KEYSTONE

D7.3: The project's data management plan (DMP)

WP7 – Project Management

Co-funded by the European Union
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the CINEA. Neither the European Union nor the CINEA can be held responsible for them.

KEYSTONE

D7.3: The project's data management plan (DMP)

Disclaimer

This Project is co-funded under the European Framework Programme for Research and Innovation Horizon Europe. The project is also co-funded by the UK Research and Innovation (UKRI).

Deliverable details

Horizon Europe GA no.	Project acronym	Project title
101103740	KEYSTONE	Knowledgeable comprehensive and fully integrated smart solution for resilient, sustainable and optimized transport operations

Deliverable	Title	Work package
D7.3	The Project's Data Management Plan	WP7

Contractual delivery date	Project month	Actual delivery date	Delivery type	Dissemination level
30 November 2023	M6	30 November 2023	R	PU

Author(s)	Organisation
Professor Umut Turksen	Coventry University
Dr Adam Abukari	Coventry University
Dr Dimitrios Kafteranis	Coventry University

Internal Reviewers
RINA - C

Acronyms

Acronym	Meaning
AHP	Analytic Hierarchical Process
API	Application Programming Interface
CEA	Cost-Effectiveness Analysis
D	Deliverable
DoA	Description of Action
DMP	Data Management Plan
DTLF	Digital Transport and Logistics Forum
EC	European Commission
EU	European Union
FAIR	Findable, Accessible, Interoperable, and Reusable
GDPR	General Data Protection Regulation
IT	Information Technology
KGA	KEYSTONE Grant Agreement
MoM	Minutes of Meeting
Steering Committee	SC
WP	Work Package

Document history

Version	Date	Author	Summary
V0.1	01 August 2023	Coventry University	Development of structure
V0.2	01 November 2023	Coventry University	Preliminary draft of deliverable
V0.3	20 November 2023	Coventry University	Completed draft of deliverable
V0.4	23 November 2023	Coventry University	Internal review and comments
V0	29 November 2023	RINA - C	External quality review and comments
V1.0	30 November 2023	Coventry University	Final review & conversion to PDF format

Table of Contents

List of Figures

List of Tables

1. Executive Summary

The D7.3 - Data Management Plan (DMP) of the KEYSTONE project shows how the project partners collect, organise, store, share, re-use, and archive data during the lifecycle of implementing the project. The purpose of this DMP is to ensure responsible, legal, and ethical management of research data by all the KEYSTONE partners. The DMP provides relevant legal and ethical guidelines for KEYSTONE partners to comply with laws and regulations on essential data issues such as data privacy and confidentiality. To this end, the DMP serves as a catalyst for ensuring integrity and quality of KEYSTONE data. The DMP will support the project partners to critically and carefully think about how to obtain and maintain reliable, accurate and secure data.

This DMP follows the structure recommended in the Commission's findable, accessible, interoperable, and reusable (FAIR) DMP template of 26 July 2016. Informed by the FAIR template, Coventry University developed and distributed DMP questionnaires to all the KEYSTONE partners and held meetings with each of the partners to gather information and discuss any issues arising from filling the questionnaire. Relevant data from the questionnaire was integrated into the development of this deliverable.

In KEYSTONE, the data have a very important role as they are the real focus and the final goal. The KEYSTONE Consortium will carefully manage research data generated and collected during the project and the procedures have been detailed in this deliverable, pursuant to the FAIR principles. This DMP is a living document that will be regularly updated and submitted to the European Commission (EC) in Month 18 and Month 36 of the project. This version of the DMP is delivered in Month 6 (i.e., November 2023) of the project. Every partner in KEYSTONE shall take data management responsibility seriously, thus handle data ethically, legally, responsibly, and securely.

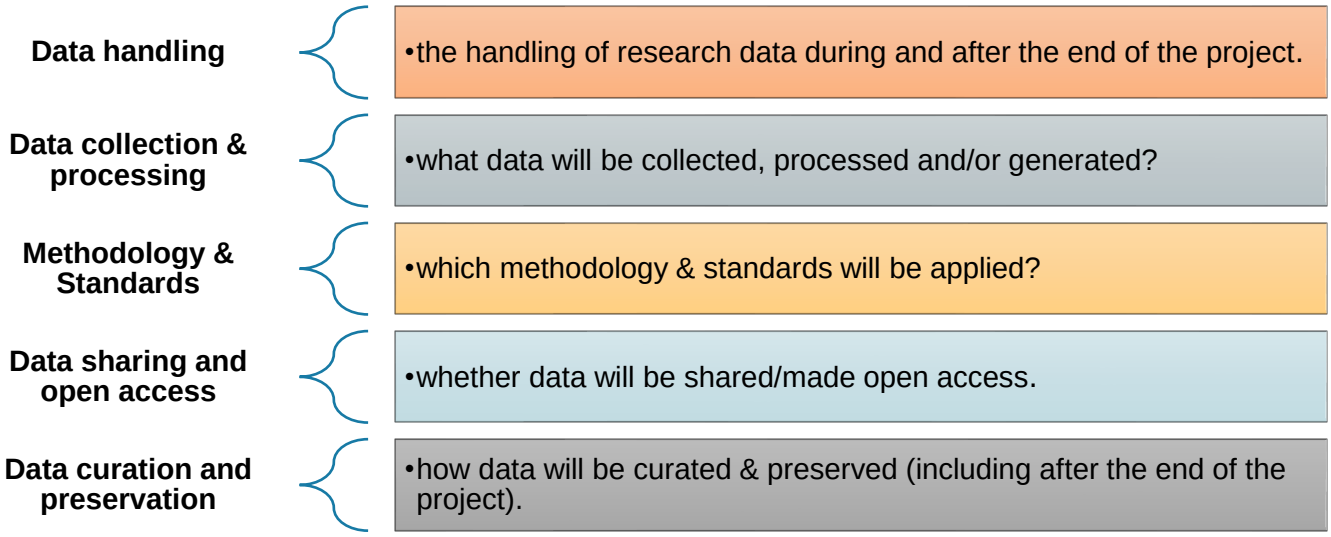
2. Introduction

2.1 Backround

This DMP corresponds to the outcome of activities performed in 'Task 7.3: Data Management' in Work Package 7 (WP7), led by Coventry University (Coventry) and contributed to by all the KEYSTONE partners. The DMP explains the management of the research data to be collected, generated, and/or processed, pursuant to the KEYSTONE Grant Agreement (KGA).

A DMP provides suitable platform and framework for sound data management in the Horizon 2020 (now Horizon Europe) research projects. Sound management of research data can be achieved if research data are managed in accordance with the dictates of the FAIR data principles. This means making research data findable, making data accessible, making data interoperable, and making data reusable in order to enhance exploitation of research data, knowledge innovation and development. According to the EC, in order to contribute to making research data FAIR, a DMP is expected to include information on the following components:[1]

Figure 1: Key Components of DMP



We have taken all the above recommended components into consideration in developing this deliverable. This DMP represents the data management and processing activities up to Month 6 (M6) of the project. KEYSTONE partners will collect, generate and/or use various datasets throughout the project lifecycle so as to conduct the relevant research to achieve KEYSTONE objectives, pursuant to the Description of Action (DoA) in the KGA. The DMP will continue to be updated during the project lifecycle based on the needs of partners, the way they will use, generate, and collect data.

At this stage, some of the partners are not yet too clear about the scope and nature of datasets with which they will be engaging later in the project. Coventry will continue to monitor data management requirements

[1] European Commission (n.d.), Data management, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm#:~:text=Rather%2C%20the%20DMP%20is%20intended,include%20a%20timetable%20for%20updates.

of all KEYSTONE partners in order to update the information in this DMP during the first review to be submitted to the EC in Month 18 and the final review to be submitted to the EC in Month 36.

2.2 Objectives and scope

The DMP's main objective is to elaborate and implement a plan to manage the production and processing of its research data and scientific publications. Pursuant to Article 4(2) of the General Data Protection Regulation (GDPR) of the European Union (EU),[2] data processing involves elements such as 'the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction' of data.[3] The Management of data in the KEYSTONE Consortium will pay attention to these elements of processing.

> *In the context of personal data, 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) GDPR).*

The DMP will follow the structure recommended in the Commission's FAIR Data Management Plan template, 26 July 2016. The DMP will describe how the use of data connected to the project will largely comply with the FAIR principles. The DMP will provide an overview of KEYSTONE data types. It will outline the applicable principles, standards and guidelines KEYSTONE will follow. The DMP will address data security, allocation of resources and compliance management.

Additionally, the DMP seeks to ensure that data, especially personal data, that is collected and processed by the KEYSTONE project is appropriately protected and compliant with the provisions of the GDPR. Each project partner handling and responsible for data collected, stored, or used in KEYSTONE will ensure compliance with the strategy and protocols outlined in this document.

For this reporting period, we are not expected to provide detailed answers to all the relevant DMP questions. Instead, this DMP is meant to be a living and working document wherein information can be made available by the project partners on a finer level of granularity through updates in the course of implementation of the project and when important changes occur in data processing and management.[4] For this reason, after

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
[3] European Commission (n.d.), What constitutes data processing? https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en#:~:text=It%20includes%20the%20collection%2C%20recording,or%20destruction%20of%20personal%20data.
[4] European Commission (n.d.), Data management, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm#:~:text=Rather%2C%20the%20DMP%20is%20intended,include%20a%20timetable%20for%20updates.

submission of this DMP in Month 6 of the project, a mechanism will be put in place to monitor and record any data processing and management changes that have taken place over time.

One of such mechanisms is that the DMP questionnaire that was initially filled by partners will all be uploaded onto KEYSTONE SharePoint (https://unimore365.sharepoint.com/sites/KEYSTONE\) with a request of partners to in an on-going basis, highlight in yellow any updates to their data processing and management conditions. Another mechanism is that partners will be requested to ensure that emerging issues/changes to data management is made a permanent feature on the agenda of the monthly steering committee meetings of the KEYSTONE consortium. Additionally, in the lead up to the middle of the project implementation, Coventry will send across provisionally updated version of this DMP (D7.3) to all partners to indicate any changes that have occurred in the respective partner institutions after M6 of the project. The result from this exercise will be sent to the EC as 'Intermediary Output: D7.4: Data Management plan report' in M18 (i.e., November 2024). The D7.4 report will equally be subjected to the same exercise as conducted on D7.3 to generate the 'Final Output: D7.5: Data Management plan report' in M36 (i.e., May 2026).

It is also within the scope of this DMP to present the institutional policies and practices of each of the partners of KEYSTONE on data management to provide an overview of data management practices in KEYSTONE. Thus, the DMP covers both personal and non-personal data, although personal data protection is relatively prioritised more than non-personal data due to the implications and important safeguards associated with personal data protection. All KEYSTONE partners must, nonetheless, comply with all the data protection and management protocols provided in this deliverable. However, the DMP does not feature any work of the partners that is external to the KEYSTONE project. We have briefly described the 6-stage lifecycle of data that symbolises the scope of the DMP in this deliverable in Table 1 below:

Table 1. Data lifecycle considered in the DMP

Component		Description
1	Planning research	This includes designing research; planning data management; planning consent for data sharing; planning data collection, processing protocols and templates; and exploring existing data sources.
2	Data collection	This includes capturing of data and metadata; and acquiring existing third-party data.
3	Processing and analysis of data	This involves entering, digitising, transcribing, and translating data; checking, validating, cleaning, and anonymising data; creating derivative data; describing and documenting data; managing and storing data; analysing and interpreting data; producing research outputs; and citing data sources.
4	Publishing and sharing data	This involves establishing copyright; creating user documentation; creating discovery metadata; electing appropriate access to data; publishing and sharing data; promoting data.
5	Preservation of data	This includes migrating data to the best formats/media; storing and backing-up data; creating preservation documents; as well as preserving and curating data.
6	Re-using data	This includes conducting secondary analysis; undertaking follow-up research; conducting research reviews; scrutinising findings; as well as using data for teaching and learning.

2.3 Structure of the report

In addition to the Executive Summary and Introduction Chapters, the DMP has 9 other Chapters as follows:.

- In Chaper 3, we explain the methodology that has been employed to gather the relevant data and information required from the 15 partners of the KEYSTONE consortium to develop this deliverable.
- Chaper 4 gives an overview of the data that will be or have been collected, gathered, used, produced, and shared in the KEYSTONE project. This section also contains an overview of the personal data processing activities to be carried out by the partners.
- Chaper 5 delves into the internal data protection and management policies used by each of our partners. Chaper 6 provides information on the FAIR principles. It also presents how the FAIR principles will be achieved in the project.
- Chaper 7 provides information on how personal data is processed and to ensure compliance with the GDPR.
- Chaper 8 shows how data security is ensured in the project.
- Chaper 9 presents ethical considerations about the data generated in KEYSTONE. Chaper 10 addresses salient elements concerning the GDPR's accountability principle.
- Chapter 10 outlines the resources allocated to the DMP and its future iterations.
- Chaper 11 is the final Chapter that concludes the DMP.
- We have also provided Annexes I and II respectively showing templates of information sheet and consent form as well as legitimate interest assessment.

3. Methodology

Coventry, with participation of all partners in the Consortium, have used the following methodology to prepare this DMP: Based on the DoA in the KGA, we first discussed the objectives and the general framework of the DMP with partners during the project kick-off meeting on 20/06/2023 and the subsequent SC meetings.

We invited each of the partners to contribute to the DMP through the questionnaires we sent out to partners on 10/07/2023. Thus, to collate relevant information on the data to be used in KEYSTONE, Coventry sent data management questionnaires to all the partners to complete.

The questionnaires were developed based on the questions in the 'Guidelines on FAIR Data Management in Horizon 2020'[5] and included relevant questions regarding the processing of personal data that fall within the scope of the GDPR. All the partners filled the questionnaire and returned them to Coventry. Coventry scheduled and held bilateral meetings with all the partners on the following dates in September and October as captured in Table 2 to discuss and clarify the answers provided in the DMP questionnaire.

[5] European Commission (2016), H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

Table 2. Meetings with partners to discuss questionnaire on the DMP

KEYSTONE Partners	Date of meeting
AETHON	28/09/2023
UPM	20/09/2023
ETELÄTÄR	28/09/2023
GRUBER LOGISTIC	13/10/2023
STA	20/10/2023
CEFRIEL	20/09/2023
T-BRIDGE	09/10/2023
TTS	20 /10/2023
AEC	09/10/2023
CIM	13/10/2023
CORTE	13/09/2023
RINA-C	25/10/2023
ICOOR	31/10/2023
UNIMORE	31/10/2023

The questionnaire has four pages/sections on Excel sheet: The instruction section, the section on non-personal data, the section on personal data, and a dedicated section on institutional policies. Generally, the questionnaire includes questions on how to comply with the FAIR principles, along with specific questions on data protection that seek to map out how data processing activities will be conducted in KEYSTONE. These include categories of data to be processed, source of data collection, legal bases, purpose of data processing, data location and sharing practices, data security, data principles, etc.

The various contributions made by partners were assimilated, synthesised, and integrated into this deliverable. Indeed, the answers to the questionnaire inform the formulation of Tables 3, and 4 in Chapter 4 and Table 5 in Chapter 5 of this DMP. After the meetings on the questionnaire, Coventry has continued to be in touch with relevant partners to receive any clarifications and updates on the answers they provided to the questionnaire.

After the submission of this deliverable, Coventry will continue to receive updates on the data processing and management changes in the consortium during the monthly SC meetings. This is to enable Coventry to have up-to-date information on any changes to data processing and management plans of the partners. This will

also ensure that the DMP can be appropriately updated from time to time whenever significant information is received from relevant partners of the Consortium.

4. KEYSTONE project's Data Overview

4.1 Status of the project in relation to data processing and management

The KEYSTONE Consortium is currently identifying relevant stakeholders and conducting meetings, focus groups and interviews with them to assess their needs and requirements. These stakeholders include logistics operators, enforcement authorities, and freight terminals. The KEYSTONE partners have also been involved in consultations, and collating data and knowledge from literature to develop their respective deliverables and technical solutions on time. There is continued exchange of information within the consortium to ensure that quality deliverables and solutions are produced.

So far, no data breach or potential breach concerns have been raised and/or noticed from the data generated and processed through these engagements, exchanges and related activities in the context of KEYSTONE.

Even though this first DMP is to be delivered in M6, the ongoing engagements with partners by Coventry on the development of the DMP have shown that, all the partners have, by far, abided by the FAIR principles and GDPR rules on data protection and management in the execution of their respective tasks. When this DMP is completed and in place, it is believed that all partners of the project will continue to act responsibly, ethically, and legally in processing and managing data related to KEYSTONE.

Coventry, together with all partners, will continue to pay attention to significant developments in data processing and management in the consortium in order to incorporate any updates in the M18 DMP (i.e., D7.4).

4.2 Summary of datasets

The personal and non-personal data collected and processed by KEYSTONE are classified into different datasets in the context of the respective WPs and tasks of KEYSTONE. The data also take a variety of formats[6] including text, images, audio, and videos. The following provides the summary of the datasets to be used and produced in KEYSTONE:

Each of the partners in KEYSTONE Consortium will process data to develop or contribute to their respective deliverables. The IT systems used by all partners include MS word, PDF, and Excel as well as KEYSTONE SharePoint to process data. Most of the partners also use Docs in their work. Other partners indicate the use of PowerPoint to process data. Although it was not captured in the DMP questionnaires, it transpired that most of the partners use PowerPoint to process data. Some partners have also indicated that they use Xml, and txt to process data.

Certain deliverables, based on their sensitivity and confidentiality, will be exclusively shared among Consortium partners and the EC. Other deliverables will be readily available to the public. Confidential materials will be stored in a secure shared folder on KEYSTONE SharePoint, which all partners of the Consortium have access to. Publicly accessible deliverables will be uploaded to the project website (https://www.keystone-project.com/), thus enhancing greater transparency dissemination and pathway to

[6] European Commission (n.d.), Data management, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm.

impact. As the project progresses, partners will actively collect a comprehensive set of academic and grey literature such as research reports, articles, working papers, and other relevant materials.

All partners of KEYSTONE will process and/or have processed contact details of colleagues within the Consortium, including processing particulars such as names, e-mail addresses and phone numbers. The following provides highlights of datasets of respective partners in KEYSTONE Consortium:

UNIMORE will collect data within WP4 (in particular, T4.1 and T4.2) for the purpose of performing Task 5.2 to produce D5.2, which will report the results of the Cost-Effectiveness Analysis (CEA) and the Analytic Hierarchical Process (AHP) aimed at studying the effectiveness of KEYSTONE solutions. It will provide a useful tool for the evaluation phase and will work as a base for the decision-making processes.

TTS will use aggregated and anonymised pilot results (i.e., from D5.2) to develop D5.4 and white paper including a roadmap of actions fostering the establishment of regulatory and policy framework supporting the large-scale deployment of a digital transport ecosystems allowing for standardisation of transport operations. By relying on the support of KEYSTONE partners, TTS will engage local, regional, and national enforcement agencies in several Member States to highlight the effectiveness of the project solution.

TB will collect data from W2 (Plug & Play framework) and T1.3 (gap analysis) to understand the current Data Management Ecosystem in KEYSTONE. TB will also collect risk data for identification and correction of possible deviations from project's goals and expected results.

RINA-C expect to collect the following data: input from WP1 (T1.3-T1.4) WP3, WP4 (T4.2-T4.4), transcripts and minutes from workshops/discussions with stakeholders, as well as reports and publications to enable RINA draft D2.5. Data from D3.1 (App design, architecture, and development plan), D3.2 (Co-created UI/UX design) and D3.3 (Cyber security infrastructure for the KEYSTONE solution) will be processed by ETELÄTÄR. Data from the business models of T2.4 are also considered.

STA will collect data from digital communication tools in terms of data concerning the usage and opt-in rate of social media channels, newsletter, website etc, to enhance its communication activities in the project.

UPM will collect data from T1.1. Focus group data to support in the development of relevant deliverables.

AETHON will, at least, have the following collection of data: input from WP1 (T1.1-T1.4), transcripts and minutes from workshops/discussions with stakeholders (experts and project coordinators), as well as their contact information, reports, frameworks, scientific publications, existing open-source standards & APIs. These will help in creating API reference model and drafting of the deliverable.

GRUBER LOGISTICS will collect data about the involvement of DTLF policies in addressing plug and play issues.

CIM will be creating data flows from Terminal System, and feeding KEYSTONE Applications, from T4.1 - Existent dataset of actual IT intermodal platform usable by enforcement authorities; from T4.2 - Dataset of intermodal IT platform usable by the project (APIs + APP), and from T4.4 - Intermodal status data collected from the platform and sent to KEYSTONE.

CEFRIEL will collect data from relevant tasks (such as T1.1, T3.2, T4.2, and T6.2), as well as relevant literature in user requirements to feed into respective deliverables.

CORTE will source data on enforcement practices and electronic tools and platforms to feed into WP1, WP2, WP4, WP5 & WP6.

AEC will collate existent dataset of enforcement procedures and interviews to enforcement authorities in order to draft deliverables such as D4.1.

ICOOR will source data from literature, previous project, evaluation working group from the FAME project to define evaluation methodology and plan so that further projects can benefit from the KEYSTONE's experience.

COVENTRY will collect data from 'T1.1 Focus group data', and relevant literature (such as in cybersecurity, ethics, and data management) in user requirements to support the development of relevant deliverables in WP1, WP3, WP5, and WP7. Data will be collected from public sources and relevant repositories including KEYSTONE SharePoint, internal SharePoint of Coventry University, and legal databases (e.g., Eur-Lex). Academic and grey literature in ethics, legal, and social impact as well as ethics codes and guidelines, legal texts, industry reports, standards, other public deliverables, and reports will be used to ensure reliability, quality, responsibleness and integrity of the data processed in the context of the KEYSTONE project.

While a few of the partners are not sure of the expected size of data to be processed, most partners have indicated that their expected data size will range between 1G to 10G. Indeed, most of the partners expect to process data size of 1G. These sizes are reasonable as far as Consortium partners only collect the data that they need to carry out their tasks in KEYSTONE and are able to securely process them.

4.3 Overview of the data to be processed in the KEYSTONE project

Table 3 provides an overview of the kind of data being processed and the information technology (IT) tools used by the partners in the KEYSTONE consortium.

Table 3. Data Overview

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
1	UNIMORE	WP5	D5.2: CEA and AHP for the KEYSTONE solutions.	Data will be collected within WP4 (in particular, T4.1 and T4.2) for the purpose of performing Task 5.2 to produce D5.2, which will report the results of the Cost-Effectiveness Analysis (CEA) and the Analytic Hierarchical Process (AHP) aimed at studying the effectiveness of KEYSTONE solutions. It will provide a useful tool for the evaluation phase and will work as a base for the decision-making processes. Evaluation analysis activities will be conducted. Contact details of partners will be used to organise meetings and exchange emails. No personal data will be collected and processed for the goal of the task. However, in order to proceed with the task activities,	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint.

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
				UNIMORE will come across personal information about the partners (mainly email address).	
		WP7	D7.1: Project Management Handbook. D7.2: Summary of the project.	Textual data from the KGA and from the SC for the purpose of developing D7.1 and D7.2. Contact details of partners will be used to organise meetings and exchange emails. No personal data will be collected and processed for the goal of the task. However, in order to proceed with the task activities, UNIMORE will come across personal information about the partners (mainly email address).	
2	TTS	WP5	D5.4: KEYSTONE evidence-based policy recommendations.	Use of aggregated and anonymised pilot results (i.e., from D5.2) to develop D5.4 and white paper including a roadmap of actions fostering the establishment of regulatory and policy framework supporting the large-scale deployment of a digital transport ecosystems allowing for standardisation of transport operations. Sharing of the White Paper developed within the Task 5.4 through numerous channels at National and International level (Italian Ministries, Local Authorities Platform, International Road Federation, Sister ITS Association all over the world including Australia, Singapore, China, and Taiwan).	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint.
		WP6	D6.1: Exploitation plans, replicability report & market uptake strategy	Use of personal data (collected from own contact network and from partners) to reach out to organisations as part of EU-wide online campaign to reach	

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
			(involves in Task 6.3: Replicability)	as many stakeholders as possible and encourage them to adopt the KEYSTONE concept. By relying on the support of KEYSTONE partners, local, regional, and national enforcement agencies in several Member States will be engaged to highlight the effectiveness of the project solution.	
3	TB	WP1	D1.3: Needs and requirements for the future digital logistics ecosystem.	Data from W2 (Plug & Play framework) and T1.3 (gap analysis) will be collected to understand the current Data Management Ecosystem and drafting of deliverables. Collection of contact detail of partners or contact points and/or request for facilitation of communication with experts to specific consortium members that have contact points, in order to organise and initiate discussions.	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint.
		WP2	D2.2: Plug & Play implementation and interconnectivity study.	EID data and CCAM data will be collected: Data from T1.3 (digital platforms data), T.4 (use cases) and T2.1 (API reference model). The object of D2.2 is information collection and elaboration on three parts of the model: in particular, interconnectivity and requirements for connecting to other platforms, information to be retrieved from those platforms and information exchange between CCAM vehicles and between vehicles and platforms.	

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
		WP3	D3.1: App design, architecture, and development plan.	Data from W2 (Plug & Play framework) and T1.3 (gap analysis) to assist in defining the requirements for the Plug & Play application. Collection of contact detail of partners or contact points and/or request for facilitation of communication with experts to specific consortium members that have contact points, in order to organise and initiate discussions.	
		WP7	D7.6: Risk Management Plan. D7.7: Risk Management Report.	Risk data collected for identification and correction of possible deviations from project's goals and expected results. Collection of contact details of partners or contact points and/or request for facilitation of communication with experts to specific consortium members that have contact points, in order to organise and initiate discussions	
4	RINA-C	WP2	D2.5: Business models and cases.	RINA expect to collect the following data: input from WP1 (T1.3-T1.4) WP3, WP4 (T4.2-T4.4), projects' deliverables (internal and perhaps sensitive ones), transcripts and minutes from workshops/discussions with stakeholders, as well as reports and publications to enable RINA draft D2.5. Contact details of experts and professionals from consortium members, Transcripts (MoM) from discussions, as well as any sensitive deliverables/documents shared by them, to enable RINA set up discussions, collect input and	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint.

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
				request for clarifications (if needed).	
		WP6	D6.1: Exploitation plans, replicability report & market uptake strategy.	Data acquisition includes input encompassing all work packages, outputs from project tasks (including those of a confidential nature), records of discussions and meetings with relevant parties, and both formal and informal documentation stemming from workshops and dialogues with stakeholders. Furthermore, reports and published materials will also be incorporated. These will be for the purpose of drafting D6.1. Contact information of specialists and professionals within the consortium's membership as well as records of conversations in the form of meeting minutes, and any confidential documents or outputs they have shared - will be gathered for the purpose of arranging discussions, gathering input, and seeking clarifications as necessary.	
5	ETELÄTÄR	WP3	D3.4: App launch and reporting.	Data from D3.1 (App design, architecture, and development plan), D3.2 (Co-created UI/UX design) and D3.3 (Cyber security infrastructure for the KEYSTONE solution) will be processed by ETELÄTÄR. Use of contact details of partners to work in a cooperative manner in the development of a web app, as well as development of market uptake strategies for the KEYSTONE solution.	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint.
		WP6	D6.1: Exploitation plans, replicability	Data from the business models of T2.4 are considered.	

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
			report & market uptake strategy (involves in Task 6.4: Market uptake).	Use of contact details of partners to work in a cooperative manner in the development of market uptake strategies for the KEYSTONE solution.	
6	STA	WP6	D6.3: Communication & dissemination plan and visual identity handbook. D6.4: Communication & dissemination plan update. D6.5: Final communication & dissemination report.	Newsletter subscribers for distribution to a list of subscribers. Data from digital communication tools in terms of Data concerning the usage and opt-in rate of social media channels, newsletter, website etc, will be processed.	PDF. Excel. MS Word. KEYSTONE SharePoint. Squarespace. Twitter. LinkedIn web.
7	UPM#	WP1	D1.2 Focus groups report including stakeholders' requirements and expectations.	Data from T1.1. Focus group data to develop deliverables. Contact details of partners and participants of stakeholder focus groups to organise meetings and focus groups as well as carry out recordings and transcripts of the focus group discussions to understand their requirements and expectations.	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint.
8	AETHON	WP2	D2.1: API Reference Model. D2.3: API standard. D2.4: API standard V2.	AETHON expect to have, at least, the following collection of data: input from WP1 (T1.1-T1.4), projects' deliverables (internal and perhaps sensitive ones), transcripts and minutes from workshops/discussions with stakeholders (experts and project coordinators), as well as their contact information, reports, frameworks, scientific publications, existing open-source standards & APIs. These will help in creating API	PDF. Excel. MS Word. KEYSTONE SharePoint.

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
				reference model and drafting of the deliverable. Contact details of experts and professionals reached to conduct interviews and discussion with, provided by consortium members - Also contact details of consortium members, domain experts and stakeholders' reference persons, in order to organise and initiate discussions. Transcripts (MoM) from discussions, as well as sensitive deliverables/documents they may share will also be processed.	
9	GRUBER LOGISTICS	WP1	D1.4: Digital ecosystem framework	Data on digital ecosystem from previous public project and their connection with private needs to draft deliverables. Gruber Logistics, with a strong commitment to upholding the highest standards of data privacy and protection, will conscientiously process and handle data on contact details of partners and stakeholders in strict accordance with all relevant regulatory frameworks, diligently adhering to privacy laws, rights, and safeguards. The company will exercise utmost caution and discretion, ensuring that personal data is managed exclusively within the boundaries and objectives of the KEYSTONE project, with the sole purpose of fulfilling its designated aims and objectives, and no other.	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint. MS Power Point. JPGs.
		WP4	D4.3: Pilots Activities.	Data on pilot related to road transport to draft deliverables.	

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
		WP5	D5.3: Evaluation with the DTLF working group.	Data about the involvement of DTLF policies in addressing plug and play issues.	
10	CIM#	WP4	D4.3: Pilots Activities (involves in Task 4.4: intermodal digital ecosystem).	Creating data flows from Terminal System, and feeding KEYSTONE Applications, from T4.1 - Existent dataset of actual IT intermodal platform usable by enforcement authorities; from T4.2 - Dataset of intermodal IT platform usable by the project (APIs + APP), and from T4.4 - Intermodal status data collected from the platform and sent to KEYSTONE. Use of contact details of partners to design pilot environment and support relevant WPs in surveying the stakeholders of intermodal world.	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint. Xml. txt.
11	CEFRIEL	WP1	D1.1: Stakeholders' identification and needs	Survey answers from T1.1, as well as relevant literature in user requirements to draft deliverables. Contact details (external to KEYSTONE project) are collected for sending them an invitation for participating in the survey and obtaining an explicit consensus to be included in a stakeholder register. Recordings and transcripts of the interview meetings are also processed to develop the deliverable.	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint.
		WP3	D3.2: Co-created UI/UX design.	Data from T3.2, as well as relevant literature in user requirements is used to develop D3.2. Contact details of partners and stakeholders (external to	

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
				KEYSTONE project) as well as recordings and transcripts of the interview meetings are used to follow up on app user interface needs.	
		WP4	D4.2: Definition and specification of the operational scenarios.	Data from T4.2, as well as relevant literature in user requirements is used to develop D4.2. Contact details of partners and stakeholders (external to KEYSTONE project) as well as recordings and transcripts of the interview meetings are used to follow up on the activities of the demonstration scenarios.	
		WP6	D6.2: Stakeholders' engagement report.	Data from T6.2, as well as relevant literature in user requirements is used to develop D6.2. Contact details of partners and stakeholders (external to KEYSTONE project) as well as Recordings and transcripts of the interview meetings are used to follow up on the activities of the project.	
12	CORTE#	WP1, WP2, WP4, WP5 & WP6	As per the project description no specific tasks have been assigned to CORTE. But CORTE play a role in stakeholder engagement as well as collection of inputs from end-users for developing KEYSTONE solutions.	Data on enforcement practices and electronic tools and platforms are used to support these WPs. Contact details of involved project partners, stakeholders, and experts to collect contact points and/or request for communication with experts/professional in order to set up discussions, collect input and request for clarifications (if needed).	PDF. Excel. MS Word. KEYSTONE SharePoint.
13		WP4	D4.1: Process and procedures	Existent dataset of enforcement procedures and interviews to	PDF. Excel.

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
	AEC		report based on the concrete use cases.	enforcement authorities in order to draft deliverables. Use of contact details of enforcement authorities to compare existing enforcement procedures and operability of the pilots for enforcement authorities (particularly police).	MS Word. Docs. KEYSTONE SharePoint.
14	ICOOR	WP5	D5.1: Evaluation Methodology and Plan.	Data from literature, previous project, evaluation working group from the FAME project will be used to define evaluation methodology and plan so that further projects can benefit from the KEYSTONE's experience. Contact details of partners will be used to organise meetings and exchange emails. No personal data will be collected and processed for the goal of the task. However, in order to proceed with the task activities, ICOOR will come across personal information about the partners (mainly email address).	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint
15	COVENTRY	WP1	D1.2: Focus groups report including stakeholders' requirements and expectations.	Data from 'T1.1 Focus group data', and relevant literature in user requirements are used to support the development of D1.2. Data will be collected from stakeholders in focus groups, from public sources and relevant repositories including KEYSTONE SharePoint. Collating contact details of partners and participants of stakeholder focus groups to organise meetings. Focus group discussions with stakeholders to understand their requirements and expectations. Recordings and	PDF. Excel. MS Word. Docs. KEYSTONE SharePoint. Internal SharePoint.

Number	Short name	WP	Deliverables involved in	Data overview	IT tools
				transcripts of the focus group discussions will be used.	
		WP3	D3.3: Cyber security infrastructure for the KEYSTONE solution	Data from T1.2, as well as relevant literature in cybersecurity will be collected. Data will be collected from public sources and relevant repositories including KEYSTONE SharePoint. Use of contact details of partners to follow up on data management requirements.	
		WP5	D5.5: Conduct an ethical, data protection and societal impact assessment on the use of KEYSTONE technologies.	Academic and grey literature in ethics, legal, and social impact as well as ethics codes and guidelines, legal texts, industry reports, standards, other public deliverables, and reports will be used to develop relevant deliverables. Data will be collected from public sources and relevant repositories including legal databases (e.g., Eur-Lex). Use of contact details of partners to follow up on data management requirements.	
		WP7	D7.3: The project's data management plan D7.4: Data Management plan report (1) D7.5: Data Management plan report (2)	Academic and grey literature in data management as well as FAIR Data Management Plan (DMP) template will be used to draft D7.3, D7.4 and D7.5. Use of contact details of partners to follow up on data management requirements.	

 # means a partner that does not lead a deliverable but contributes to tasks that result in producing a deliverable. This includes UPM, CIM and CORTE.

4.4 Overview of personal data to be processed in the KEYSTONE project

This section seeks to provide an overview of the personal data processing at the different stages of KEYSTONE on each of the versions of the project's DMP. The data in Table 4 below pertains to the M6 version of the DMP.

Table 4. Overview of personal data

Number	Short name	WP	Processing	Legal basis
1	UNIMORE	WP5	Evaluation analysis activities will be conducted. Contact details of partners will be used to organise meetings and exchange emails. No personal data will be collected and processed for the goal of the task. However, in order to proceed with the task activities, UNIMORE will come across personal information about the partners (mainly email address), which could be only shared internally for the purpose of performing tasks with other beneficiary partners.	Informed consent. Performance of KEYSTONE contract.
		WP7	Contact details of partners will be used to organise meetings and exchange emails. No personal data will be collected and processed for the goal of the task. However, in order to proceed with the task activities, UNIMORE will come across personal information about the partners (mainly email address), which could only be shared internally for the purpose of performing tasks with other beneficiary partners.	
2	TTS	WP5	Use of aggregated and anonymised pilot results (i.e., from D5.2) to develop D5.4 and white paper including a roadmap of actions fostering the establishment of regulatory and policy framework supporting the large-scale deployment of a digital transport ecosystems allowing for standardisation of transport operations. No personal data sharing is expected internally or externally at this point.	Performance of KEYSTONE contract.
		WP6	Use of personal data (collected from own contact network and from partners) to reach out to organisations as part of EU-wide online campaign to reach as many	

Number	Short name	WP	Processing	Legal basis
			stakeholders as possible and encourage them to adopt the KEYSTONE concept. Data will only be shared internally for the purpose of performing project tasks.	
3	TB	WP1	Data from W2 (Plug & Play framework) and T1.3 (gap analysis) will be collected to understand the current Data Management Ecosystem and drafting of deliverables. Partners' contact details will be collected for the purpose of facilitating communication with experts to specific consortium members that have contact points, in order to organise and initiate discussions. Data is not expected to be shared externally to third parties.	Informed Consent. Performance of KEYSTONE contract.
		WP2	Data from T1.3 (digital platforms data), T.4 (use cases) and T2.1 (API reference model) will be processed to develop D2.2. Contact details and role of contact in organisation will be processed and shared for the purpose of drafting relevant deliverables.	
		WP3	Collection of contact detail of partners or contact points and/or request for facilitation of communication with experts to specific consortium members that have contact points, in order to organise and initiate discussions. Data will only be shared internally.	
		WP7	Collection of contact detail of partners or contact points and/or request for facilitation of communication with experts to specific consortium members that have contact points, in order to organise and initiate discussions. Data will only be shared internally.	
4	RINA-C	WP2	Contact details of partners collected will not be shared with other beneficiaries, but only the processed data (no personal Data) will be shared in order to carry out the Project.	Informed consent. Performance of KEYSTONE contract.
		WP6	Contact information of specialists and professionals within the consortium's membership as well as records of conversations in the form of meeting minutes, and any confidential documents or	

Number	Short name	WP	Processing	Legal basis
			outputs they have shared - will be gathered for the purpose of arranging discussions, gathering input, and seeking clarifications as necessary. No, the data itself will not necessarily be shared with other beneficiaries, but only the processed data (no personal Data) in order to carry out the Project.	
5	ETELÄTÄR	WP3	Use of contact details of partners to work in a cooperative manner in the development of a web app, as well as development of market uptake strategies for the KEYSTONE solution. Thus, the data will be shared with other beneficiaries for the purpose of carrying out the tasks on the Project.	Informed consent. Performance of KEYSTONE contract.
		WP6	Use of contact details of partners to work in a cooperative manner in the development of market uptake strategies for the KEYSTONE solution. That means, the data will be shared with other beneficiaries for the purpose of conducting the relevant tasks of the Project	
6	STA	WP6	Data from digital communication tools in terms of Data concerning the usage and opt-in rate of social media channels, newsletter, website etc, will be processed. No personal data is expected to be shared internally or externally.	Informed consent. Performance of KEYSTONE contract.
7	UPM	WP1	Contact details of partners and participants of stakeholder focus groups to organise meetings and focus groups as well as carry out recordings and transcripts of the focus group discussions to understand their requirements and expectations. Personal data will be shared only internally but not externally.	Informed consent. Performance of KEYSTONE contract.
8	AETHON	WP2	Contact details of experts and professionals reached to conduct interviews and discussion with, provided by consortium members - Also contact details of consortium members, domain experts and stakeholders' reference persons, in order to organise and initiate discussions. The contact details are expected to only be internally shared to build the reference model for the API and proceed with building	Informed consent. Performance of KEYSTONE contract.

Number	Short name	WP	Processing	Legal basis
			the API standard that will benefit the project, its pilots and assist in achieving the overachieving goal of the project	
9	GRUBER LOGISTICS	WP1	Gruber Logistics will responsibly share the data with other beneficiaries to fulfil their tasks on the project. They prioritize data privacy, sensitivity, and respect for confidentiality throughout this process. No external sharing of data is anticipated.	Informed consent. Performance of KEYSTONE contract.
		WP4	Gruber Logistics will responsibly share the data with other beneficiaries to fulfil their tasks on the project. They prioritize data privacy, sensitivity, and respect for confidentiality throughout this process. No external sharing of data is anticipated.	
		WP5	Gruber Logistics will responsibly share the data with other beneficiaries to fulfil their tasks on the project. They prioritize data privacy, sensitivity, and respect for confidentiality throughout this process. No external sharing of data is anticipated.	
10	CIM	WP4	Use of contact details of partners to design pilot environment and support relevant WPs in surveying the stakeholders of intermodal world. Contact details will be shared only internally, especially with GRUBER Logistics, CEFRIEL, and AETHON and with all the other beneficiaries to carry out the tasks of the project.	Performance of KEYSTONE contract.
11	CEFRIEL	WP1	Contact details (external to KEYSTONE project) are collected for the purpose of sending them an invitation for participating in the survey and obtaining an explicit consensus to be included in a stakeholder register. Yes, the data might be shared with other beneficiaries to carry out the tasks on the Project. No external sharing of this data is anticipated.	Informed consent. Performance of KEYSTONE contract.
		WP3	Contact details (external to KEYSTONE project) are collected for the purpose of sending them an invitation for participating in the survey and obtaining an explicit consensus to be included in a stakeholder register. Yes, the data might be shared with other beneficiaries to carry out the tasks on	

Number	Short name	WP	Processing	Legal basis
			the Project. No external sharing of this data is anticipated.	
		WP4	Contact details (external to KEYSTONE project) are collected for the purpose of sending them an invitation for participating in the survey and obtaining an explicit consensus to be included in a stakeholder register. Yes, the data might be shared with other beneficiaries to carry out the tasks on the Project. No external sharing of this data is anticipated.	
		WP6	Contact details (external to KEYSTONE project) are collected for the purpose of sending them an invitation for participating in the survey and obtaining an explicit consensus to be included in a stakeholder register. Yes, the data might be shared with other beneficiaries to carry out the tasks on the Project. No external sharing of this data is anticipated.	
12	CORTE	WP1, WP2, WP4, WP5 & WP6	Contact details of involved project partners, stakeholders, and experts to collect contact points and/or request for communication with experts/professional in order to set up discussions, collect input and request for clarifications (if needed). Thus, only internal sharing of this data is expected.	
13	AEC	WP4	Use of contact details of enforcement authorities to compare existing enforcement procedures and operability of the pilots for enforcement authorities (particularly police). Yes, the data will be shared with other beneficiaries to carry out the tasks on the Project.	Performance of KEYSTONE contract.
14	ICOOR	WP5	Contact details of partners will be used to organise meetings and exchange emails. No personal data will be collected and processed for the goal of the task. However, in order to proceed with the task activities, ICOOR will come across personal information about the partners (mainly email address). Yes, contact data will be shared with other beneficiaries to carry out the tasks on the Project.	Informed consent. Performance of KEYSTONE contract.
15		WP1	Collating contact details of partners and participants of stakeholder focus groups to	Informed consent.

Number	Short name	WP	Processing	Legal basis
	COVENTRY		organise meetings. Yes, the data will be shared with other beneficiaries to carry out the tasks on the Project. No external data sharing is expected.	Performance of KEYSTONE contract.
		WP3	Use of contact details of partners to follow up on data management requirements. The data will be shared with other beneficiaries to carry out the tasks on the Project. No external data sharing is expected.	
		WP5	Use of contact details of partners to follow up on data management requirements. The data will be shared with other beneficiaries to carry out the tasks on the Project. No external data sharing is expected.	
		WP7	Use of contact details of partners to follow up on data management requirements. The data will be shared with other beneficiaries to carry out the tasks on the Project. No external data sharing is expected.	

5. Applicable data management policies and procedures

As the DMP is an important document that presents how research data should be properly managed throughout the lifecycle of the project right from collection, organisation, storage, preservation, and down to sharing or disposal or even re-use of data,[7] organisations are expected to establish appropriate policies and procedures that symbolise an institutional framework and foundation to develop and operationalise the DMP. The following table presents the data management policies and procedures by the various partners of KEYSTONE in the nutshell.

Table 5. Overview of data management policies and procedures

Number	Short name	Data management policy and procedures in your institution
1	UNIMORE	KEYSTONE project deliverables will be available in the project SharePoint https://unimore365.sharepoint.com/sites/KEYSTONE\. The server is hosted in the Microsoft cloud in physical locations in the European Union. The backup and resilience policies are those by Microsoft and guarantee high level of safety. For more information see https://learn.microsoft.com/en-us/compliance/assurance/assurance-sharepoint-onedrive-data- resiliency.

[7] European Commission (n.d.), Data management, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm#:~:text=Rather%2C%20the%20DMP%20is%20intended,include%20a%20timetable%20for%20updates.

Number	Short name	Data management policy and procedures in your institution
		UNIMORE has a dedicated person responsible for the protection of personal data is a figure, mandatory for public bodies, provided for by Art. 37 of Regulation (EU) 2016/679 on the protection of personal data. This is a person who carries out support and control, consultative, training and information functions relating to the application of the Regulation itself. He/she cooperates with the Authority and constitutes the point of contact, also with respect to interested parties, for issues related to the processing of personal data (Articles 38 and 39 of the Regulation). More information: https://www.unimore.it/dpo.html.
2	TTS	The store and protection of the data in TTS Italia works as follows: all the computers used for recording the data are password protected; processed data is encrypted, replicated locally and in cloud servers. TTS uses an external hosting service, provided by the company Azigoo, with the servers being located in France.
3	TB	T Bridge, as a Company Controlled by BV-Tech S.p.A., applies the data management and data protection policy defined in the Group Rules Document "Regolamento Privacy Aziendale - Politica organizzative e di sicurezza in materia di protezione dei darti personali", that complies with GPRD - Regulation (EU) 2016/679 of the European Parliament and of the Council. Such compliance is ensured by a Group Data Protection Officer. In particular, the Company privacy policies can be found at https://www.tbridge.it/images/stories/TBridge_Privacy_Policy.pdf. Here you can download and consult the Privacy Policy of BV TECH S.p.A. https://www.bv-tech.it/wp-content/uploads/2020/04/Privacy-Policy_3-2.pdf.
4	RINA-C	Information security controls are implemented within RINA's Corporate ICT services in line with the Information Security Management System whose principles, guidelines and rules are articulated according to the structure suggested by Annex A of ISO/IEC 27001. Accordingly, RINA-C has in force policies, codes, and procedure for data management, among which: Code of Ethics Organizational Privacy and Data Protection Model Security Policy Information Security Manual Information Security Controls Manual. In addition, RINA-C refers also to external references, in particular to GDPR and national legislations. https://www.rina.org/en/privacy.
5		In the case of users of the web app application to be developed in the context of the KEYSTONE project, the subjects have to give their explicit consent to allow Etelätär Innovation and their employer to process personal data for a specific purpose. For this, the following aspects are of importance: • Request for consent is prominent and separate and is written in clear, plain, easy to understand language. • It should include The identity and the contact details of the Controller The purposes of the processing

Number	Short name	Data management policy and procedures in your institution
	ETELÄTÄR	The recipients of the personal data the period for which the personal data will be stored The existence of the subject's rights to: request access / rectification / erasure / restriction of processing, object to processing, data portability, withdraw consent, lodge a complaint with a supervisory authority The existence of automated decision-making, including profiling. If this exists, then meaningful information should be provided about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. • Subjects should be asked to positively opt in • Subjects should be asked to consent separately to different purposes and types of processing • Consent is not a precondition of the service and subjects who wish to withdraw their consent are not penalised. Each subject has a set of rights, which each natural person needs to be informed of before consenting to the collection of data: • Right to be informed: Individuals have the right to be informed in case that any personal data is collected and how it is handled and processed. • Right of access: Individuals have the right to obtain confirmation as to whether or not personal data are being processed. The subjects should be aware and should be able to verify the lawfulness of the processing. If requested, proof must be provided without delay, at the latest within one month of receipt of the request. • Right to rectification: Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete. If requested, a response should be given within one month from the request. • Right to erasure: Individuals can request the erasure of their personal data under specific circumstances: when data is no longer necessary, when the individual withdraws their consent, when the individual objects to the processing. • Right to data portability: This right allows individuals to obtain and reuse their personal data for their own purposes across different services. Therefore, personal data should be easily copied, moved, transferred from one IT environment to another in a safe and secure way and free of charge. This means that, if requested by the subject, personal data should be provided in a structured, commonly used, and machine-readable form (for example as a csv file). • Rights related to automated decision-making including profiling: Profiling includes algorithms to analyse or predict behaviour, location, or movements. Automated decision making must not concern underage persons and must not be based on processing special categories of data. In such cases: Meaningful information about the logic involved in profiling should be provided together with the significance and consequences. Appropriate mathematical or statistical procedures should be involved for the profiling. Measures to enable the correction of inaccuracies and to minimise risk of errors should be implemented.
6	STA	STA has a document at https://www.smart-transportation.org/data-and-privacy-policy-sta that lays down its Data and Privacy policy.

Number	Short name	Data management policy and procedures in your institution
7	UPM	UPM follows a number of data management and data protection policies in its research activities including: (i)Regulation 2016/679 - Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); (ii) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; (iii) Ley Orgánica 6/2001, de 21 de diciembre, de Universidades; (iv) Statutes of the Polytechnic University of Madrid. Decree 74/2010, of October 21(BOCM November 15). Partial Amendment: Decree 26/2018, of April 3 (BOCM, April 9).
8	AETHON	AETHON follows the data management and data protection policy of the The Guidelines on FAIR Data Management in Horizon 2020 (V. 3.0, July 2016); AETHON respects and follows the European Commission Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 and has a collaboration with a privacy legal professional for all data protection matters.
9	GRUBER LOGISTICS	Gruber Logistics will utilize the data provided solely for the specific purposes of research and job-related activities pertaining to this particular project. It is important to note that our data treatment policy strictly adheres to the highest standards of protection, confidentiality, and privacy. Sensitive data issues are given significant consideration, and robust measures are in place to ensure the security of all entrusted information. Rest assured that under no circumstances will any data, whether of public or private nature, be divulged, disclosed, or made accessible to any third parties. At Gruber Logistics, great importance is placed on maintaining the utmost confidentiality and respect for privacy. Gruber Logistics is fully committed to handling data with the utmost care and understanding the sensitive nature surrounding data-related matters. If there are any concerns or a need for further clarification, please feel free to contact Gruber Logistics.
10	CIM	CIM S.p.A. through its Terminal company manages all intermodal traffic from and to the Rheine-Alpine corridor. To perform all the activities, CIM uses a data transmission system to register and send to all stakeholders every status of the intermodal transport chain (i.e., Train dep and arr, ETA, ATA, UTI load/unload etc.). All data are encrypted and exchanged through an owned system named EDIGES, where each subject is identified and well known. CIM SpA follows GDPR rules in terms of anonymization and data management. Data Management privacy is charged by IT department, under supervision of the General Direction of the group. Our systems are protected by antivirus network platform equipped with a 24h controlled system that generates an alert in presence of a threat. Third parties that want to access our digital information must send a specific request and wait for our feedback.

Number	Short name	Data management policy and procedures in your institution
11	CEFRIEL	CEFRIEL follows a number of data management and data protection policies in its research activities including: The Guidelines on FAIR Data Management in Horizon 2020 (V. 3.0, July 2016); Website Cookies Standard: https://www.cefriel.com/privacy-policy/?lang=en
12	CORTE	CORTE is committed to respecting the privacy of its members and treating their personal data with strict confidentiality in accordance with applicable data protection laws. The information on the data CORTE collects, the purpose for which it is collected, the way it is used and stored as well as the rights data providers have with respect to their data, can be found in CORTE's data privacy statement here: https://www.corte.be/images/CORTE_DATA_PRIVACY_STATEMENT.pdf.
13	AEC	AEC will utilize the data provided solely for the specific purposes of research and job-related activities pertaining to this particular project. At AEC, great importance is placed on maintaining the utmost confidentiality and respect for privacy, and under no circumstances will any data, whether of public or private nature, be divulged, disclosed, or made accessible to any third parties. Our data treatment policy adheres to the standards of protection, confidentiality, and privacy: https://www.aecarretera.com/politica-de-privacidad.
14	ICOOR	ICOOR is a consortium of several Italian universities: each university has its own organisational policy.
15	COVENTRY	Coventry follows a number of data management and data protection policies in its research activities including: The Guidelines on FAIR Data Management in Horizon 2020 (V. 3.0, July 2016); Coventry Policy on Research Data Management and Sharing; and general information on security and data protection policy - https://www.coventry.ac.uk/legal-documents/information-security-policy/. Furthermore, Coventry has the following standards and processes in relation to data management and protection: Consent Management Standard; Data Protection Impact Assessment Standard; Direct Marketing Standard; Freedom of Information Requests; Records Retention and Management Standard; Data Breaches Standard; Data Protection by Design and Default Standard; Data Sharing and Data Processing Agreements; Data Subject Rights Standard; Disclosure of Personal Data to Third Parties Standard; International Data Transfers Standard; Privacy Notices Standard; Records of Processing Activities Standard; and Website Cookies Standard. https://www.coventry.ac.uk/the-university/gdpr-and-data-protection/.

By complying with the established data policies and procedures, KEYSTONE partners can be in a better position to responsibly, ethically, legally, efficiently, and securely handle research data. It comes with interesting benefits when standard data policies are operationalised. These include but not limited to promotion of data integrity and quality; promoting the FAIR principles; facilitation of sharing of data and collaboration; promoting ethical and legal compliance; enhancing company's brand and performance; as well as ensuring data reliability, predictability, and security.

6. The FAIR principles

According to the Horizon 2020 Programme Guidelines on "FAIR" Data Management, making data "FAIR" does allow the data to be managed soundly,[8] which fosters better science through enabling reproducibility of results and reuse of data for any future experiments.[9]

This section shows how the KEYSTONE project will, as much as possible, adhere to the FAIR principles. KEYSTONE will, in this regard, be guided by the 'as open as possible, as closed as necessary' principle, with a focus on 'encouraging sound data management as an essential part of research best practice'.[10]

6.1 Open science - research data management

Open science seeks to ensure that everyone has more transparent access to research and scholarly communication. The idea is that research should be made freely available to everyone, in order that it can be built upon and better used for the benefit of the society. Practices included in open science include open access publishing, open data, as well as open-source software.

The partners of KEYSTONE must responsibly manage the digital research data generated in the action ('data'), in line with the FAIR principles and pursuant to the KGA, by taking all of the following actions:

- As soon as possible and within the deadlines set out in the DMP, deposit the data in a trusted repository; if required in the call conditions, this repository must be federated in the EOSC in compliance with EOSC requirements.

- As soon as possible and within the deadlines set out in the DMP, ensure open access - via the repository - to the deposited data, under the latest available version of the Creative Commons

[8] European Commission (2016), H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.
[9] Mark D. Wilkinson et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship, Nature Scientific Data, 3 (160018).
[10] European Commission (n.d.), Data management, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm#:~:text=Rather%2C%20the%20DMP%20is%20intended,include%20a%20timetable%20for%20updates.

Attribution International Public License (CC BY) or Creative Commons Public Domain Dedication (CC 0) or a licence with equivalent rights, following the principle 'as open as possible as closed as necessary', unless providing open access would in particular: be against the beneficiary's legitimate interests, including regarding commercial exploitation, or be contrary to any other constraints, in particular the EU competitive interests or the beneficiary's obligations under this Agreement.

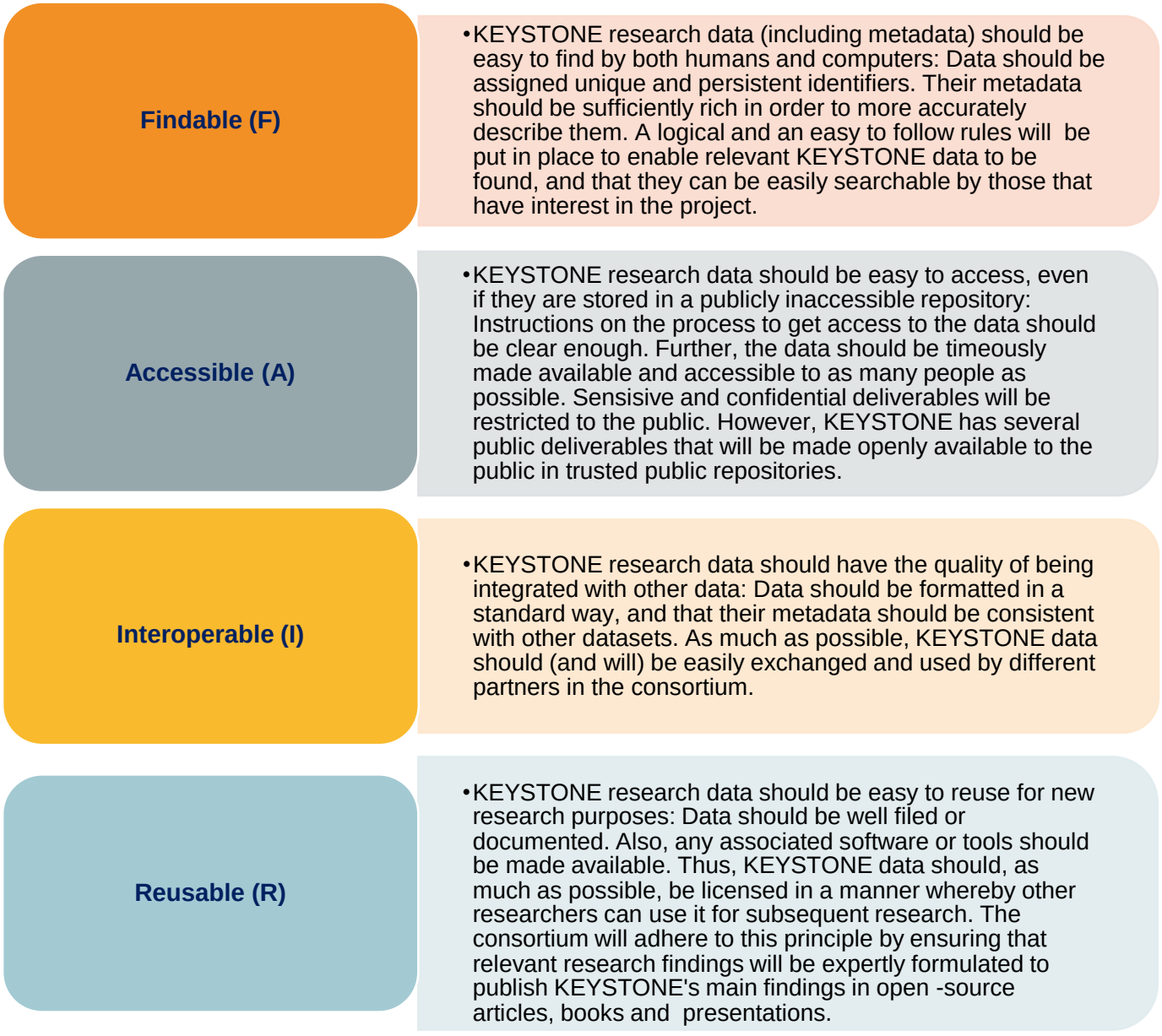
- Provide information via the repository about any research output or any other tools and instruments needed to re-use or validate the data.

Metadata of KEYSTONE data that has been deposited must be open under a Creative Common Public Domain Dedication (CC 0) or equivalent (to the extent legitimate interests or constraints are safeguarded), in line with the FAIR principles (in particular machine-actionable) and provide information at least about the following: datasets (description, date of deposit, author(s), venue and embargo); Horizon Europe or Euratom funding; grant project name, acronym and number; licensing terms; persistent identifiers for the dataset, the authors involved in the action, and, if possible, for their organisations and the grant. Where applicable, the metadata must include persistent identifiers for related publications and other research outputs.

Open science and research data management are essential for ensuring that research is transparent, reproducible, and accessible to everyone. Following best practices for research data management, can help KEYSTONE partners to make their research more impactful and beneficial to the society.

Open research data management has a number of advantages such as increased transparency and reproducibility of research, increased data reuse and innovation, increased collaboration and sharing of research findings, as well as reduced duplication of effort in research. Open research is also critical to the FAIR principles.

Figure 2. The FAIR Principles in the nutshell



The following sections will explore each of the principles of FAIR in the context of KEYSTONE.

6.2 Making data findable

Generally, most of the data of KEYSTONE that is produced, being produced, will be produced and/or used by the partners is or will be findable, as they can be identifiable and discoverable. Out of the thirty-three (33) deliverables of KEYSTONE, only seven (7) of them are likely to lack the capacity to be findable mainly because of their classification in the KGA as of sensitive nature, requiring confidentiality and restrictive dissemination. Table 6 has provided matrix presentation of all the deliverables in the project and their position in relation to the FAIR principles.

It is beneficial for the KEYSTONE Consortium to make data easily findable. This is because it will enable partners to carry out their tasks more efficiently. It is also advantageous to reviewers and EC who can easily access the information they need to conduct their reviews. Additionally, findable data is beneficial for future researchers and the public as they are more likely to be able to understand the project and use its outputs if they can easily access the different documents of the project. But because of the sensitive nature of some data, these shall be kept exclusive to the Consortium partners and EC. In such a situation, the consortium should be able to establish processes to follow to make the data findable by the partners.

The KEYSTONE Consortium has taken the following measures to make the project largely finable:

Location: Working documents used in the project are stored in folders on the KEYSTONE SharePoint dedicated folders for the project, where documents are stored and are accessible by all partners. All public deliverables will be available on the project website. Any datasets which are publicly shareable will be made available on common data repositories.

Naming of files: In the KEYSTONE SharePoint dedicated folders, and on partners own machines, files are all titled according to the task or deliverable which they relate to. Partners title documents with clear version numbers and dates where it is necessary to distinguish similar files.

Documenting contributors: All deliverables have a common frontmatter which includes a table on history of revisions. Partners fill out this table to indicate the updates they have made to files, and the date these updates took place.

All the public deliverables in the project will be findable both within and outside KEYSTONE. However, the sensitive deliverables can only be largely findable within the consortium.

6.2.1 KEYSTONE (collaborative space) SharePoint

The KEYSTONE Consortium uses a dedicated SharePoint space for the KEYSTONE project whereby partners can store, share, and access any document including deliverables for the project. This access to SharePoint has been provided by UNIMORE (the project coordinator), who has granted access to the platform for all KEYSTONE partners. The SharePoint of KEYSTONE is a secure cloud storage service provided by Microsoft which servers are located within the EU.[11] All partners have access to the SharePoint through a unique user account and password of their choice.

KEYSTONE project deliverables that are public will be available on the project SharePoint https://unimore365.sharepoint.com/sites/KEYSTONE\. The server is hosted in the Microsoft cloud in physical locations in the European Union. The backup and resilience policies are provided by Microsoft and guarantee high level of safety.

[11] Microsoft data locations in the EU, https://docs.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide.

In terms of Findable and Accessible data, KEYSTONE ensures generated data will be findable (i.e., identifiable and easily discoverable). For this purpose, metadata based on the OpenAIRE guidelines for Data Archives will be created. OpenAIRE has adopted the DataCite Metadata Schema v3.1 and, apart from a Digital Object Identifier (DOI), accepts also other persistent identifier schemes, such as Archival Resource Key (ARK), Handle, Persistent Uniform Resource Locator (PURL), Uniform Resource Name (URN), and Uniform Resource Locator (URL). All the data will include a unique User ID and a timestamp allowing for proper indexing and handling of the stored data. Additionally, the project data will be offered under Creative Commons License Attribution-Non-Commercial CC, BY-NC2, which is a machine-readable license to make most of deliverables accessible.

6.3 Making data accessible

The KEYSTONE project will comprehensively follow relevant recommendations and the EU requirements, legislation, and policies in relation to open science, data management, curation, and storage. Partners will follow the "Recommendation on Access to Research Data from public funding" revised in January 2021 that aims to share data and results to have many potential benefits (i.e., more accurate verification of results, reduction of duplications research, studies, and projects). KEYSTONE is a project that aims to collect knowledge and spread it as widely as possible. All these innovations, together with the actual knowledge that will be collected and elaborated, will be available to all the interesting stakeholders and researchers.

In order to share data efficiently, the partners agree to develop a tool that could give a direct answer to the stakeholders' needs. All the knowledge that will be created and elaborated through KEYSTONE will be broadly accessible so that KEYSTONE outputs can reach as many interested parties as possible. Furthermore, sharing the results will help the citizens' trust in science. This allows, in the future, easier citizens involvement in research and projects. It shall also allow easier commercialisation of the results as the project's findings are open.

KEYSTONE values open access to our deliverables, although seven of the deliverables are not accessible to the public. These are D5.5 Conduct an ethical, data protection and societal impact assessment on the use of KEYSTONE technologies; D7.1 Project Management Handbook; D7.2 Summary of the project; D7.4 Data Management plan report (1); D7.5 Data Management plan report (2); D7.6 Risk Management Plan; and D7.7 Risk Management Report. These deliverables are drawn from only two WPs, thus WPs 5 and 7, with majority of them coming from WP7 in relation to project management and coordination. Thus, only one deliverable (i.e., D5.5) that is outside of the project management ecosystem is part of these sensitive deliverables. Nonetheless, most of the data KEYSTONE generate or use are openly accessible to the public. The rest of the 26 deliverables of the 33 deliverables of the project are, indeed, accessible to the public – with full utility to accommodate or comply with the requirements of the FAIR principles.

6.3.1 Open access to research data and scientific publications

Article 17 of the KGA provides for open science and visibility. The article obliges all partners of the project to ensure open access to peer-reviewed scientific publications relating to their results. In particular, KEYSTONE partners must ensure that:

i. At the latest at the time of publication, a machine-readable electronic copy of the published version or the final peer-reviewed manuscript accepted for publication, is deposited in a trusted repository for scientific publications.

ii. Immediate open access is provided to the deposited publication via the repository, under the latest available version of the Creative Commons Attribution International Public Licence (CC BY) or a licence with equivalent rights; for monographs and other long-text formats, the licence may exclude commercial uses and derivative works (e.g., CC BY-NC, CC BY-ND); and

iii. Information is given via the repository about any research output, or any other tools and instruments needed to validate the conclusions of the scientific publication.

Beneficiaries (or authors) must retain sufficient intellectual property rights to comply with the open access requirements.

Metadata of deposited publications must be open under a Creative Common Public Domain Dedication (CC 0) or equivalent, in line with the FAIR principles (in particular machine-actionable) and provide information at least about the following: publication (author(s), title, date of publication, publication venue); Horizon Europe or Euratom funding; grant project name, acronym and number; licensing terms; persistent identifiers for the publication, the authors involved in the action and, if possible, for their organisations and the grant. Where applicable, the metadata must include persistent identifiers for any research output, or any other tools and instruments needed to validate the conclusions of the publication. Only publication fees in full open access venues for peer-reviewed scientific publications are eligible for reimbursement.

Essentially, therefore, every partner of KEYSTONE must ensure open access (i.e., free of charge online access for any user) to all peer-reviewed scientific publications relating to its results. Open access research is a major benefit for the KEYSTONE project as more people will be able to access the outputs, which potentially lead to greater publicity, readership, and more impact.

6.4 Making data interoperable

Making data interoperable means to make different data systems to seamlessly understand and exchange data.[12] It is an important aspect of open science and data exchange, which enables researchers to combine and analyse data from multiple sources to obtain deeper insights. In order to achieve data interoperability in KEYSTONE, the consortium is required to formulate a comprehensive approach that encompasses various strategies and considerations.

The KEYSTONE Consortium uses a number of file formats and data sources. To ensure that documents are accessible and usable by all partners, and that documents which can be shared are accessible by the public, partners will use common file formats as much as possible (e.g., DOCX, XSLX, MS Word, or PDF) as well as CSV, JSON, or XML.

[12] United Nations, Chapter 1: Data Management, Governance and Interoperability, https://unstats.un.org/wiki/pages/viewpage.action?pageId=36144005.

In terms of making data interoperable, all the data within the project will be available using dedicated scripts. The relevant APIs will be open and thoroughly documented to enable and encourage its usage from every third-party application without forcing any dependencies on the provided scripts. It will also use established standards as much as possible. Data models supported by the software will be open and available to interested developers. The project tools will be based on open-source software to facilitate their adoption and possible modifications. The data in the Warehouse will be exposed in a text format following well-known and established standards (e.g., CSV, JSON, or XML).

All the public deliverables in the project will be interoperable both within and outside KEYSTONE. However, the sensitive deliverables can only be largely interoperable within the Consortium.

6.5 Making data re-usable

Data reusability does allow researchers to leverage existing data to conduct new analyses, build upon previous work, and accelerate scientific or knowledge discovery. KEYSTONE will make data reusable by following best practices and adopting strategies that enhance data storage, interoperability, accessibility, and understandability.

The KEYSTONE Consortium will make sure that public deliverables are made public on the project website https://www.keystone-project.com/ once such deliverables are approved by the EC. Files which are open to the public will be created in a common file format. With respect to datasets, they will be made openly available where it is possible, taking into consideration the sensitive nature of some of the deliverables of KEYSTONE as earlier highlighted.

In terms of making data interoperable, all the data within the project will be available using dedicated scripts. The relevant APIs will be open and thoroughly documented to enable and encourage its usage from every third-party application without forcing any dependencies on the provided scripts. It will also use established standards as much as possible. Data models supported by the software will be open and available to interested developers. The project tools will be based on open-source software to facilitate their adoption and possible modifications. The data in the Warehouse will be exposed in a text format following well-known and established standards (e.g., CSV, JSON, or XML).

All the public deliverables in the project will be reusable both within and outside KEYSTONE. However, the sensitive deliverables can only be reusable within the Consortium.

6.6 FAIR principles in the context of KEYSTONE Deliveables

As indicated earlier, a few deliverables in the KEYSTONE project are sensitive, as such, some of the data in KEYSTONE could not be strictly FAIR due to their restrictive and confidential nature. Indeed, seven (7) of the KEYSTONE deliverables that are sensitive cannot adhere strictly to the FAIR principles (See Table 6 below).

By virtue of the sensitive nature of these deliverables, insights from the partners' responses to the DMP questionnaire confirm that these deliverables could not strictly adhere to the FAIR principles. However, it is feasible to make some data from these deliverables findable, interoperable, reusable, and accessible, at least, within the Consortium.

Table 6. KEYSTONE Deliverables that would not strictly adhere to FAIR principles

Lead beneficiary	Deliverable	Dissemination level	F	A	I	R
COVENTRY	D5.5 Conduct an ethical, data protection and societal impact assessment on the use of KEYSTONE technologies.	Sensitive	Findable only by KEYSTONE partners and commission services. However, the partners can transform some data from this deliverable into publicly findable format such as scientific publications and presentations, which the Consortium will explore any potential wavelengths to securely do so.	Accessible only to KEYSTONE partners and commission services. However, the partners can transform some data from this deliverable into publicly consumable format such as scientific publications and presentations, which the consortium will explore any potential wavelengths to securely do so.	It is feasible for data from this deliverable to be integrated into other datasets in the KEYSTONE.	Data from this deliverable can be appropriately documented to be reused by other researchers only within the consortium without compromising the sensitive integrity of the data as originally intended by the KEYSTONE Consortium.
UNIMORE	D7.1 Project Management Handbook	Sensitive	Findable only by KEYSTONE partners and	Accessible only to KEYSTONE partners and	It is feasible for data from this deliverable to be	Data from this deliverable can be appropriately

			commission services.	commission services.	integrated into other datasets in the KEYSTONE.	documented to be reused by other researchers only within the consortium without compromising the sensitive integrity of the data as originally intended by the KEYSTONE Consortium.
UNIMORE	D7.2 Summary of the project	Sensitive	Findable only by KEYSTONE partners and commission services.	Accessible only to KEYSTONE partners and commission services	It is feasible for data from this deliverable to be integrated into other datasets in the KEYSTONE.	Data from this deliverable can be appropriately documented to be reused by other researchers only within the consortium without compromising the sensitive integrity of the data as originally intended by the KEYSTONE Consortium.
COVENTRY	D7.4 Data Management plan report (1)	Sensitive	Findable only by KEYSTONE partners and commission services. However, the partners can transform some data	Accessible only to KEYSTONE partners and commission services. However, the partners can transform some data	It is feasible for data from this deliverable to be integrated into other datasets in the	Data from this deliverable can be appropriately documented to be reused by other researchers only within

			from this deliverable into publicly findable format such as scientific publications and presentations, which the consortium will explore any potential wavelengths to securely do so.	from this deliverable into publicly consumable format such as scientific publications and presentations, which the consortium will explore any potential wavelengths to securely do so.	KEYSTONE.	the consortium without compromising the sensitive integrity of the data as originally intended by the KEYSTONE Consortium.
COVENTRY	D7.5 Data Management plan report (2)	Sensitive	Findable only by KEYSTONE partners and commission services. However, the partners can transform some data from this deliverable into publicly findable format such as scientific publications and presentations, which the consortium will explore any potential wavelengths to securely do so.	Accessible only to KEYSTONE partners and commission services. However, the partners can transform some data from these deliverables into publicly consumable format such as scientific publications and presentations, which the consortium will explore any potential wavelengths to securely do so.	It is feasible for data from this deliverable to be integrated into other datasets in the KEYSTONE.	Data from this deliverable can be appropriately documented to be reused by other researchers only within the consortium without compromising the sensitive integrity of the data as originally intended by the KEYSTONE Consortium.
TB	D7.6 Risk Management Plan	Sensitive	Findable only by KEYSTONE partners and commission services. However, the partners can transform	Accessible only to KEYSTONE partners and commission services. However, the partners can transform	It is feasible for data from this deliverable to be integrated into other datasets in the	Data from this deliverable can be appropriately documented to be reused by other researchers

			some data from this deliverable into publicly findable format such as scientific publications and presentations, which the consortium will explore any potential wavelengths to securely do so.	some data from this deliverable into publicly consumable format such as scientific publications and presentations, which the consortium will explore any potential wavelengths to securely do so.	KEYSTONE.	only within the Consortium without compromising the sensitive integrity of the data as originally intended by the KEYSTONE Consortium.
TB	D7.7 Risk Management Report	Sensitive	Findable only by KEYSTONE partners and commission services.	Accessible only to KEYSTONE partners and commission services.	It is feasible for data from this deliverable to be integrated into other datasets in the KEYSTONE.	Data from this deliverable can be appropriately documented to be reused by other researchers only within the consortium without compromising the sensitive integrity of the data as originally intended by the KEYSTONE Consortium.

Table 7 briefly puts into context a matrix of the relationship between each of the 33 deliverables of KEYSTONE and the FAIR principles. Most of the responses by the Consortium partners to the DMP questionnaire confirm the conclusions of this evaluation matrix.

Table 7. Matrix of FAIR principles in the context of KEYSTONE deliverables

Number	Short name	Deliverables involved in	*Is the deliverable in question findable, accessible, interoperable, reusable, or not? (Yes, or No?)*			
			F	**A**	**I**	**R**
1	UNIMORE	D5.2: CEA and AHP for the KEYSTONE solutions.	Yes	Yes	Yes	Yes
		D7.1: Project Management Handbook.	No	No	No	No
		D7.2: Summary of the project.	No	No	No	No
2	TTS	D5.4: KEYSTONE evidence-based policy recommendations.	Yes	Yes	Yes	Yes
		D6.1: Exploitation plans, replicability report & market uptake strategy (involves in Task 6.3: Replicability)	Yes	Yes	Yes	Yes
3	TB	D1.3: Needs and requirements for the future digital logistics ecosystem.	Yes	Yes	Yes	Yes
		D2.2: Plug & Play implementation and interconnectivity study.	Yes	Yes	Yes	Yes
		D3.1: App design, architecture, and development plan.	Yes	Yes	Yes	Yes
		D7.6: Risk Management Plan.	No	No	No	No

Number	Short name	Deliverables involved in	*Is the deliverable in question findable, accessible, interoperable, reusable, or not? (Yes, or No?)*			
			F	**A**	**I**	**R**
		D7.7: Risk Management Report.	No	No	No	No
4	RINA-C	D2.5: Business models and cases.	Yes	Yes	Yes	Yes
		D6.1: Exploitation plans, replicability report & market uptake strategy.	Yes	Yes	Yes	Yes
5	ETELÄTÄR	D3.4: App launch and reporting.	Yes	Yes	Yes	Yes
		D6.1: Exploitation plans, replicability report & market uptake strategy (involves in Task 6.4: Market uptake).	Yes	Yes	Yes	Yes
6	STA	D6.3: Communication & dissemination plan and visual identity handbook.	Yes	Yes	Yes	Yes
		D6.4: Communication & dissemination plan update.	Yes	Yes	Yes	Yes
		D6.5: Final communication & dissemination report.	Yes	Yes	Yes	Yes
7	UPM	D1.2 Focus groups report including stakeholders' requirements and expectations.	Yes	Yes	Yes	Yes
8	AETHON	D2.1: API Reference Model.	Yes	Yes	Yes	Yes

Number	Short name	Deliverables involved in	*Is the deliverable in question findable, accessible, interoperable, reusable, or not? (Yes, or No?)*			
			F	**A**	**I**	**R**
		D2.3: API standard.	Yes	Yes	Yes	Yes
		D2.4: API standard V2.	Yes	Yes	Yes	Yes
9	GRUBER LOGISTICS	D1.4: Digital ecosystem framework	Yes	Yes	Yes	Yes
		D4.3: Pilots Activities.	Yes	Yes	Yes	Yes
		D5.3: Evaluation with the DTLF working group.	Yes	Yes	Yes	Yes
10	CIM	D4.3: Pilots Activities (involves in Task 4.4: intermodal digital ecosystem).	Yes	Yes	Yes	Yes
11	CEFRIEL	D1.1: Stakeholders' identification and needs	Yes	Yes	Yes	Yes
		D3.2: Co-created UI/UX design.	Yes	Yes	Yes	Yes
		D4.2: Definition and specification of the operational scenarios.	Yes	Yes	Yes	Yes
		D6.2: Stakeholders' engagement report.	Yes	Yes	Yes	Yes
12	CORTE	No specified deliverables nor tasks. Involved in WP1, WP2, WP4, WP5 & WP6.	Uncertain / mixed	Uncertain / mixed	Uncertain / mixed	Uncertain / mixed
13	AEC	D4.1: Process and procedures report based on the concrete use cases.	Yes	Yes	Yes	Yes

Number	Short name	Deliverables involved in	*Is the deliverable in question findable, accessible, interoperable, reusable, or not? (Yes, or No?)*			
			F	**A**	**I**	**R**
14	ICOOR	D5.1: Evaluation Methodology and Plan.	Yes	Yes	Yes	Yes
15	COVENTRY	D1.2: Focus groups report including stakeholders' requirements and expectations.	Yes	Yes	Yes	Yes
		D3.3: Cyber security infrastructure for the KEYSTONE solution	Yes	Yes	Yes	Yes
		D5.5: Conduct an ethical, data protection and societal impact assessment on the use of KEYSTONE technologies.	No	No	No	No
		D7.3: The project's data management plan	Yes	Yes	Yes	Yes
		D7.4: Data Management plan report (1)	No	No	No	No
		D7.5: Data Management plan report (2)	No	No	No	No

7. Protection of personal data in KEYSTONE

Personal data protection is very important to safeguard individuals' fundamental rights, privacy, and autonomy, especially in the age of growing digitalisation. Personal data such as name and contact details of people are currently collected and processed by the Consortium, thus making it imperative to ensure that all partners are able to actively support in the protection of such data from unauthorised access, disclosure, or misuse. KEYSTONE partners collect and process the minimum amount of personal data required for the completion of the project tasks. This section describes how personal data will be protected and processed in compliance with the GDPR. It elaborates on the description of personal data processing activities, getting

into the specifics of GDPR compliance, namely the data protection principles, data transfers, DPIAs, and how rights of data-subjects are facilitated. It also notes aspects relating to data security, persons responsible for data management, and ethical use of data.

7.1 Types of personal data

Where personal data is processed under the GDPR, a legal basis is required. In KEYSTONE, all partners have provided an appropriate legal basis for processing such data. It is generally for legitimate interest and performance of KEYSTONE contract.

Pursuant to the GDPR, personal data refers to:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*[13]
>
> With respect to how identifiable a data subject is, '*account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.*[14]

Where it is not 'reasonably likely' that a data subject can be identified, then such data can be treated as anonymous data. But anonymisation can be a high threshold to meet, and all objective factors should be taken into account when making such an assessment, particularly in terms of data-subjects being singled-out, the re-identification risk, and the potential to infer personal data from a supposedly anonymous data-subject.[15] It is also imperative to note that anonymous data does not mean 'risk free' data processing; supplementary measures might need to be implemented to ensure successful anonymisation, or to mitigate risks of re-identification. Before sharing anonymous personal data, partners should also conduct a risk assessment to consider risks of re-identification and what they will do if re-identification occurs. This must also consider the issue that data that is anonymous today might not be anonymous in future if new data processing techniques are developed, and so anonymous data should be treated as personal data and destroyed when no longer needed.[16]

Where steps have been taken to de-identify a data subject, but it is still possible to identify them using additional information (e.g., the original names of data subjects have been replaced with alpha-numeric tokens), then the data subject is pseudonymous. As stated in the GDPR:

> *pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;*[17]

[13] Art.4(1), GDPR.
[14] Recital 26, GDPR.
[15] See Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP 216, Adopted on 10 April 2014, pp.11-12, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf .
[16] See, for example, Elliot, Mark, Elaine Mackey and Kieron O'Hara, *The Anonymisation Decision-Making Framework: European Practitioners' Guide*, 2nd edn., UKAN Publications, Manchester, UK, 2020.
[17] Art.4(5), GDPR.

As it would be possible to identify a data subject using additional information, pseudonymous data is still personal data. All partners in KEYSTONE should, therefore, treat pseudonymous data as personal data and provide a legal basis for the processing of such data. KEYSTONE partners must take all practical possible steps to minimise personal data and allow the research purposes to be reached.

7.1.1 Sensitive personal data

Personal data that reveals very personal or private details can be seen as sensitive. Under the GDPR, there are two types of sensitive data: special categories of data and criminal conviction/offence data. For both types of sensitive personal data, the GDPR places a general prohibition on processing these data. In order to process them, an exception must apply, as defined under Article 9.2 of the GDPR.

The GDPR defines special category data as:

> *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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*[18]

Currently, KEYSTONE partners are not processing special categories of data in the context of KEYSTONE research. In the future, if partners consider there is a need to process this kind of data, the DMP will accordingly be updated. In such a situation, the exemptions most likely to apply would be:

(1) scientific research, requiring that processing for scientific purposes must include safeguards for the data subject, as required under Article 89(1) and national law, such as pseudonymisation or anonymisation, where possible.[19]

(2) processing relates to personal data which are manifestly made public[20] by the data subject. This exemption is specifically thought to apply in case partners were collecting special categories of data from the Internet performing a standard search. Personal data will never be extracted from private forums or websites where users access with a private account or password and/or through invitation.

With respect to criminal offence/conviction data:

> '*Processing of personal data relating to criminal convictions and offences, or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects*[21].'

This data will at this stage not be shared by Consortium partners.

7.2 Lawfulness, fairness and transparency

Lawfulness, fairness, and transparency do govern the processing of personal data pursuant to the GDPR and other relevant data protection laws. These principles are necessary to safeguard the privacy of individuals while also ensuring that their personal information is responsibly and ethically handled. The KEYSTONE project will only process personal data where it is lawful, fair, and transparent. Personal data is processed only insofar as it is necessary for the purposes of research, dissemination, and exploitation of the project results. The processing of personal data in KEYSTONE can be grouped into the following activities: (1) communication and dissemination, and (2) research.

[18] Art. 9(1), GDPR.
[19] Art. 9(2)(j), GDPR.
[20] Art. 9(2)(e) GDPR.
[21] Article 10, GDPR.

Lawfulness:

Legal bases for communication and dissemination activities in KEYSTONE:

1. Consent (which can be withdrawn at any time)[22] where people subscribe themselves to receiving informative communications about the KEYSTONE project and the project newsletter.
2. The legitimate interest of the partners, balanced against the interests of the data subjects, where the newsletter and informative communications about the project will be sent to those potentially interested to read news from the project.[23] A legitimate interest assessment has been carried out. Those people contacted on the basis of the legitimate interests of the KEYSTONE partners are free to opt out of communications at any time through using an 'unsubscribe' option which will be in plain view at the bottom of all email communications these people receive.

Legal bases for research activities:

- KEYSTONE project partners will gather data directly from data subjects on the basis of consent especially in WP1 regarding needs assessment (which can be withdrawn at any time);[24] in the case of survey responses and interviews to enforcement authorities and logistic operators conducted by the partners.[25] In accordance with data protection law and good research practice, participants provide consent to participate in the research project and a separate consent for the personal data processing and are able to withdraw their consent from the research activities, and the processing of their personal data, at any time without any negative consequences. Professor Alexeis Garcia Pereza (Coventry) is the contact point for data subject rights to exercise data protection rights.

Currently, no partner in the Consortium has envisaged to re-purpose datasets. If at a later stage in the project it is needed, this will mostly be on the basis that the re-purposing for scientific research is compatible with the original purpose and so 'no legal basis separate from that which allowed the collection of the personal data is required'.[26] Where any special category of personal data is processed, this will be processed under the scientific research exemption,[27] in accordance with Article 89 GDPR, and national law that provides for use of the scientific research exemption.

Partners will perform a legitimate interest assessment when relying upon legitimate interest as the most appropriate legal basis. In this regard, legitimate interest assessment template has been included in Annex II of this deliverable.

Fairness

The fairness principle requires that personal data are processed in a way that is fair and requires consideration of whether the personal data is processed in a way that is unfair, such as data collected by deception, data processed in an unreasonable way, or having an unjustified impact of data-subjects.[28] No data collected, or re-purposed (if any) by the KEYSTONE project will be unfair, collected by deception or processed in an unreasonable way. DPOs are required to get actively involved with the research teams within their organisation.
The KEYSTONE project is exclusively a research project, thus, the KEYSTONE technologies will not be used in any ongoing investigations, and so will not be used to create effects for data subjects and, in any case, the project takes steps to reduce the risks of incidental findings – consequently, there will be no unjustified impacts on data subjects.

[22] Art.6(1)(a), GDPR.
[23] Art.6(1)(f), GDPR.
[24] Art. 6(1)(a) and Recital (39), GDPR.
[25] Art. 9(2)(a), GDPR.
[26] Recital 50, GDPR.
[27] Art. 9(2)(j), GDPR.
[28] Kuner, Christopher, Bygrave, Lee, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, OUP, Oxford, 2020, p.314; ICO, *Guide to the GDPR*, ICO, p.22.

Transparency

Transparency requirements under the GDPR are provided under Article 13, where data is collected from the data subject, and Article 14 where data is not collected from the data subject.
Partners provide the information required under Article 13, through the information sheet and informed consent form signed by data subjects and the data protection policy that can be found on the KEYSTONE website. Templates for information sheets and informed consent form have been included in Annex I of this document.

Where it is impossible, or would require disproportionate efforts, to notify a data subject under Article 14, as it might be the case when performing data crawling from the Internet by the technical partners, the partners will abide by the exemption contemplated under Article 14(5)(b). Additionally, data subjects can get information on the project through the data protection policy on the KEYSTONE website https://www.keystone-project.com/.

7.3 Purpose limitation

The purpose limitation principle requires data to be collected for a specific, explicit, and legitimate purpose. Or, if data are re-used, that the purpose of secondary processing is compatible with the original purpose.

Noting that scientific research in and of itself is a legitimate purpose,[29] the research activities conducted in the KEYSTONE project are for specific and explicit purposes detailed in the project KGA. Additionally, the processing of personal data for communication activities are for the specific and explicit purposes of disseminating information on the KEYSTONE project to interested stakeholders as required under the KGA, which does not create disproportionate effects on data subjects, and are therefore legitimate.

If datasets were to be re-purposed in the KEYSTONE project, this would only occur where the re-purposing is compatible with the original purpose. For communication activities, the re-purposing of contact details to share information about a research project with people who we feel will be interested in is, therefore, compatible with the original purpose, and the re-purposing of personal data for scientific research is stated by the GDPR itself to be *prima facie* compatible with the original purpose[30].

7.4 Data minimisation

The data minimisation principle requires that personal data are adequate, relevant, and limited to what is necessary for the purposes sought.[31]

Partners follow good data governance practices and collect no more personal data than is necessary. KEYSTONE partners ensure that only data, which is adequate, relevant, and limited to what is needed for their tasks is collected/processed. As such, partners do not collect extraneous information from participants where such personal data is not required to complete the task at hand. If additional personal data beyond what is necessary is provided to partners, they will continue to erase it as soon as is practicable.

The KEYSTONE partners aim to minimise the amount of personal data they process and still enable the research purposes to be reached. This involves pseudonymising some data by, for example, changing data subject names and telephone numbers for fictional names and numbers, and removing real names and identifying information from survey responses.

[29] Recitals 156-162, GDPR.
[30] Art.5(1)(b), GDPR.
[31] Art.5(1)(c), GDPR.

7.5 Accuracy

The accuracy principle requires that personal data are kept up-to-date and that any inaccuracies are rectified, or, bearing in mind the purposes, the data are destroyed.[32]

Where KEYSTONE partners are made aware that any personal data, which they are processing is inaccurate, then they rectify such data. If it is not possible, then they will seek to erase the data. However, noting that such data could be essential to fulfilling research purposes, then an assessment might need to be made on how the accuracy principle can be fulfilled whilst meeting the research purposes.

7.6 Storage limitation

The storage limitation principle requires that personal data is not kept, or kept in an identifiable form, for longer than is necessary to achieve the purposes.[33] Partners store personal data only for so long as it is necessary to keep it.[34] Where identifying information is no longer needed, it will be destroyed.

The storage limitation principle should be applied in line with the obligation of the partners to keep records and other supporting documentation in order to prove implementation of the action for a period of 5 years as set out in Article 18 of the KGA. As such, personal data may be retained for this period of time where it is necessary to do so in order to provide records and documentation to the EC should they choose to carry out an audit of any partner. Moreover, the GDPR explicitly notes that scientific research purposes might involve holding personal data for longer than is necessary, and that technical and organisational measures should be taken to protect personal data in such circumstances.

7.7 Accountability

The accountability principle entails that partners are individually responsible for complying with the above-mentioned principles and are able to demonstrate compliance with them.[35] Partners are able to demonstrate compliance through providing necessary information in this data management plan, their organisational policies and the internal and technical processes carried out on each data processing activity. Additionally, a specified individual who is responsible for data management for each partner and a list of DPOs or equivalent professional, is provided in Table 8.

7.8 Rights of individuals

The GDPR outlines a number of rights which data subjects have with regard to their personal data. This section outlines each right and how the KEYSTONE partners can fulfil these rights as far as reasonable.

The right of access: Article 15 GDPR allows data subjects to find out if their personal data is being processed, to have access to such data, and to have access to relevant supplementary information.[36] Partners will provide this information, subject to Articles 12, 13 and 14 of the GDPR.

The right to rectification: Under Article 16 of the GDPR, data subjects have the right to rectify inaccurate data which is held about them, or complete data that is incomplete. This links with the requirements for obtaining accurate information noted above,[37] but requires data controllers to reconsider data accuracy upon request.

[32] Art.5(1)(d), GDPR.
[33] Art.5(1)(e), GDPR.
[34] Art.5(1)(e) and Recital (39), GDPR.
[35] Art.5(2), GDPR.
[36] Art.1(a)-(h), GDPR.
[37] See Section 5.5; Art.5(1)(d), GDPR.

KEYSTONE partners will rectify any inaccurate information which they process, and will also endeavour to provide data subjects with opportunity to complete any data which is incomplete.

The right of erasure: Article 17 of the GDPR provides data subjects the right for their personal data to be erased from processing. This links with personal data being removed from data sets where individuals withdraw their consent, as mentioned above. Partners will endeavour to comply with requests of erasure, but note that data processors are exempt from doing so where erasure would endanger the fulfilment of research activities (that include safeguards to protect personal data).[38]

The right to restrict processing: In certain circumstances, Article 18 of the GDPR provides data subjects with grounds for restricting processing of their personal data. Should any KEYSTONE partner receive a request from an individual who wishes to restrict the processing of their personal data, they will abide by that request where Article 18(1)(a)-(d) apply and will store relevant data until the matter is resolved. Following resolution, partners will either destroy that data or process it in a way that the data subject has consented to.

The right to data portability: Article 20 of the GDPR provides data subjects with a right to request personal data which is held about them in a 'structured, commonly used and machine-readable format' which can be used to transfer data from one data controller to another. Data subjects can only request such data where the data is processed on the basis of consent, or a contract, and where the processing is done by automated means.[39]

The right to object: Under Article 21 of the GDPR, data subjects have the right to object to processing of their personal data in some circumstances. Where personal data is collected as part of a research activity, data subjects can refuse to provide consent to processing and so this averts any need to exercise a right to object to processing. Where personal data is processed as part of a dissemination activity, data subjects may object to processing by clicking 'unsubscribe' which will be at the bottom of all electronic communications from the KEYSTONE Consortium; this provides data subjects with an opportunity to object to processing of their personal data on the basis of the legitimate interests of the KEYSTONE partners.

Rights in relation to automated decision-making and profiling: Article 22 GDPR provides people with the right not to be subject to automated decision-making or profiling which creates legal or similar effects for such persons. However, where the data subject consents to this process, such processing can be lawful.[40]

It is also important to note that, depending upon the applicable Member State law, some of these rights might not apply to the processing of personal data under the scientific research regime where facilitating exercise of these rights would prevent achievement of the scientific purposes.[41] A table with different national data protection laws has been provided in D8.3. Further, it is also important to note that where processing of personal data does not require identification (i.e. the data are pseudonymised), then the data controller is not required to identify a data subject for the purposes of GDPR compliance and these rights can be limited unless the data subject sufficiently identifies themselves.[42]

Currently, Coventry acts a point of contact for data subjects who wish to exercise their data protection rights in the context of interviews and surveys. Furthermore, the following email address keystone@smart-

[38] Art. 17(3)(d), GDPR.
[39] Art. 20(1)(a)-(b), GDPR.
[40] Art. 22(2)(c), GDPR.
[41] Art. 89(3), GDPR.
[42] Art. 11, GDPR.

transportation.org has been set up as the contact point for data subjects on the KEYSTONE website https://www.keystone-project.com/.

7.9 International data transfers

KEYSTONE partners are based in the EU except for one partner (Coventry) based in the UK. The KEYSTONE Consortium intends to process personal data within the boundaries of the EU and UK, for the latter, an adequacy decision was adopted June 2021.[43] Additionally, the UK has made an 'Adequacy Regulation' with respect to the transfer and protection of personal data transferred from the UK to the EU and so are lawful under Article 45 of the UK GDPR.

The majority of partners, as can be seen in 'Table 3. Data overview', are and will be using Microsoft Office applications which is widely used across industries. Partners will be storing their data locally through private owned data centres in the territories where partners are based.

Microsoft stores data within the EU for its various software applications, including Microsoft 365 and SharePoint. Currenlty, Microsoft European data centres are located in Austria (Vienna), Finland (Helsinki), France (Paris, Marseille), Ireland (Dublin), Italy (Milan), Netherlands (Amsterdam), Poland (Warsaw), and Sweden (Gävle, Sandviken, Staffanstorp).[44]

7.10 Data Protection Impact Assessments

Article 35 of the GDPR provides for Data Protection Impact Assessments (DPIA). It essentially provides that if certain types of data processing activities pose a high risk to the rights and freedoms of individuals or data subjects, a DPIA will be required. The DPIA seeks to identify and mitigate these risks by providing a description of the processing operations and their purposes, assessing the necessity and proportionality of the processing, assessing the risks to individuals' rights and freedoms, and proposing measures to address these risks.

The initial DPIA assessment on partners to determine whether DPIA requires to be conducted on them has shown that no partner has yet need a DPIA to be carried out. Coventry requested a "Yes" or "No" answer from partners in the DMP questionnaire on the following parameters:

Evaluation or scoring (including profiling and predicting aspects concerning the data subject i.e., economic situation, reliability, and location), Automated Decision Making, Systematic monitoring, Sensitive Data, Large scale, Matching or combining datasets, Vulnerable groups, Use of innovative technologies, and Prevention (i.e., whether data processing will prevent data subjects from exercising a right or using a service or a contract). If two (2) out of the nine (9) criteria are met, the conclusion will be that a DPIA is required.

However, all the project partners scored a "No" from this assessment, indicating that DPIA is currently not required in any of the partners. To the extent that personal data is processed as part of activities, steps will be taken by the Consortium to see if and how to perform a DPIA before the commencement of such activities.[45]

[43] Commission adopts adequacy decisions for the UK, https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183.
[44] Microsoft data locations for the European Union, https://docs.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide.
[45] A29WP Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p. 10,

7.11 Persons responsible for data management in KEYSTONE

Protection of personal data is the responsibility of everyone in a company. It is, however, the responsibility of organisational management and DPOs to ensure that appropriate procedures, policies, and related measures are formulated and overseen to ensure that appropriate safeguards are in place to secure personal and related data in the organisation. Article 37 GDPR provides as follows:

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. 2The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Pursuant to the above provision, particularly Article 37(1), the KEYSTONE Consortium has provided designated DPOs in respective partners as can be seen in Table 8 below.

https://ec.europa.eu/newsroom/article29/items/611236; TRACE, D1.1 Data Management Plan (European Union H2020, January 2022).

Table 8. Persons responsible for data management

Number	Short name	Responsible persons for managing data
1	UNIMORE	avv. Vittorio Colomba (https://www.unimore.it/dpo.html)
2	TTS	Leonardo Domanico, Leonardo.domanico@ttsitalia.it
3	TB	dpogruppo@bv-tech.it
4	RINA-C	rina.dpo@rina.org
5	ETELÄTÄR	José Papí, j.papi@etelatar.com.
6	STA	Friederike L. Kühl, f.kuhl@smart-transportation.org
7	UPM	proteccion.datos@upm.es
8	AETHON	Magdalena Pawlikowska
9	GRUBER LOGISTICS	Dr. Fabrizio Borgogna, fabrizio.borgogna@gruber-logistics.com.
10	CIM	Inapplicable / No DPO[46]
11	CEFRIEL	privacy@cefriel.com
12	CORTE	Remy Russotto, r.russotto@corte.be.
13	AEC	Inapplicable / No DPO[47]
14	ICOOR	ICOOR is a Consortium of several Italian Universities. Each university has its own DPO.
15	COVENTRY	Gurdeep Chayra, dpo@coventry.ac.uk

8. Data Security

KEYSTONE partners are responsible for securely storing[48] any personal data they retain. This includes storing data on password-protected SharePoint sites, or password-protected machines at their own premises. Microsoft engineers only administer SharePoint through a PowerShell console that requires two-factor authentication and do not have access to the data. SharePoint is protected through encryption and does not

[46] However, CIM have a GDPR document, which they are updating in line with a recent governance change, which provides relevant procedures to work properly according to privacy and data protection rules.
[47] However, AEC is part of the Spanish Road Association, which has someone who deals with data protection and management issues (responsible for computer security, passwords management, etc.). But this person has a very national profile, all international issues are usually centralized by Elena de la Peñaor edelapena@aecarretera.com or Lourdes Díaz Toribio ldiaz@aecarretera.com who can be contacted on data management matters in AEC.
[48] Art.5(1)(f), GDPR.

authenticate connections over HTTP,[49] rather redirecting to HTTPS. SharePoint encrypts data using SSL/TLS connections, and all SSL connections are established using 2048-bit keys.[50]

Additionally, Consortium partners can store local copies of research data on their own machines, servers, or cloud-storage systems. At the very least, partners must:

- Regularly back up KEYSTONE research data with recovery capabilities.
- Adequately protect local machines and servers against cyber threats by installing and updating anti-virus software, anti-malware software, and using firewalls.
- Store the project research data securely with clearly defined access controls (e.g., encryption, password-protection, restricting access to authorized personnel).
- Evaluate any privacy or data protection risks associated with data processing and implement appropriate mitigation measures to protect personal data.
- Process any personal data in a manner that safeguards the data subject's privacy and confidentiality, including preventing unauthorized access to or use of personal data and the equipment used for personal data processing.

9. Ethical Aspects

Article 14 of the KGA obligates all the partners to conduct their work in accordance with ethical principles and the highest standards of research integrity. This includes adhering to the European Code of Conduct on Research Integrity,[51] which mandates that researchers uphold the principles of reliability, honesty, respect, and accountability. In addition, researchers must adhere to rules on good practice and research integrity.

All KEYSTONE partner research that involves collection of data from human participants must provide information sheets and informed consent forms that comply with research ethics standards and data protection regulations. These forms must include the following information: Background and purpose of the research, Contact information for the researchers, Voluntary nature of participation and the right to withdraw at any time, as well as Potential risks and benefits of participation.

Compliance with these ethical principles and standards is essential for ensuring the validity, reliability, and trustworthiness of KEYSTONE research. It also demonstrates the commitment of KEYSTONE to protecting the rights and well-being of research participants. Additionally, these documents will explain in plain and simple language data processing that may take place, and how the privacy of the participants can be safeguarded. An example of information sheet and informed consent form is included in Annex I in this deliverable.

In terms of Ethics Management in Research, the KGA provides as follows:

[49] How SharePoint and OneDrive safeguard your data in the cloud, https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data

[50] Data Encryption in OneDrive for Business and SharePoint Online, https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide

[51] ALLEA, The European Code of conduct on Research Integrity, 2017, https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

KEYSTONE will ensure a full understanding by all the participants of the information given when inviting them to participate in a study protocol and their ability to give or withdraw consent; ensuring in parallel that the study subjects are not selected or rejected for the wrong reasons and that there are no secondary or hidden interests when performing the research. To this end, a Research Ethics & Privacy Board (EPB) will also be established to respect fundamental ethical principles such as integrity, justice, beneficence, and respect, determine that risks and benefits are appropriately balanced from the research point of view and that the proposed strategy for subject recruitment is fair, and that voluntary, informed consent will be sought from each potential subject. Personal data will not be shared between partners or linked to any results or stakeholders' opinions/input.

10. Allocation of resources

Funding for publication costs is allocated within the budget of KEYSTONE. Costs associated with enhancing FAIR data will be borne by the individual partners responsible for sharing the data. Open data dissemination will be achieved through the deposition of data in open repositories or partner institutional open repositories, where no data sharing costs are expected.

The role of data manager is part of the Consortium. Ethics and Data Management Manager (WP7) is Professor Alexeis Garcia Pereza (Coventry University). This is to ensure compliance with legal and ethical data processing standards. Coventry will periodically revise and review the DMP to reflect new information that arises during the project and will continue to consult with partners to clarify any outstanding issues. Revisions to this DMP may be necessary in circumstances such as:

The availability of new or unanticipated datasets, re-classification of existing datasets due to changes in data protection regulations or emerging concerns, technological advancements affecting data security or data protection, and partner exits or new partners joining the Consortium, as well as updates to data management, personal data, or privacy policies of partners that could impact the KEYSTONE Consortium.

Partners are responsible for informing Coventry of any of the above issues, or any other developments that could affect their data usage during the project.

11. Conclusions

Data has a very important role in KEYSTONE, as it is the real focus and the final goal. The KEYSTONE Consortium will carefully manage research data generated and processed during the life of the project. This DMP contains the initial output (i.e., D7.3 Data Management Plan) in M6 that details the relevant standards, policies, and procedures for managing the research data in the context of the KEYSTONE project. It presents KEYSTONE's plan for managing the production, collection, processing, and storage of data generated within the project. The data and research outputs follow the FAIR principles. The deliverable has thus presented KEYSTONE management plan for research that will be collected, generated, and/or processed within the project pursuant to principles of "FAIR data" and "as open as possible, as closed as necessary".

Each project partner is accountable for ensuring that their handling of data within the KEYSTONE project complies with the procedures and strategies outlined in this document. KEYSTONE partners have resolved with firm dedication to sound data management practices, having recognised that doing so can enhance

research quality by producing data that is well-organized, documented, preserved, and accessible. This, in turn, facilitates more efficient and outstanding research not only for the Consortium but also for other projects that can benefit from the data that is generated or used by the Consortium.

This deliverable will be continually updated as new information becomes available, with revised versions being respectively submitted in M18 and M36.

References

A29WP Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p. 10, https://ec.europa.eu/newsroom/article29/items/611236.

ALLEA, The European Code of conduct on Research Integrity, 2017, https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf.

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP 216, Adopted on 10 April 2014, pp.11-12, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Commission adopts adequacy decisions for the UK: https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183.

Data Encryption in OneDrive for Business and SharePoint Online: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide

Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP 216, Adopted on 10 April 2014, pp.11-12, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf .

Elliot, Mark, Elaine Mackey and Kieron O'Hara, *The Anonymisation Decision-Making Framework: European Practitioners' Guide*, 2nd edn., UKAN Publications, Manchester, UK, 2020.

European Commission (n.d.), Data management, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm#:~:text=Rather%2C%20the%20DMP%20is%20intended,include%20a%20timetable%20for%20updates.

European Commission (n.d.), What constitutes data processing? https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en#:~:text=It%20includes%20the%20collection%2C%20recording,or%20destruction%20of%20personal%20data.

European Commission (2016), H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

European Commission (n.d.), Data management, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm.

European Commission (2016), H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

FAIR, FAIR Principles, https://www.go-fair.org/fair-principles/.

How SharePoint and OneDrive safeguard your data in the cloud: https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data.

ICO, *Guide to the GDPR*, ICO, p.22.

Kuner, Christopher, Bygrave, Lee, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, OUP, Oxford, 2020.

Mark D. Wilkinson et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship, Nature Scientific Data, 3 (160018).

Microsoft data locations for the European Union: https://docs.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

TRACE, D1.1 Data Management Plan (European Union H2020, January 2022).

United Nations, Chapter 1: Data Management, Governance and Interoperability, https://unstats.un.org/wiki/pages/viewpage.action?pageId=36144005.

Appendices

1. ANNEX I: PARTICIPANT INFORMATION SHEET AND INFORMED CONSENT TEMPLATE

PARTICIPANT INFORMATION SHEET AND CONSENT FORM

Introduction

You have been invited to take part in a research study. Before making a decision on whether you want to participate or not, please read this document carefully. Please ask all the questions you may have, including around risks and benefits, so you can be sure to understand all the proceedings of the study.

Description of the project

By signing the attached informed consent form, I understand that I am consenting to participate in the KEYSTONE project funded by the European Union (Grant Agreement number 101103740) and UK Research and Innovation (UKRI) and coordinated by Universita Degli Studi Di Modena E Reggio Emilia (UNIMORE). I am aware that the purpose of the KEYSTONE project is to develop and conceptualise a sustainable, efficient, and safe transport system, which allows enforcement authorities to access data for compliance checks.

1. The partners of the Consortium are: Universita Degli Studi Di Modena E Reggio Emilia (UNIMORE); 2. TTS Italia (TTS); 3. T Bridge SPA (TB); 4. Rina Consulting SPA (RINA-C); 5. Etelatar Innovation Ou (ETELÄTÄR); 6. Smart Transportation Alliance (STA); 7. Universidad Politecnica De Madrid (UPM); 8. Aethon Engineering Single Member PC (AETHON); 9. Gruber Logistics S.P.A. (GRUBER LOGISTICS); 10. Centro Interportuale Merci-C.I.M. SPA-Novara (CIM); 11. Cefriel Societa Consortile A Responsabilita Limitata (CEFRIEL); 12. Confederation of Organisations in Road Transport Enforcement Aisbl (CORTE); 13. Asociacion Espanola De La Carretera (AEC); 14. Consorzio Interuniversitario Per L'ottimizzazione E La Ricerca Operativa (ICOOR); and 15. Coventry University (COVENTRY).

The KEYSTONE project duration is from 01 June 2023 to 31 May 2026.

Information about your involvement

- I understand that my participation might involve interviews, workshops, webinars, surveys and/or written responses to questionnaires, where I will be invited to offer my views about the tools developed by KEYSTONE partners and/or discuss the current needs from Enforcement Authorities. I am participating in these activities voluntarily, and I am free to end my participation at any time. I may refuse to answer any questions I do not wish to discuss. I understand that I have the right to ask questions and receive clear answers before making any decision. I understand that I may be asked to provide professional or personal views and that the record of my involvement in the research will be kept confidential.

- I understand that my responses to any workshop/webinar/discussion, or any interview/survey/questionnaire may be recorded and that physical copies of such recordings will be safely stored under lock and key by the KEYSTONE partner leading the activity.

- I understand that, when the information I provide is used for the writing of any deliverable in the project, the consortium will remove my name and all identifying features of that information so that my identity and experiences remain confidential (unless attribution is required, and I have consented to it). I understand that I can request a copy of the data I have provided.

- I understand that any information that might identify me will be removed. Only the research team undertaking the research project will be able to access such data. Personal information received will be stored in separate files in a secure manner (including password protection where required). I understand that the project will only collect information that is relevant to its activities. Personal information will be stored on internal servers, and accessible to only the partners involved in KEYSTONE. The partners will password-protect any and all records with personal data. All computers will also have password protection to prevent access by unauthorised users. Only members of the research staff will have access to the passwords.

- I understand that this research conforms to European Commission guidelines and compliance with the current legislation.

- I understand that my responses may result in incidental and secondary findings, i.e., some information that was not the focus or primary purpose of the question(s). In such cases, I understand that I may opt out of my consent for KEYSTONE's use of the incidental findings. Otherwise, I understand that KEYSTONE will manage the incidental findings in the same way as the principal findings, i.e., that the information will be deleted within five years after EU project funding comes to an end and that any use of such information will be anonymised. The Consortium will report incidental findings to the project's Ethics Board and, if necessary or if the Ethics Review Panel so chooses, it can evaluate incidental findings.

Name:

Date: ___/___/_____

Signature:

DATA PROTECTION

Data Controller

The Data Controller of my personal data is *[complete with the name of the data controller]* with registered office at *[complete with the registered address of the data controller].* I can contact the Data Protection Officer at *[complete with details of the data controller's DPO]* for any queries related to the personal data processing.

Categories of Data

The Data Controller will collect: [*list the categories of data to be processed: name, surname, email address, opinions, voice etc]*

Purpose and Legal Basis

The purpose of the data processing is to *[explain the purpose of the data processing]* and will be performed on the basis of my consent. I have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

Recipients of the data

My personal data will not be shared with any legal or natural person outside the project, unless required by law.

Data Transfers

My personal data may be transferred to the UK for which the Commission has adopted an adequacy decision on the 28th of June of 2021.

Retention Period

The data will only be retained for as long as necessary and up to 5 years after the end of the project, pursuant to Article 18 of the Grant Agreement which imposes the obligation for partners to keep records and other supporting documentation for a period of 5 years in order to prove the proper implementation of the project and the costs declared as eligible.

Data Protection Rights

I have the right to access, rectify or erase my personal data, restrict the processing or to object to the data processing as well as the right to data portability.

I also have the right to lodge a complaint with the competent Data Protection Supervisory Authority: *[provide details of the relevant data protection authority]:*

Name:

Date: ___/___/_____

Signature:

2. ANNEX II: LEGITIMATE INTEREST ASSESSMENT TEMPLATE (LIA)

Completed by: [NAME], [ROLE], [E-MAIL]

LIA conducted to assess: [PROJECT OR PROCESS NAME AND BRIEF DESCRIPTION]

Date: [DATE]

Preamble

Under Article 6(1)(f) of the GDPR, processing of personal data is lawful if:

"processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of the personal data, in particular where the data subject is a child."

This LIA allows for a 3-stage legitimate interest assessment to ensure that the interests, rights and interests of individuals do not override and outweigh your organisation's legitimate interests and that its processing is lawful.

The outcome of this LIA has been recorded in order to comply with its accountability obligations under Articles 5(2) and 24 of the GDPR.

Purpose Test

Does this processing rely on Legitimate Interest?

Purpose test	Answer
Name of process/activity and relevant department	
Is this process/activity part of your organisations core/public task or part of an ancillary/secondary task? Please describe the process in detail:	
Why does your organisation want to process the data? What are the key objectives in carrying out this process?	
Please describe the Legitimate Interest in carrying out this activity, does the activity; 1. benefit society overall; and/or 2. benefit an individual, organisation or group financially or otherwise (such as the delivery of HR services, the delivery of security services/protection of safety etc.).	
What would be the impact if your organisation could not process data in these ways?	
Is the processing likely to give rise to a complaint? (i.e., a process which involves legal consequences, refusal of applications, ratings or rankings etc.	

Necessity Test

Is the processing necessary for the above purpose?

Necessity test	Answer
How does the processing further your organisations goals and objectives?	

Necessity test	Answer
Are there any categories or types of personal data that are not strictly necessary to carrying out the task but provide additional benefit? For example, the processing of marketing cookies, or conducting an additional survey etc.	
Could the same objective be achieved by processing fewer personal data?	
Are there similar methods of processing personal data that would allow for the same outcome? For example, your organisation is procuring analysis software. The same outcome could be achieved by manual processing; however, the use of this new software provides additional benefits etc.	
Why have you chosen the proposed method of data processing or system?	

Balancing Test

Do the individuals' interests, rights and freedoms override the legitimate interest?

Balancing test	Answer
What is the nature of your organisation's relationship with the individuals?	
Is any of the data particularly sensitive or private? (This could include health data, financial, DOB, relationship status, PPSN, maiden name etc.)	
How will you inform the data subjects of this processing?	
Are some people likely to object or find it intrusive?	
Does this processing involve any potential impacts on the individual's life or status? This could include a refusal of a loan, refusal of an application, not receiving a promotion etc.	
How would you describe the significance of the potential impact? (Could the impact be long lasting, impact future applications etc.)	
What measures relevant to this process are currently in place or are envisioned to protect personal data and minimise risk?	
Will this process involve the processing of young person's/children's data?	
Are any of the individuals vulnerable in any other way? (This could include persons with a disability, in financial distress, ill health).	
Can your organisation offer an opt-out to this process?	

Balancing test	Answer
After considering the potential impacts on the individual and the Legitimate Interest of your organisation, do the benefits of these Legitimate Interests outweigh the potential risk posed to the individual?	

Decision & outcome

Decision & outcome	Answer/decision	Name & title	Date
Summary of the outcome of the LIA			
Please confirm: Whether process shall continue, shall cease, or requires adjustments?			
Process owner or authorised person providing the above outcome of this LIA			
Next review date for LIA (where processing is ongoing)			

KEYSTONE

Let’s stay in touch

Follow us online & subscribe to our newsletter!

www.keystone-project.com

KEYSTONE EU

@KEYSTONE_EU