonable attempts to inform you in advance about this, unless it is subject to legal restrictions.

Article 4 - Duration of the processing

The personal data are kept and processed by us for a period that is necessary as a function of the purposes of the processing as described in article 3, and as a function of the contractual relationship between CERTH/HIT and ECTRI and you:

- **IP address and tracking cookies:** up to 6 months after the project end (December 31, 2027).

- **E-mail address, name:** for the duration of the requested delivery of services.
- **Name, e-mail address, organisation, job title:** for the duration of the requested delivery of services.

The aforementioned personal data are in any case kept in accordance with prescription periods that oblige us to maintain your personal data for a longer period, e.g. in order to defend ourselves against an action at law.

Article 5 - Your rights

• 5.1. Your Rights

CERTH/HIT and ECTRI are committed to ensuring fair and transparent data processing. You can always contact ECTRI in case of questions about the data subject rights and are free to exercise your data subject rights where the respective legal requirements are satisfied:

- Right to information, Art 15 GDPR
- Right to rectification, Art 16 GDPR
- Right to deletion (right to be forgotten), Art 17 GDPR
- Right to restrict processing, Art 18 GDPR
- Right to data portability, Art 20 GDPR
- Right to withdraw your consent, Art 7 Para 3 GDPR

Furthermore, you have the right to object to processing of your personal data on basis of our legitimate interests on grounds relating to your particular situation, Art 21 GDPR.

• 5.2. Exercising your rights

You can exercise your rights by contacting us either via email: the.reskilling.project@gmail.com, or by post to: either CERTH/HIT, 6th Km Harilaou Thermi, 57001 Thessaloniki, Greece or ECTRI, Square de Meeûs 38/40, 1000 Brussels, Belgium. Please provide information allowing us to identify you. This can be your name, organisation, e-mail address and postal address. If you send us a copy of your official form of identification, please black out all other information apart from your first and last name and address.

• 5.3. Automatic decisions and profiling

The processing of your Personal Data does not include any profiling, nor will you be subject by us to automated decisions.

• 5.4. Right to file a complaint



You have the right to file a complaint with:

- the Hellenic Data Protection Authority (HDPa), Kifisias 1-3, 115 23 Athens, Greece, Tel: +30 210 6475600, Email: contact@dpa.gr
- the Belgian Data Protection Authority, Rue de la Presse 35, 1000 Brussels, Tel: +32 (0)2 274 48 00, Email: contact@apd-gba.be