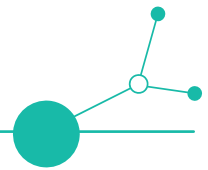# DRIVE2TRANSFORM DATA MANAGEMENT PLAN

Version 1

02 2025

1. Introduction

This document serves as the Data Management Plan (DMP) for the Drive2Transform project, ensuring compliance with data handling best practices, including the FAIR (Findable, Accessible, Interoperable, and Reusable) principles. It details how project data is collected, stored, processed, and shared while maintaining security and privacy standards in line with GDPR and Interreg Central Europe requirements.

DMP aims to present the principles and measures the consortium adopts to ensure the compliance of Drive2Transform data flows.

Each partner in the project is responsible for platforms that are used to carry out the project work. The partners collaborate to ensure that correct and compliant data, privacy, security and other procedures are followed.

The EU General Data Protection Regulation 2016/679 (GDPR) are enshrined in the practices of the Drive2Transform project. The Drive2Transform consortium is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. The consortium is dedicated to safeguarding the personal information under our remit and providing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the GDPR.

2. Data Summary

The processing of personal data that occur under Drive2Transform are related to its use in project activities (and without prejudice of the fact that in many cases the relevant entities will be legal persons and, as such, the corresponding data used for such purposes will not constitute personal data):

- Mapping: mapping of potential stakeholders for Wp activities and communication

- Promotion: sending communications by email to the professional contacts of the potential interested entities related to the relevant open calls and events.

- Implementation of activities: involving the participating entities (SMEs, BSOs, policy makers) in the Drive2Transform activities and contacting them for this purpose, e.g. event registration and participation records, webinars and video recordings

- Dissemination of results: Project website and social media analytics; producing media content, including with relation to the Drive2Transform events.

- Connection to other related initiatives: share the contact details of stakeholders with other projects if stakeholders have each given their consent.

- Logistics and administration: putting in place the necessary means for the organization of project activities, such as identification needed for security purposes or dietary requirements.

- Reporting: complying with any reporting obligations in relation to the EC under the project.

These datasets will be used for project execution, reporting, and dissemination purposes. No sensitive personal data will be published, and any personal data processing will comply with GDPR regulations.Personal data collected are processed based on consent and legitimate interests.

No personal sensitive data (defined by Article 9 of the GDPR as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (…) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation") are collected by the Drive2Transform project.

Data are collected, depending on the purpose and method of collection in machine-readable, physical, and other formats.

Data originate from multiple platforms, with different project partners responsible for the various platforms used in the delivery of the project. The project maps the platforms used in the delivery of the action to maintain a data management plan mapping. The project does not reuse any existing data unless the terms under which such data was originally supplied provide for such re-use.

The Drive2Transform project will generate various datasets, including:
- Stakeholder engagement and mapping
- Event registration and participation records
- Webinars and video recordings
- Consent to use image, audio, video and text in dissemination actions
- Project website and social media analytics
- External expert interactions
- Research and readiness assessment datasets

3. FAIR Data Management

3.1 Making Data Findable
- Metadata will be standardized and indexed to ensure discoverability.

- Unique identifiers will be assigned to datasets where applicable.

- Naming conventions will be consistent across platforms.

3.2 Making Data Openly Accessible
- Open-access data will be published via the project website and relevant repositories.

- Confidential and proprietary data will be restricted based on agreements.

3.3 Making Data Interoperable
- Standardized formats (CSV, JSON, PDF) will be used to enhance interoperability.

- Common vocabularies and metadata standards will be applied.

3.4 Increasing Data Re-use
- Licensing frameworks (e.g., Creative Commons) will be applied where possible.

- Data retention policies will follow EC and GDPR guidelines.

4. Allocation of Resources

Each partner in Drive2Transform is responsible for the application of the DMP for the data it contributes to the MS sharepoint and data that is received, stored, modified or deleted on a platform the project uses that is such partner's responsibility

5. Data Security

All consortium members must understand their data security obligations and responsibilities. Such procedures are defined in the present DMP. There is a dedicated focus on privacy by design and the rights of individuals engaged in the project. Each partner organization takes responsibility for the platforms which they contract and/or operate for the project.

Each partner reviews each of the platforms they use to deliver the project with regards to data security, data encryption, data retention, secure access, secure transfer, and the security of storage.

In sum, the Drive2Transform project maintains protection of personal data and compliance with Data Regulations as per national and European legislation regarding the protection of personal data. Procedures are in place for applicable technical means to avoid the loss, misuse, alteration, access by unauthorized persons and/or theft of the data provided to this entity. Notwithstanding, security measures (particularly for Internet accessible data) are not impregnable.

Drive2Transform participants (data owners) exercise their right to be forgotten.

Breach procedures are put in place by the consortium members to ensure that the partners are able to identify, assess, investigate, and report any reported or detected data breach at the earliest possible time.

Additionally, all consortium members were asked to adopt security measures to protect computers, laptops, mobile phones, and similar tools to prevent unauthorized access in case of leaving the tool unattended or in case of loss or theft.

6. Ethical Aspects

While no ethics issues apply to the Drive2Transform project, ethics are taken into consideration in the way data is collected, stored and regarding who can visualize and use it. The project works to ensure that management of personal data is compliant with GDPR and other applicable legal frameworks related to personal data protection. During the project, each partner considers the standards, treaties and laws regarding data protection and privacy in both EU and national level legislation. Informed consent will be obtained where required. Anonymization techniques will be applied where necessary.

7. Conclusions

This DMP ensures that Drive2Transform follows best practices in data management, security, and accessibility.