



RESKILLING

Deliverable D1.4 Data Management Plan Updated

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 2026
Actual Date of Delivery to EC	30 June 2026
Task Number	Task 1.4
Dissemination level	Public

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

Reviewers
Evangelos Beckiaris (CERTH, Greece) , Manon Coyne (POLIS, Belgium), Teresa De la Cruz Eiriz (ZLC, Spain), Evy Rombaut (VUB, Belgium), Caroline Alméras (ECTRI, Belgium).

Disclaimer

This Deliverable is a draft version submitted to the European Commission and is pending validation. Its content is subject to potential revision following the Commission's review.

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 and of the 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
0.1	22/05/2026	Ingrid Skogsmo (VTI, Sweden)	First draft for internal review (this version reference will be removed before submission).
0.2	17/06/2026	Matina Loukea (CERTH, Greece) Ingrid Skogsmo (VTI, Sweden)	Second draft following review of feedback and consolidated modifications .
1.0	26/06/2026	Ingrid Skogsmo (VTI, Sweden), Matina Loukea (CERTH, Greece)	Version ready for submission after internal quality review, handling of feedback and consolidated modifications.

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)
Ref-ID	Reference-ID (for personal data)
WP	Work Package

Table of Contents

Executive Summary	6
Introduction.....	7
1.1. Purpose of the document.....	7
1.2. Intended Audience	7
1.3. Interrelations.....	8
2. Data in RESKILLING - Generation and Use	8
2.1. Main Data Categories.....	9
2.2. Data description.....	13
2.2.1. Metadata.....	14
3. FAIR Data Principles.....	15
4. Data Sharing and Access	17
4.1. Access levels - Confidentiality.....	17
4.2. Open Access principles	17
4.3. Re-use.....	18
5. Data governance.....	19
5.1. Roles	19
5.2. Data ownership.....	20
6. Data Storage and retention	20
6.1. Internal storage	20
6.2. External storage.....	21
6.3. Data/meta-data repository (RESKILLING databases).....	21
6.4. Data Preservation.....	22
7. Data Security, Personal Data and Privacy	22
7.1. GDPR compliance.....	22
7.2. Internal record keeping.....	23
7.3. Data Privacy Impact Assessment (DPIA).....	24
8. Data management obligations (personal data)	25
8.1. Research consent	25
8.2. Privacy by design	25
9. Conclusions and next steps.....	26
Annex 1 Data processing - record keeping template.....	27
Annex 2 Data Privacy Impact Assessment (DPIA) template	31
Annex 4 RESKILLING Privacy Policy.....	37
1) Who we are	2

2)	Data controllers and contact	2
3)	What personal data we process	3
4)	Why we process your data and our legal bases	4
5)	Where we get the data.....	4
6)	Who we share data with (recipients).....	6
7)	International transfers outside the EEA	6
8)	How long we keep your data (retention).....	6
9)	Your rights	7
10)	Complaints	8
11)	Activity-specific notices.....	8
12)	Updates to this notice	8
Article 1 - Personal data that you communicate to us		4
Article 2 - Personal data that we collect indirectly.....		4
Article 3 - Purposes of the processing		4
Article 4 - Duration of the processing.....		6
Article 5 - Your rights		6

List of Figures

Figure 1. Schematic view of data in the RESKILLING project.....	12
Figure 2. Data Registry Headlines.....	20

List of Tables

Table 1: Examples of data that will be collected, used, generated in RESKILLING WPs	10
Table 2: Dataset Description Template.....	13
Table 3: Data documentation matrix.....	14
Table 4: Dissemination levels of RESKILLING project data.....	17

Executive Summary

This deliverable is an update of the first version of the Data Management Plan (DMP) which was presented as Deliverable D1.3.

The updated DMP provides a comprehensive overview of the data-related activities within the project. Specifically, it describes the main dimensions and characteristics of the data the project collects, processes and generates.

For this update, the work packages (WPs) have identified their specific types of datasets, and, in light of that, assessed procedures and forms described in D1.3. for applicability and relevance. Additionally, experiences from practical use of the first version of DMP has been taken into account. In short, this deliverable updated details **standards and methodologies for:**

- **data collection, processing, documentation, and long-term management,**
- **data management** (how data is exploited, shared, and preserved beyond the project's lifetime) in accordance with the **FAIR principles**— Findability, Accessibility, Interoperability, and Reusability.
- **data protection and privacy**, including compliance with relevant legal and ethical frameworks, particularly the General Data Protection Regulation (**GDPR**).
- Application of **anonymisation and pseudonymisation** techniques, including informed consent procedures that will be followed for data processing in compliance with the GDPR and relevant national legislation.
- **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 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.

Specific actions taken have resulted in more relevant forms and procedures for dataset description and control. The Data Protection Impact Assessment (DPIA) and Consent forms have been updated, access to data has been further detailed. For open data sharing a Zenodo community has been created. A privacy policy for the RESKILLING project as a whole has been developed, complementing the one already available for the website.

It should be noted that the DMP – now in its 2nd version, is a Deliverable in M18 (Month 18) 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 Deliverable D1.5 DMP – final update (M31).

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 RESKILLING Data Management Plan (“DMP”) provides a comprehensive overview of the data-related activities within the project. Specifically, it describes the main dimensions and characteristics of the data the project collects, processes and generates, including details on the content, type, format, and expected volume of the data.

The purpose of the present deliverable D1.4 Data Management Plan Updated, is to provide an update of the plan’s first version, D1.3. Since the launch of the first DMP, RESKILLING has undertaken numerous activities that involve data gathering, generation, and processing. This update builds on the experience with and practical use of the DMP in work packages (WPs) and tasks, and feedback on relevance and applicability.

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 adequate data protection and privacy for participants and stakeholders involved in project activities, including, but not being limited to operators, municipalities, authorities, users of mobility , 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 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 are 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 are directly involved in data gathering activities, while others process and utilise data outputs from preceding or parallel WPs.

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

Within WP3, reviews and analyses of interviews are performed and existing data in literature and online provides 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 and WP5.

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 also involves iterative creation and testing of content, requiring structured data capture at different phases.

WP5 uses and analyses data from WP2 and outcomes from WPs 3 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, 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 is generated and iteratively refined at different stages, including data produced in the case studies and user feedback loops, all of which are 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 that is or will be collected, generated, and processed within the RESKILLING project, along with the corresponding methodologies for their handling.

2.1. Main Data Categories

RESKILLING's activities 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 are 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 collected or processed in the project 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 not only uses data as input to support the development of key outcomes but also **generates 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—are themselves considered project-generated datasets. Comparable processes occur in WPs 4 to 6, where data is both used and produced through the development of training content, business models, scenario analyses, case studies, and communication outputs. These outputs contribute to the broader project knowledge base and, where appropriate, are 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 generate results for their own further use. That use of a certain output may also generate some

subjective user feedback, e.g. usefulness and handling. Furthermore, data that can be used to assess the output's functionality is also generated.

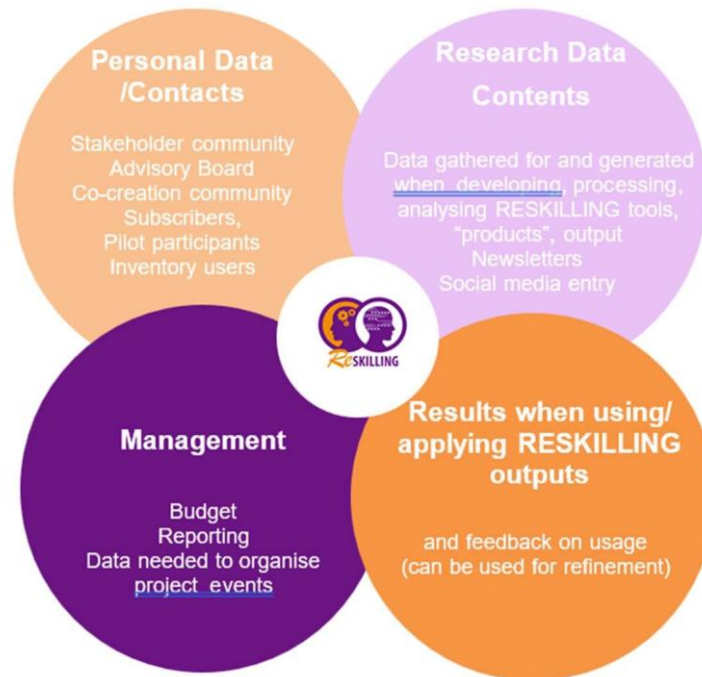
Data that are collected, used and generated in all RESKILLING WP's are shown in Table 1, that will be updated and revised as needed in the next DMP iteration (D1.5 at M36) . Figure 1 provides a schematic overview of the data categories.

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 using RESKILLING outputs tools
WP1 Project management	Budget, Reporting, Administrative data	Internal mailing lists, named individuals in review or reporting contexts		
WP2 Stakeholder community		Stakeholders, Advisory Board	Mapping, Engagement activity (e.g. survey) processing and results	
WP3 Employment & Socioeconomic effects of CCAM		Interviewees	Mapping, Developing, analysing, processing, Results	
WP4 Towards job creation, growth and innovation		Co-creation community, i.e. stakeholders, Participants in workshops and similar events, interviewees, observatory users	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 (for iterative enhancement)

	Management data	Personal / Contact data, Subjective data	Research data / Content	Data generated when using RESKILLING outputs tools
			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 is 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 includes 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 is considered “confidential” according to ISO 27001 standards on information security and is only be accessible to the RESKILLING Consortium members. The same data protection measures also applies 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 is 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 are collected, generated and managed in RESKILLING. Datasets refer to the file extension of the data, and in RESKILLING the following types are handled:

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

The RESKILLING project produces different categories of datasets:

- Context data: data that describe the context of an activity.
- Acquired and derived data: data that contain all the collected information related to an activity or action.
- 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 understanding, analysis, pre-processing.
- Aggregated data: data summary obtained by reduction of acquired data and generally used for data analysis.

For RESKILLING's different datasets Table 2 shows the template used by the WPs for descriptions of their respective datasets, including their reference, file format, standards, methodologies and metadata and repository to be used.

Table 2: Dataset Description Template

Dataset Reference	RESKILLING
Collected / Created	
Dataset name	
Metadata (Dataset description)	Brief description here – provide details as in Table 3. If a standard is used, indicate which.
Dataset type	
File format	
Data size	
Owner	
Privacy level	
Repository during the project (for private/public access)	Open access repository / Partner storage (private cloud/private drop box)/etc.
Data Sharing	Open / Restricted / Confidential
	For Open: Provide information on specific methods or software are needed to access the data (if this is needed)
Back-up frequency	Daily backup for items stored on Sharepoint
Duration of preservation (in years)	4 years after project end
Archiving and Preservation	The preservation guarantee and the data storage during and after the project (for example: databases, institutional

Dataset Reference	RESKILLING
	repositories, public repositories ...) Open access repository/partner storage (private cloud / private drop box) etc., or destroyed after end of project
Link to dataset	

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. As a minimum, each dataset should have metadata that includes details defining the origin, the type, the creation dates and the way these data were created and/or modified. See Table 3, which should be filled out when the data has been created and/or modified, and at least before storing it.

When applicable the metadata should also 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.

Table 3: Data documentation matrix

	Source 1	Source 2	Source n
Data name			
Who created/contributed to data			
Date created			
Data modified			
Conditions			

	Source 1	Source 2	Source n
When applicable: definitions of variables, methods applied to gather and capture data based on common standards. (detailed and technical specification of data)			

3.FAIR Data Principles

The data generated within the RESKILLING project that are made publicly available will be included in an open access repository and will be consistent with all the 'FAIR' principles. RESKILLING will apply the FAIR principles as follows:

Making data findable, including provisions for metadata

- All datasets, reports, and other research outputs that are made publicly available will be deposited in Zenodo under the RESKILLING community and assigned a Digital Object Identifier (DOI). This ensures long-term discoverability and citability. (link: <https://zenodo.org/communities/reskilling/>)
- For datasets that remain internal or restricted (e.g. GDPR-protected personal data), only metadata could be published openly, with a corresponding DOI that resolves to a landing page describing access conditions.
- 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 is defined in the "Metadata" section of the dataset description Table 2.

Making data openly accessible

- Datasets openly available are marked as "Open" in the "Data Sharing" section of the dataset description table (see 2).
- The repository that each dataset is stored in (default is Zenodo) including Open access datasets, is mentioned in the "Archiving and Preservation" section of the dataset description table (see 2).
- The "Data sharing" section of the dataset description table (see 2) 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 2) 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 “Metadata” section of the dataset description table (see 2).

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 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 the “Data Sharing” section of 2.
- 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, those 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 open access data no restrictions will be imposed on their access during which the data is openly available. In case RESKILLING generates IPR protected or proprietary data or make such data available as background assets in the context of the project by one or more beneficiaries, access to this data is to 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 if referred to for the respective dataset’s description in section 2.2. Additional peer-reviews will take place in case of publication in journals.

4.Data Sharing and Access

4.1. Access levels - Confidentiality

RESKILLING will produce data with different levels of confidentiality – which is summed up in Table 4.

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

Data is be stored in secure areas (physical, network, cloud-based). Data to be shared for analysis shall 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.

Each dataset needs to have one or more identified dataset owner(s), 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 case studies will be undertaken in the second half of the project. , 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 final version of this DMP (D1.5 M31).

Data and document sharing within the RESKILLING project uses Sharepoint (see section 6.1 of this deliverable). Access to Sharepoint is restricted to the WP teams directly involved, the Partners Board, RESKILLING's management team (coordinator, ethics manager, data manager, quality manager) and, where necessary, to auditors or reviewers under confidentiality obligations. Dedicated folders with limited access can be set up in Sharepoint to share select material with individuals external to the Consortium but with a specific role, e.g. members of RESKILLING Advisory Board.

4.2. Open Access principles

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 publications. Publications and shared research data will not contain personal or confidential information. All publications resulting from project work must be published in open-access journals, with the aim of maximising scientific impact while respecting security and confidentiality requirements.

The RESKILLING Consortium will make public deliverables, scientific publications, and selected research datasets openly available through the project website and the dedicated RESKILLING community on Zenodo (<https://zenodo.org/communities/reskilling>). Where feasible, shared datasets will be provided in accessible and reusable formats (e.g. CSV) to support use with open-access tools and software. The Consortium will strive to make as many datasets as possible openly accessible, subject to agreement by Consortium members and data owners. Where access is restricted, the reasons will be described in the relevant data-sharing section for the dataset concerned.

Data re-use by external researchers and stakeholders will be possible for selected datasets. If applicable, any embargo period will last at least for the duration of the project to allow partners to manage data collection, analysis, and reporting activities. Data sharing and re-use within the central database will follow the preferences and guidance of the data depositor.

Scientific publications and datasets may also be deposited in institutional repositories maintained by project partners. The choice of repository will depend on the publication creator and the nature of the data. Partners without publicly accessible institutional repositories will use domain-specific repositories or the EU-recommended OpenAIRE service to identify appropriate repositories.

The minimum metadata required for RESKILLING scientific publications deposited in repositories includes:

- The terms “European Union (EU)” and “Horizon Europe”
- The action type: “Research and Innovation Action”
- The acronym and grant number: “RESKILLING, Grant No. 101147328”
- Publication date, authors, and publication name
- Embargo period, where applicable
- A persistent identifier

When referencing open-access data, the following acknowledgement of EU funding will be included in the repository metadata:

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

4.3. Re-use

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.

5.Data governance

5.1. Roles

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 respective Task (T1.4) and is responsible for the DMP Deliverables in the project (D1.3, and its updates D1.4, D1.5).).
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 Data 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 Project Management Team will specify which particular partners are the Data Controllers for each case study (after their definition), and which natural person (Local Ethics Representative) has the operational role of collecting and storing the consent forms and the Reference ID (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 final 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.

5.2. 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.

RESKILLING has established a "Data Registry" in which the various datasets handled in the six WPs are identified. For each dataset a data owner and whether there are GDPR data (if so: is it identifiable, pseudonymised or anonymised) is stated. The Registry also gives an overview of confidentiality level, storage, and sharing. Headlines for the registry are shown in Figure 2.

WP	Responsible partner / data owner	Dataset Name / Description	Type of Data according to GDPR	Confidentiality Level	Anonymised / pseudonymised / identifiable	GDPR Personal Data?	Storage & Preservation	Sharing / FAIR Management	Notes
----	----------------------------------	----------------------------	--------------------------------	-----------------------	---	---------------------	------------------------	---------------------------	-------

Figure 2. Data Registry Headlines

6. Data Storage and retention

6.1. Internal storage

The data collected in RESKILLING will be stored internally in a data repository provided by VTI (Microsoft SharePoint). It constitutes a platform for data sharing and information management within the consortium. As a general principle data will be stored on RESKILLING's Sharepoint, to which the Consortium members have access and editing rights.

Material in the SharePoint area is stored in the cloud. Backup is built-in and data is retained for 120 days. 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.

Access is restricted to the WP teams directly involved, the Partners Board, RESKILLING's management team (coordinator, ethics manager, data manager, quality manager) and, where necessary, to auditors or reviewers under confidentiality obligations. Dedicated folders with limited access can be set up in Sharepoint to share select material with individuals external to the Consortium but with a specific role, e.g. members of RESKILLING Advisory Board.

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

6.2. External storage

The external open data will be published on the project website and stored in the public repository ZENODO, hosted by CERN where a community has been established:
<https://zenodo.org/communities/reskilling/>.

6.3. 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.

Regarding the databases, the following actions are to be taken:

- Upload: Each partner creating a dataset will also be responsible for their upload to the central database to the allocated space.
- Conditions for dataset use:
The administrator of the database and the data responsible need to agree 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.
- Restrictions:
 - Identify and categorise any inherent restrictions in datasets because of the services or applications they are generated from.
 - Evaluate whether indirect restrictions might apply related to software developed for work to be carried out by a specific partner (e.g. in-house s/w, tools, etc.). Notice that there might be license or operating restrictions that should be considered (e.g. compatibility and access only with certain hard- or software or s).

,

6.4. 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.

Ex-post audits of Horizon projects can take place after the project has ended. RESKILLING documentation considered essential for such an ex-post audit will be retained for five years after the final payment has been made.

7. Data Security, Personal Data and Privacy

RESKILLING provides security mechanisms and management procedures to ensure personal (sensitive) data protection through a strict process of data collection and pseudonymisation/anonymisation, and to guarantee data integrity and reliability.

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.

7.1. GDPR compliance

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.”*

In terms of **personal data protection**, personal data is pseudonymised or anonymised and strictly used for the project's purposes. Before collecting any personal data, the Local Ethics Representative will be responsible for informing the involved 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..

In practice, the Local Ethics Representative will collect those data required for contacting the participants, and then issue a single “Ref-ID” (*Reference ID*) for each of them. The 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, 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. This information will be safeguarded, stored and processed 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 deduce the personal identity of participants neither from the anonymised or pseudonymised data nor from any other available information.,

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 case study 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.

7.2. 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.

7.3. Data Privacy Impact Assessment (DPIA)

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 purpose of 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 policies for the project and its 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 4 of this deliverable. A privacy policy for the full project has also been developed and is available as Annex 5 of this deliverable, where the website's privacy policy also can be found.

8.Data management obligations (personal data)

8.1. 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 3 **Fel! Hittar inte referenskölla..** 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.

8.2. 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 project's procedures 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).

9. Conclusions and next steps

This version of the Data Management Plan provides an update of the high-level data types, the data privacy policy, data treatment and management prerequisites according to GDPR, allocation of data related roles, and an updated form for Data Privacy Impact Assessment. Practical experience from using the first version of the DMP (D1.3) have been taken into account. To enhance the applicability of the DMP process adaptations have been made and, where appropriate, forms have been simplified. Data storage and repositories have been further defined. A RESKILLING community has been created on Zenodo for storage of datasets. Furthermore, a privacy policy for the project level of RESKILLING has been developed.

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 (DPO). 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.*

NOTE: There are two templates: one for the Data Controller, one for the Data Processor.

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
	Default (please change in case erasure will take place earlier/later) Raw interview recordings, identifiable transcripts and coded datasets needed for analysis and validation are retained only for the minimum period required to complete the research tasks and project reporting, and no longer than the project lifetime + 5 years (i.e. December 2032), in line with HE audit requirements. Pseudonymised datasets may be stored for the same duration and are deleted or fully anonymised at the end of this period. Fully anonymised datasets may be preserved for long-term scientific reuse, including archiving in Zenodo, where records are maintained indefinitely according to Zenodo's preservation policy. At the end of each applicable retention period, all data are securely erased or irreversibly anonymised following institutional procedures.

General description of technical and organisational security measures

In case other procedures will be applied, please inform DPO and Data Manager for agreement before making intended modifications.

Pseudonymisation and encryption of personal data

Before analysis or internal sharing, personal data will undergo a structured anonymisation pipeline:

1. Removal of direct identifiers

- Names, email addresses, phone numbers, job titles, institutional affiliations, or any field that directly identifies a participant or organisation

2. Masking of contextual identifiers

- Elements that could allow re-identification in combination (e.g. unique roles within small municipalities, specific geographic references, rare organisational contexts) when needed, these are generalised or redacted

3. Pseudonymisation

- Participants are assigned structured codes (e.g. MS-001, INT-034, PP-12)
- The re-identification key is stored separately on secure institutional servers accessible only to the responsible partner's DPO or designated data custodian

4. Aggregation of results

- Interview data are summarised at thematic or categorical levels, removing narrative details that could indirectly reveal identity
- Survey datasets are published only as aggregated statistics or fully anonymised indicators

Storage and access

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.

Access is restricted to the WP teams directly involved, RESKILLING's management team (coordinator, ethics manager, data manager, quality manager) and, where necessary, to auditors or reviewers under confidentiality obligations.

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

General description of technical and organisational security measures

In case other procedures will be applied, please inform DPO and Data Manager for agreement before making intended modifications.

Pseudonymisation and encryption of personal data

Before analysis or internal sharing, personal data will undergo a structured anonymisation pipeline:

5. Removal of direct identifiers

- Names, email addresses, phone numbers, job titles, institutional affiliations, or any field that directly identifies a participant or organisation

6. Masking of contextual identifiers

- Elements that could allow re-identification in combination (e.g. unique roles within small municipalities, specific geographic references, rare organisational contexts) when needed, these are generalised or redacted

7. Pseudonymisation

- Participants are assigned structured codes (e.g. MS-001, INT-034, PP-12)
- The re-identification key is stored separately on secure institutional servers accessible only to the responsible partner's DPO or designated data custodian

8. Aggregation of results

- Interview data are summarised at thematic or categorical levels, removing narrative details that could indirectly reveal identity
- Survey datasets are published only as aggregated statistics or fully anonymised indicators

Storage and access

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.

Access is restricted to the WP teams directly involved, RESKILLING's management team (coordinator, ethics manager, data manager, quality manager) and, where necessary, to auditors or reviewers under confidentiality obligations.

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

Annex 3 Informed consent template

What is this all about?

The RESKILLING project (Research initiative for Enhancing and Adapting Workforce SKILLS for Implementing TraNsport Automation with Employment Growth - Grant No 101147328) is a European Research Project research project aiming to implement a strategic approach, which will empower the workforce and businesses of Europe's mobility (of people and goods) sector, to effectively cope with the anticipated changes in the sector from CCAM deployment, but also to actively participate in advancing and refining the sector. RESKILLING aims to propose, implement, apply and validate a comprehensive approach, guided by inclusivity, co-creation, and social innovation principles, which will efficiently and sustainably coordinate a range of novel services and tools, fostering optimal adaptation of the mobility sector (covering both people and goods) to the deployment of CCAM solutions and services. This will range from analysing the socio-economic and employment impacts of CCAM across the entire value chain to facilitating businesses and workers in mitigating drawbacks and leveraging opportunities brought about by CCAM deployment. This involves innovating business models and employing mechanisms and tools for skill enhancement and adaptation, with an emphasis on their replication and transferability potential and customised scalability for adoption throughout the EU.

The project is by the European Commission as part of its Horizon Europe programme and consists of 20 partners across Europe (the "**RESKILLING Research Partners**", "**we**", "**us**"). Further information about the RESKILLING project is available here: <https://reskilling-project.eu/>.

You have been asked to participate in an **interview** as part of the RESKILLING project.

What is the purpose, methodology and timeframe of the interview?

To discuss employment effects of CCAM.

Who is conducting this interview?

Name, org is conducting the interview as part of RESKILLING Research Partners.

Type of information collected during the interview

Information collected from you during the interview will be processed in accordance with our privacy policy, which can be found here [link to Privacy Policy](#). The RESKILLING Privacy Policy also sets out your rights to control personal information we hold about you. We will notify you if any changes that materially affect the processing relevant to your participation are made to our Privacy Policy.

Who is responsible for the study?

The Lead Researcher is **XXX, who is based at XXX** (one of the RESKILLING Research Partners). You can contact **her/him at: XXX**

Participant Consent Form

I agree to participate in **this interview** being carried out as part of the RESKILLING project.

☐

I can confirm that (please tick each box to indicate you agree):

I have read and understood the information relating to **this interview**,

☐

I understand I can ask questions at any point before, during or **after the interview**,
using the contact details provided.

☐

I understand that the data collected for this study will be stored securely.

☐

I understand that all information collected during **this interview** will be recorded and stored
securely with restricted access.

☐

I understand that all information collected during **this interview** will be used for research purposes only.

☐

I understand that my name will not be used on any documents or in any presentations about the research

☐

I understand that I can leave the study at any time without needing to say why

☐

I consent to receiving emails from the RESKILLING Research Partners relating to RESKILLING's
events, technologies and services.

☐

Signature of participant.....

Name (in capitals) Date.....

If you have any questions about this research, please feel free to contact:

Name: **XXX**

Email: **xxx**

Telephone: **XXXX**

Annex 4 RESKILLING Privacy Policy

The current versions of the privacy policies for 1. the RESKILLING project and 2. for the project's website are presented in the following. They will be updated as needed and the most recent documents can be found at: [https://reskilling-project.eu/RESKILLING Privacy Policy.pdf](https://reskilling-project.eu/RESKILLING_Privacy_Policy.pdf) .

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

ReSKILLING

Grant Agreement Number: 101147328

Project Privacy Notice



Funded by
the European Union

1) Who we are

RESKILLING envisions to implement a strategic approach, which will empower the workforce and businesses of Europe's mobility (of people and goods) sector, to effectively cope with the anticipated changes in the sector from CCAM deployment, but also to actively participate in advancing and refining the sector. For this to be achieved, RESKILLING will propose, implement, apply and validate a comprehensive approach, guided by inclusivity, co-creation, and social innovation principles, which will efficiently and sustainably coordinate a range of novel services and tools, fostering optimal adaptation of the mobility sector (covering both people and goods) to the deployment of CCAM solutions and services. This will range from analysing the socio-economic and employment impacts of CCAM across the entire value chain to facilitate businesses and workers in mitigating drawbacks and leveraging opportunities brought about by CCAM deployment. It involves innovating business models and employing mechanisms and training tools for skill enhancement and adaptation, with an emphasis on their replication and transferability potential and customised scalability for adoption throughout the EU. RESKILLING aspires to create a CCAM innovation system capable of not only generating innovation but also delivering solutions to societal challenges.

The project website, communications, stakeholder engagement, research, interviews, surveys, workshops, co-creation activities, case studies and use of project outputs may involve processing of personal data.

2) Data controllers and contact

Controllers for website and core communications:

- CERTH/HIT – Centre for Research and Technology Hellas / Hellenic Institute of Transport, 6th Km Charilaou-Thermi Road, 57001 Thessaloniki, Greece.
- ECTRI – European Conference of Transport Research Institutes, Square de Meeûs 38/40, 1000 Brussels, Belgium.
- POLIS Network AISBL, Rue du Trône 98, 1050 Brussels, Belgium.

Joint controllership when applicable:

For specific activities such as website content, newsletter updates, event organisation/registration and stakeholder engagement, CERTH/HIT, ECTRI and POLIS may act as joint controllers in accordance with Article 26 GDPR, where they jointly determine the purposes and means of the processing.

Controllers and processors for project research activities:

For research activities, including surveys, interviews, focus groups, workshops, case studies and testing or feedback activities, the relevant RESKILLING partner(s) organising or leading the activity act as Data Controller(s). Partners processing data on behalf of a Controller, for example by supporting analysis or reporting, act as Data Processors. This allocation is activity-specific and is recorded in the project's data-processing records and/or DPIA documentation.

Single contact point for privacy requests:

- Email: the.reskilling.project@gmail.com
 - Postal requests may also be sent to any of the controller addresses listed above.
- The email address is monitored regularly by the Coordinator and the Dissemination Manager.

Data Protection Officer / privacy contact:

The RESKILLING DMP identifies VTI's DPO as Jakob Sunesson for VTI-related data protection matters.

3) What personal data we process

Depending on how you interact with RESKILLING, we may process the categories below. Data minimisation applies: only data necessary for the specific project purpose will be collected.

Interaction / activity	Indicative categories of personal data
Website use	IP address, technical identifiers, authentication and tracking cookies, analytics identifiers, browser/device information, and other technical logs needed for website security, functionality and improvement.
Newsletter / mailing list	Name, surname, email address, subscription status and engagement metrics such as opens, clicks, bounces and geographic information derived from newsletter tools.
Event registrations and stakeholder activities	First name, last name, email address, organisation, position/job title, professional role, sectoral affiliation, attendance records, dietary/accessibility information where strictly necessary for event organisation, and follow-up communications.
Stakeholder mapping and Advisory Board activities	Contact details, professional affiliation, expertise area, role, organisation, public professional information and records of engagement with the project.
Surveys, interviews, focus groups and workshops	Contact details for recruitment/follow-up, demographic information where relevant (e.g. age group, gender, region), professional profile, employment status, sectoral affiliation, opinions, needs, expectations, feedback, interview notes, transcripts, audio/video recordings where consented, and attendance logs.
Training, tools, Observatory, Business Model Toolkit and other RESKILLING outputs	User account details where applicable, professional role/profile data needed to generate personalised or contextual outputs, user feedback, interaction data, technical logs, tool performance metrics, usage statistics and evaluation data.
Photos and videos	Images, video recordings and voice recordings where individuals may be identifiable, only where relevant for dissemination, reporting, documentation or research and subject to the appropriate consent/legal basis.
Project partner staff and internal coordination	Names, institutional emails, organisation, role, meeting attendance, mailing-list membership, contact information, administrative records and contribution records needed for project management, reporting and coordination.

The project does not intend to request information relating to beliefs, political opinions or sexual preferences. Special categories of personal data will not be collected unless strictly necessary, clearly justified, covered by an appropriate legal basis and safeguards, and addressed in an activity-specific notice and/or DPIA.

4) Why we process your data and our legal bases

RESKILLING processes personal data only when there is a lawful basis under GDPR. The main purposes and legal bases are:

Purpose	Examples	Legal basis
Operate, secure and improve the website	Website functionality, security, performance monitoring, analytics and anonymous statistics.	Legitimate interests (Art. 6(1)(f)) and/or consent for certain cookies/analytics, depending on the cookie setup.
Send project news and newsletters	RESKILLING Brief, project updates, invitations and dissemination material.	Consent (Art. 6(1)(a)); consent can be withdrawn at any time through the unsubscribe link or by email request.
Manage event participation and stakeholder engagement	Registration, logistics, attendance lists, communications before/after events, stakeholder community management and project reporting.	Legitimate interests (Art. 6(1)(f)) and/or consent where required.
Use photos/videos for communication and dissemination	Website, social media, newsletters, presentations, dissemination materials, internal project documentation.	Prior/explicit consent (Art. 6(1)(a)) where applicable.
Conduct research and evaluation activities	Surveys, interviews, focus groups, workshops, co-creation, case studies, assessment of employment and skills needs, evaluation of project outputs.	Consent (Art. 6(1)(a)) and/or legitimate interests (Art. 6(1)(f)); where applicable for public research organisations, task in the public interest (Art. 6(1)(e)) may be used according to the controller's institutional/legal framework.
Develop and validate RESKILLING outputs	Training profiles/modules, Business Model Toolkit, CCAM Employment & Skills Observatory, recommendations, roadmap, impact assessment and user feedback loops.	Consent and/or legitimate interests, depending on the activity; activity-specific notices will specify the exact basis.
Comply with legal, audit and contractual obligations	Horizon Europe reporting, audit trail, accountability, ethics and GDPR record keeping.	Legal obligation (Art. 6(1)(c)) and/or legitimate interests (Art. 6(1)(f)).

For surveys, interviews, case studies, workshops and tool-testing activities, short activity-specific notices and consent forms should be provided when personal data are collected, especially where recordings, detailed professional profiles or potentially sensitive contextual information are involved.

5) Where we get the data

- Directly from you, for example through forms, event registrations, email sign-ups, surveys, interviews, workshops, focus groups, project tools, feedback forms and direct communications.

- From project partners, when they organise or support RESKILLING activities and share data strictly as needed for project implementation.

- From publicly available or lawful professional sources, for example public organisational websites, professional profiles, publications, stakeholder directories, press releases or other publicly available information relevant to stakeholder mapping and engagement.
- From technical systems used by the project, for example website analytics, newsletter distribution tools, registration platforms, project SharePoint, databases, training platforms or the CCAM Employment & Skills Observatory, where applicable.

6) Who we share data with (recipients)

Personal data are shared only where necessary for project implementation, research, communication, reporting or legal compliance. Recipients may include:

- RESKILLING project partners, strictly on a need-to-know basis and according to their role in the relevant activity.
- The project management team, including the Coordinator, Ethics Manager, Data Manager and Quality Manager, where required for oversight, compliance, reporting and audit purposes.
- Work package/task teams directly involved in the relevant activity.
- Auditors, reviewers, the European Commission/CINEA or other competent authorities, where required under Horizon Europe rules, legal obligations or audit procedures, and subject to confidentiality obligations where applicable.
- Service providers acting as processors under the project's instructions, such as Google Analytics for analytics and Mailchimp for newsletter distribution.
- Technology providers or platform operators supporting RESKILLING tools, training activities, databases, meeting/event platforms or secure document storage, where applicable and subject to appropriate safeguards.

RESKILLING does not sell, rent or commercially share personal data. Personal data will not be shared with external databases for further reuse. Data shared internally for analysis should not include direct personal or identification data unless strictly necessary and authorised.

7) International transfers outside the EEA

Some service providers may process personal data outside the European Economic Area. For example, Mailchimp may involve international transfers for newsletter distribution. Where such transfers occur, they will be safeguarded through appropriate mechanisms such as Standard Contractual Clauses (SCCs), additional safeguards and/or other GDPR-compliant transfer mechanisms, as applicable.

Project partners are responsible for assessing transfers linked to their own activity-specific tools or processors and documenting them in the relevant record of processing activities and/or DPIA.

8) How long we keep your data (retention)

RESKILLING keeps personal data only for as long as needed for the purposes described above, for accountability, and to comply with legal, contractual and Horizon Europe audit obligations. The default retention rules below should be adapted where an activity-specific notice or controller policy requires a shorter or longer period.

Data category	Indicative retention
Website logs/cookies	Up to 6 months after their collection, unless a shorter cookie-specific period applies or longer retention is required for security/legal reasons.

Data category	Indicative retention
Newsletter data	Until you unsubscribe or withdraw consent. Minimal suppression records may be retained to ensure that unsubscribe requests are respected. Periodic checks will be carried out and inactive contacts will be deleted where appropriate.
Event registration data	For the duration needed to manage the event, follow-up and project reporting, then deleted or anonymised unless longer retention is needed for legal claims, audit or accountability.
Raw interview/audio/video recordings and identifiable transcripts	Only for the minimum period needed to complete research, validation and reporting, and no longer than the project lifetime plus 5 years (indicatively until December 2032), unless a shorter period is set by the relevant controller or consent form.
Consent forms and re-identification keys	Stored separately and securely by the responsible Local Ethics Representative/data custodian. The Ref-ID key linking participant identity to research data should be retained only for as long as it remains necessary for the research, validation, legal and/or audit purposes, and should be deleted as soon as it is no longer needed, and in any case no later than the end of the project, leading to the full anonymisation of results.
Pseudonymised research datasets	May be retained for the project lifetime plus 5 years for validation, reporting and audit, then deleted or fully anonymised.
Fully anonymised datasets and metadata	May be preserved for long-term scientific reuse, including in ZENODO or other repositories, because they no longer identify individuals.
Horizon Europe audit documentation and essential project records	Retained for 5 years after the final payment, in line with Horizon Europe audit requirements.

At the end of the applicable retention period, data will be securely deleted or irreversibly anonymised following the relevant partner's institutional procedures.

9) Your rights

Subject to the conditions and limits set out in GDPR, you have the right to:

- Access your personal data (Art. 15 GDPR).
- Ask for inaccurate or incomplete data to be corrected (Art. 16 GDPR).
- Ask for your data to be erased where the legal conditions are met (Art. 17 GDPR).
- Ask for the restriction of processing (Art. 18 GDPR).
- Receive your data in a portable format where applicable (Art. 20 GDPR).
- Object to processing based on legitimate interests (Art. 21 GDPR).
- Withdraw consent at any time where processing is based on consent (Art. 7(3) GDPR), without affecting the lawfulness of processing carried out before withdrawal.

To exercise your rights, contact the project privacy inbox at the.reskilling.project@gmail.com and provide enough information to identify you and the relevant activity. You may also contact the relevant controller directly by post using the addresses listed in Section 2.

If you send a copy of an identification document, please black out all information except what is necessary to identify you for the purpose of the request. The processing of your personal data does not include automated decision-making or profiling that produces legal or similarly significant effects on you.

10) Complaints

You have the right to lodge a complaint with your local data protection supervisory authority. For the controllers listed in this notice, relevant authorities include:

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

You may also contact the supervisory authority in your country of residence, place of work or place of the alleged infringement.

11) Activity-specific notices

This overall notice should be supplemented by short activity-specific privacy notices when RESKILLING carries out activities such as:

- surveys, interviews, focus groups or workshops, especially when recordings are made;
- case studies, pilots, validation or testing activities;
- training platform or restricted-area accounts;
- use of the CCAM Employment & Skills Observatory or other tools generating personalised or activity-specific outputs;
- processing involving special categories of data, if ever required and justified;
- activities involving third-party platforms, new processors or international transfers not already covered in this notice.

Minimum information to include in each activity-specific notice:

- Activity name and responsible controller(s).
- Contact details of the lead researcher/activity lead and Local Ethics Representative, where applicable.
- What personal data will be collected, including whether audio/video recording will be used.
- Purpose and legal basis for processing.
- Recipients, processors, tools/platforms and any transfers outside the EEA.
- Retention period and anonymisation/pseudonymisation procedure.
- Participant rights, withdrawal process and privacy contact point.

For research activities, participants should receive the relevant information and consent form before the activity begins. Consent forms and Ref-ID keys should be stored separately from research data by the responsible Local Ethics Representative or authorised data custodian.

12) Updates to this notice

This notice may be updated to reflect changes in RESKILLING processing activities, tools, processors, controllers, legal requirements or DMP updates. All updates will be published on the RESKILLING website and/or made available through the relevant activity communication materials.

Project website: <https://reskilling-project.eu/>



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



Funded by
the European Union

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

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, the European Conference of Transport Research Institutes (ECTRI), as WP Dissemination leader and co-responsible for the content of the ReSKILLING website and Newsletter updates, and POLIS Network AISBL (POLIS), as WP Stakeholder Engagement leader and co-responsible for the content of certain events registration forms, 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 controllers:

- 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>.
- POLIS Network AISBL, with registered premises at Rue du Trône 98, 1050 Brussels, Belgium, VAT Number BE.0460.400.701

For specific activities such as event organisation, registration collection, and stakeholder engagement, CERTH/HIT, ECTRI and POLIS act as **joint controllers** and jointly determine the purposes and means of processing personal data in accordance with Article 26 GDPR.

Please read through this Privacy Policy carefully, since it contains your rights vis-à-vis CERTH/HIT, ECTRI, and POLIS. 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)

This data is processed through Mailchimp, our external Newsletter communication provider.

1.3. When registering to the events:

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

These data may be collected directly by POLIS on behalf of the ReSKILLING project.

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 when subscribing to the Newsletter is based on your explicit consent. Your subscription is handled via Mailchimp, which securely collects and processes your name and email address for the purpose of sending project updates. The subscription form is accessed through a secure [iframe](#) from our Website – linked to Mailchimp's signup form. The processing of your personal data is carried out in accordance with our Privacy Policy and GDPR
- **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. Event registration data (name, email, organisation, position) may also be collected and processed by POLIS Network as part of their role in organising or co-organising project events. In such cases, POLIS acts as a joint controller together with CERTH/HIT and ECTRI, and processes your data exclusively for the purpose of managing event participation, communication with participants, and reporting obligations of the ReSKILLING project

- **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 subscribe to the ReSKILLING Newsletter ('ReSKILLING Brief'), your data will be processed by Mailchimp for the purpose of distributing our updates. Mailchimp acts as a processor on our behalf and processes your data exclusively according to our instructions.

Mailchimp is located outside the European Economic Area (EEA). Personal data transfers to Mailchimp are safeguarded through Standard Contractual Clauses (SCCs) and additional measures provided by Mailchimp to ensure GDPR-compliant processing

This consent can be withdrawn at any time – free of charge and without any obligation for a justification via a weblink embedded at the bottom of each Newsletter edition or via [this hyperlink](#).

- **3.3. Transfer to third parties**

CERTH/HIT, ECTRI, and POLIS 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, ECTRI, and POLIS will not sell your personal data, rent them out, share them or otherwise make them commercially available to third parties. Mailchimp is used exclusively for managing newsletter subscriptions and sending communications. Mailchimp does not use your data for its own purposes.

- 3.4. Legal requirements

In rare cases, it is possible that CERTH/HIT, ECTRI, and POLIS 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, ECTRI, and POLIS 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, ECTRI, POLIS, 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, ECTRI, and POLIS 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; ECTRI, Square de Meeûs 38/40, 1000 Brussels, Belgium, or POLIS, Rue du Trône 98, 1050 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.

If your personal data is processed through Mailchimp, you may also exercise your rights (such as access or erasure) directly through the [unsubscribe link](#) embedded in each email or by contacting us using the details above.

• 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