

TRUST Traffic Safety Culture | A Systematic Transition towards Shared
Responsibility for Safe and Sustainable Mobility in the EU

D1.2 | Data management plan I

TRUST

Project identification

Acronym	TRUST
Full title	Traffic Safety Culture – A Systematic Transition towards Shared Responsibility for Safe and Sustainable Mobility in the EU
Project term	01.05.2025 – 30.04.2028

Document identification

Deliverable number	1.2
Deliverable title	Data management plan I
Work package	1 Management
Contractual due date	31.10.2025
Submission date	31.10.2025
Dissemination level	Public
Responsible author	Susanne Kaiser KFV
Contributions from	Armin Kaltenegger, Dagmar Lehner, Klaus Machata KFV
Internal reviewer	Armira Kontaxi NTUA

Citation

Kaiser, S., Kaltenegger, A., Lehner, D., & Machata, K. (2025). Data management plan. Deliverable 1.2 of the EC Horizon Europe project TRUST

Funding note



This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 10119799

Disclaimer

The content of this publication is the sole responsibility of the publishers, and it does not necessarily represent the views expressed by the European Commission or its services. While the information in the document is believed to be accurate, the authors(s) or any other participant in the TRUST consortium make no warranty of any kind regarding this material. Neither the TRUST Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise however in respect of any inaccuracy or omission herein. Without derogating from the generality of the foregoing, neither the TRUST Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright

© TRUST Consortium, 2025-2028. This deliverable contains original unpublished work except where indicated otherwise. Acknowledgement of previously published material and work of others has been made through appropriate citation. Reproduction is authorized provided the source is acknowledged.

Table of Contents

Glossary & abbreviations	4
1. Introduction	5
2. Project objectives and required (personal) data	6
2.1. Required data to achieve objectives	6
3. Data protection & data security	8
3.1. Data protection	8
3.2. Data security	10
4. FAIR principles	11
4.1. Findability	11
4.2. Accessibility	11
4.3. Interoperability	12
4.4. Re-usability	12
5. Other issues	13
5.1. Data ownership	13
5.2. Resource allocation	13
5.3. Update of the DMP	13
References	14

Glossary & abbreviations

Term / abbreviation	Explanation
CC BY	Creative Commons Attribution International Public License
CC0	Creative Commons license
DEC	Dissemination, Exploitation and Communication
DMP	Data Management Plan
DOI	Digital Object Identifier
ESRA	E-Survey of Road users' Attitudes
ETSC	European Transport Safety Council (project partner)
FAIR	Findable, Accessible, Interoperable, Reusable
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
KFV	Kuratorium für Verkehrssicherheit (Austrian Road Safety Board, Coordinator)
LLM	Large Language Model
TSC	Traffic Safety Culture

Statement on the use of AI

AI-powered language tools were used to support grammar correction, translation, and editorial consistency across different language versions of this report. No content was generated without human oversight, and all outputs were reviewed and adapted to reflect project terminology and context-specific nuance.

1. Introduction

This document is the first version of the Data Management Plan (DMP) with the purpose of describing data handling of all data generated, collected and processed within the TRUST project in accordance with GDPR guidelines, the Grant Agreement and FAIR principles (Findable, Accessible, Interoperable, Reusable). Partner organizations from non-EU member states have committed themselves to complying with all relevant EU directives. The DMP will be updated continuously and re-submitted twice, at the midpoint of the project and at the end of the project term, resulting in two additional documents, with the purpose of ensuring data quality, accessibility and security beyond the conclusion of the project in 2028. The DMP is a support document for project partners, facilitating efficient yet correct data handling.

The main purpose of data collection within the TRUST project is to achieve the proposed objectives with regards to defining 'Traffic Safety Culture' (TSC), modelling the relationship between TSC and road safety outcomes, measuring TSC in different context and developing necessary measuring tools, designing and validating interventions to grow TSC in 7 different pilot areas, and to develop and publish a wide range of tools and materials which facilitate the growth of TSC in organizations as well as communities. TRUST will generate, collect, process and store only data which is necessary to achieve its objectives and applies principles of "privacy by design" and "privacy by default", meaning that TRUST only collects data absolutely necessary and in GDPR conforming manner (Art. 28 GDPR).

2. Project objectives and required (personal) data

The overall aim of TRUST is:

To contribute to a significant reduction of fatal and seriously injured road traffic victims, by growing a positive traffic safety culture in Europe.

In order to achieve this overall aim, the following is needed:

- a scientifically grounded and operational definition of traffic safety culture (TSC) and its underlying components
- convincing evidence that a strong traffic safety culture reduces road crash risk
- tools to assess the level of TSC and its components
- guidance on effective interventions that will increase the level of TSC
- effective dissemination of tools, guidance and good practice to boost TSC all over Europe.

The TRUST project objectives to achieve this are:

1. **Definition** | Define clearly TSC and provide an operational definition that is suitable for modelling, measurement tools and interventions.
2. **Model** | Development of a validated model of the relationship between TSC and road safety outcomes.
3. **Safe System & sustainability**: Show the added value of the TSC concept for a Safe System approach integrated with sustainable mobility.
4. **Measurement** | Develop practical tools that can be used to assess TSC at all levels, and as a baseline for interventions.
5. **Intervention** | Develop intervention mechanisms and guidance for improving TSC in communities and organisations.
6. **Evaluation** | Test and evaluate tools and interventions in seven pilots, representing different road safety contexts.
7. **Communication** | Creation of the TRUST platform as the starting point for communication, dissemination and exploitation activities. This platform will include easily accessible information, tools, and benchmarking facilities for different stakeholders withing organisations as well as communities.

2.1. Required data to achieve objectives

The following section describes the data generated, collected or processed per objective. Data is required either from experts on a subject matter, stakeholders, road users or interested persons. A fundamental distinction is made between personal data and anonymous data. Personal data will strictly be used according to GDPR requirements (see 3), while anonymous or anonymized data will be made available according to FAIR principles as much as possible. The following table summarises the required data to achieve TRUST objectives, however, does not present the entirety of the work programme.

TRUST objectives	Action	Data generated, collected or processed
Definition	The Delphi Method will be applied to reach consensus on the definition of TSC and impact factors shaping TSC. For this purpose, up to 60 experts on road safety, TSC, public health and organizational safety culture will be consulted via e-mail.	Name, affiliation, and contact details of relevant experts
		Qualitative written data from consulted experts
	Complementary expert interviews will be conducted if needed.	Name, affiliation and contact details of experts
		Audio recordings, transcripts
Model	Based on ESRA2 and ESRA3 data, TRUST will statistically model TSC components and their influence on road safety outcomes.	Quantitative survey data from the ESRA initiative
	Collection of representative data from road users in Norway, Sweden, Bulgaria and Serbia via polling agencies on self-reported behavioural, motivational and cognitive factors.	Quantitative survey data from road users
Safe System & sustainability	Expert interviews	Name, affiliation and contact details of experts
		Qualitative verbal data from experts (audio recording)
Measurement	Development of a Large Language Model (LLM) to assess organizations' level of TSC with a data corpus of publicly available documents	LLM
	Development of a self-assessment tool for organizations, which will be available via the TRUST platform to gain insight into levels of TSC	Self-assessment data of users
Evaluation	Evaluation of interventions within 7 pilots targeted at actors in authorities and companies and road users with pre- and post-intervention quantitative and qualitative measurements of TSC. The interventions will target individuals in seven different road safety relevant contexts (7 Pilots).	Lists of participants per pilot (name, contact details, availability)
		Qualitative verbal data from individuals subject to interventions
		Quantitative survey data from individuals subject to interventions
Communication	The TRUST platform is a website which will provide results and resources generated within the project. Interested website visitors are given the option to register for a newsletter.	List of users registered to newsletter (e-mail addresses)
		Website traffic data
	Photos and videos will be taken of TRUST meetings and events to facilitate dissemination and communication	Photos, videos

TABLE 1 | Overview of TRUST objective and actions and data generated, collected or processed

3. Data protection & data security

The coordinator KfV has appointed an in-house ethics advisor who regularly monitors the compliance of project activities with the applicable ethics and data protection standards. The advisor is furthermore the first point of contact for TRUST partners for questions of any kind related to the guidelines of the DMP as well as for application of the data protection regulation GDPR and relevant passages of the Grant Agreement.

3.1. Data protection

As described in chapter 2, data of various kinds needs to be collected and processed to achieve the project's goals. Special attention needs to be paid to the protection of data types which include personal data – that is any kind of data which allows conclusions to be drawn about an identified or identifiable natural person (e.g., name, ID number, location data, IP address). If needed, an individual assessment of partners' roles will be made in accordance with GDPR and additional agreements will be concluded (e.g., if personal data needs to be shared with a sub-contractor).

Before processing any kind of personal data, the person in question needs to be asked for consent. This request entails also the provision of information on the purpose of data collection and the data subject rights. Such information must include:

- Contact details of responsible TRUST member
- Purpose and legal basis of data processing
- Duration of storage of data
- If applicable, information on who receives the data
- Rights of data subject (Art. 13 GDPR) on information, rectification, erasure of data, withdrawal of consent to process data with effect for the future as well as the right to issue a complaint to the data protection authority (of the respective country)

From linking objectives with required (personal) data (see 2.1), four types of data can be extracted. They are listed in the table below (TABLE 2), including storage and processing information as well as requirements and guidelines for data handling, in particular for personal data (highlighted in grey).

Data type		Format	Requirements and guidelines
Personal data according to GDPR	List of experts	• Excel list including name, affiliation, profession and e-mail address of relevant experts	• Consent for data processing from the data subject will be obtained. • When requesting consent, extensive information must be provided (see list above table). • The lists will only be used for the purpose of establishing contact, scheduling interview dates or e.g., training, and submitting relevant information in preparation for a meeting or training. • The lists will only be accessible to members of TRUST who are involved in the respective activity.

Data type		Format	Requirements and guidelines
	List of participants (Pilots)	Excel list with Pilot participants including name, availability (e.g., for participating in training =intervention), e-mail address, phone number	- Lists will be deleted once the respective activities and related reporting are fully completed. - The data of a subject needs to be deleted upon request. - The data subject must be provided with information about the data held about the person upon request. - All data provided by the subjects other than listed in column 2 (format), such as statements from an interview, answers to a questionnaire etc. will be anonymized and stored separately from the lists with names, affiliations and contact details.
	List of people registered to the TRUST newsletter	List with e-mail addresses stored in WordPress	- Consent for data processing from the data subject will be obtained. - Double opt-in procedure: registration must be confirmed via e-mail. - When requesting consent, extensive information must be provided (see list above table). - The lists will only be used for the purpose of sending e-mails with news items in relation to the TRUST project, platform, results or TSC related information. - The list will only be accessible to members of TRUST responsible for distributing the newsletter (ETSC and KfV). - The data of a subject needs to be deleted upon request and an un-subscription option must be provided with each newsletter sent.
	Event pictures and videos	- Pictures and videos taken from project meetings and events - Stored at the local servers of TRUST partners responsible for the task	- Consent for data processing from the data subject will be obtained. - Participants of events, meetings, training, etc. must be informed that photos will be taken and/or videos recorded. - Participants of events, meetings, training, etc. must be informed about the purpose of photos and videos taken as well as their rights. - The data of a subject needs to be deleted upon request.
No personal data according to GDPR	Qualitative data from Delphi method	Written statements received via e-mail and collected in .docx format	- The statements made will be stored separately from any information that allows conclusions to be drawn about the subject. - Stored at the local servers of TRUST partner responsible for the task or SharePoint.
	Qualitative data from expert interviews	- Recorded verbal statements, transcribed and processed into .docx format - Stored at the local servers of the TRUST	

Data type		Format	Requirements and guidelines
		partner responsible for the task	
	Quantitative data generated through online surveys of polling agencies	• Respondents' answers, largely quantitatively coded, in .xlsx and .sav format as submitted by the polling agency • Stored at the local server of the TRUST partner responsible for the task	• At no point will there be personal data received about the subject person. The answers of the respondents will not allow for conclusions to be drawn about the person.
	Quantitative data generated through online surveys created by TRUST members	• Respondents' answers, largely quantitatively coded, in .xlsx and .sav format, retrieved from TRUST partners' own survey infrastructure	

TABLE 2 | Type of data generated, collected or processed in TRUST and requirements for data protection. Rows highlighted in grey list data types which include personal data and thus are subject to stricter data protection requirements according to the GDPR guidelines.

3.2. Data security

Data security mainly concerns the prevention of loss of any kind of project data as well as the secure storage and transmission of personal and sensitive data.

To avoid data loss or leak of data stored at local servers of the project partners, the corresponding organizations must meet at least the following security standards:

- Data backup: Regular backups must be performed and stored securely.
- Patch management: Systems must be updated regularly and protected against known security vulnerabilities.
- Firewalls and intrusion detection: use of firewalls and systems to detect and defend against attacks.
- Access controls: restriction of access to data to authorized personnel only and multi-factor authentication whenever possible.

To protect sensitive and personal data as described in chapters 2 and 3, this type of data will be:

- Only accessible to authorized personnel and secure data transfer methods will be used.
- Transferred only via methods allowing for up-to-date encryption methods such as AES-256, TLS 1.2 or higher. The default system to share data within the project is Microsoft's SharePoint, which ensures appropriate encryption.
- Disposed of when the data is no longer needed for achieving the project's objectives.

4. FAIR principles

Data generated, collected and processed will be managed according to the principles of FAIR data management, meaning they are Findable, Accessible, Interoperable, and Re-usable (Wilkinson et al., 2016).

4.1. Findability

Criteria to make data findable are:

- (Meta)data are assigned a globally unique and persistent identifier
- Data are described with rich metadata (see also Re-usability)
- Metadata clearly and explicitly include the identifier of the data it describes
- (Meta)data are registered or indexed in a searchable resource

Findability applies to both humans and machines. Therefore, any kind of artefacts produced by TRUST, that will be commonly accessible will be accompanied by machine-readable metadata and a Digital Object Identifier (DOI, persistent identifier). According to the Grant Agreement, metadata of deposited/archived publications will be open under a Creative Commons Attribution International Public License (CC BY), Creative Commons License (CC0) or equivalent license. Metadata will, at a minimum, include information about:

- Publication (author(s), title, date of publication)
- Horizon Europe funding reference
- Grant project name
- Acronym
- Licensing terms
- Persistent identifier
- Authors involved in the action

Furthermore, each metadata record deposited will include meaningful key words to increase findability in repositories and archives (see 4.2) and the following file naming convention will be established:

TRUST_HEU_ORG_Type_Description_YYMM_Version

- ORG: TRUST partner who collected the data, e.g., *NTUA* for National Technical University of Athens, or *DBL* for Deep Blue
- Type: data type, such as *research data*, *survey* or *report*
- Description: refers to the kind of data, e.g., *TSC index*, *self-reported behaviour* or a deliverable title
- YYMM: year and month of data collection or processing, e.g., *2607*
- Version: version number, e.g. *1.2*, *3.0* or version label such as *final*

4.2. Accessibility

Data, results and tools created in TRUST will be shared according to the principle stated in the Grant Agreement: “as open as possible, as closed as necessary”. Personal data will be protected and will not be accessible at any time; however, it will be made available on an aggregated level whenever possible.

TRUST uses “Zenodo” for the deposition of all public deliverables and other publishable artefacts (see Accessibility), which automatically assigns a DOI to every published record. Zenodo is a digital online repository created by CERN for EC funded research¹. For scientific publications, gold open access publishing will be chosen whenever possible. All public deliverables will also be published on the TRUST platform under <https://trafficsafetyculture.eu>.

4.3. Interoperability

Data deposited in open access archives (Zenodo) will be described using common metadata standards and terms, aiming at ensuring potential combination with similar types of data. Data formats will adhere to common standards:

- Reports, deliverables, manuscripts, scientific papers: pdf format
- Data sets: xls or csv format
- Visual material (photos, graphics, logos, etc.): png and/or svg format
- Videos (e.g. recorded webinar): mp4 format

4.4. Re-usability

The re-use of publicly available project data will be ensured through conscientious compliance with the first three FAIR principles, Findability, Accessibility, and Interoperability, as well as the licensing types CC0 or CC BY for all public outputs. To achieve high quality data from experimental tasks, rigorous documentation of all procedures is required. The quality standards for documentation are defined in the Quality Assurance Manual (internal document). Furthermore, the dedicated work package “Evaluation” focuses primarily on establishing procedures and plans to ensure the production of high-quality research results.

¹ <https://about.zenodo.org/>

5. Other issues

5.1. Data ownership

The project will ensure that all data are owned by the appropriate parties and that any intellectual property rights (IPR) are respected. The project will also ensure that any data sharing or dissemination is conducted in compliance with relevant regulations and guidelines. Both aspects are covered under the project's DEC plan and its updated versions.

5.2. Resource allocation

Data management will be overseen under Task 1.4 where appropriate personnel resources are allocated to the coordinator KfV, but also to partners POLIS, TOI, VIAS, NTUA, VTI and DBL. Furthermore, sufficient personnel resources are assigned to the project's Ethics Advisor to address any requests related to GDPR and ethical considerations. The project budget includes funds for survey implementation, publication fees, and for the use of repositories and archives, in cases where free versions do not meet the project's requirements. The allocation of resources will be reviewed throughout the project duration and updated accordingly.

5.3. Update of the DMP

This Data Management Plan will be updated continuously and submitted midway through the project (31.10.2026) and at the end of the project (30.04.2028).

The intermediary update of the DMP will include specification for all data types and will address any issues which will come up during the first half of the project regarding data handling and the data life cycle. It will also provide an updated outline of data storage, access, and use beyond the project's completion.

References

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., ... & Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific data*, 3(1), 1-9.