Orchestra

www.orchestra2020.eu

ORCHESTRA Project Deliverable: D1.2

Data Management Plan

Authors: Anne Freiberger, IKEM, Anna-Katharina Hübers, IKEM, Divy Gupte IKEM

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

About ORCHESTRA

The long-term vision of the ORCHESTRA is a future where it is easy to coordinate and synchronise the traffic management of all modes to cope with diverse demands and situations. Also, to facilitate optimal utilisation of transport networks and efficient multimodal transport services, both in rural and urban areas.

The project will:

- Establish a common understanding of multimodal traffic management concepts and solutions, within and across different modes, for various stakeholders and multiple contexts
- Define a Multimodal Traffic Management Ecosystem (MTME) where traffic managements in different modes and areas (rural and urban) are coordinated to contribute to a more balanced and resilient transport system, bridging current barriers and silos
- Support MTME realisation and deployments, through the provision of tools, models, and guidelines – including support for connected and automated vehicles and vessels (CAVs)
- Validate and adjust MTME for organisational issues, functionality, capability, and usability
- Maximise outreach and uptake of project results through strong stakeholder involvement

The project will provide a Polycentric Multimodal Architecture (PMA) that specify how diverse system components collaborate and interact, taking into account smart infrastructures, technical and organisational aspects and polycentric governance. The PMA will be supported by: 1) Enabling toolkit, 2) Deployment toolkit, 3) Documented lessons learned.

The project will validate the PMA and related tools and toolkits in two Living labs (in Norway and Italy), collectively covering both road, rail, water, and air transport. The Italian Living lab is focusing on traffic orchestration for the mobility of people, while the Norwegian Living lab is focusing on traffic orchestration for freight. The Living labs will be supported by simulations to enhance evaluations.

Legal disclaimer

This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

Acknowledgment of EU funding

The project has received funding from the European Union’s Horizon 2020 research and innovation program under Grant Agreement No 953618.

For more information

Project Coordinator: Runar Søråsen, runar.sorasen@its-norway.no

Dissemination Manager (WP7 leader): Jenny Simonsen, jenny.simonsen@its-norway.no

Executive Summary

The data management plan (DMP) provides an overview of how research data in ORCHESTRA will be managed during the implementation phase, as well as after the end of the project.

It establishes a data summary, which explains the purpose of the different data collection activities in ORCHESTRA. The different purposes range from gathering barriers and enablers for MTMEs, as well as designing the vision of multimodal traffic orchestration, both for a 2030 and 2050 scenario. Moreover, the data collection will help to develop the enabling toolkits and architecture for MTMEs. The data summary also covers aspects of the possible re-use of data, the data origin and the estimated size. The analysis of the data utility expects the data to be useful for scientists in the field of traffic management, as well as EU and national institutions or third parties, such as fleet operators.

Furthermore, the DMP covers action, that will be implemented in order to apply the FAIR principle (findable, accessible, interoperable and re-usable). Therefore, it distinguishes between data storage solutions during the implementation phase of the project and afterwards. It also covers the topic of allocated resources and estimated costs for Open Access publications.

The topic of safety and security of data addresses the legal requirements deriving out of the General Data Protection Regulation (GDPR) in regard of the most important general principles, like purpose limitation, data minimisation, storage limitation, integrity and confidentiality. Cybersecurity requirements explain measures, like pseudonomysation, encryption, confidentiality and the resilience of systems amongst others. The roles of responsibility establishes the difference between processors and controllers. The consequences for publication activities are summarised, which mainly address the requirements of informed consent.

Moreover, Intellectual Property Rights (IPR), which can arise in the context of research data are illustrated covering the definition of trade secrets, copyrights, special database rights, patents as well as the waiver and licensing of rights. In addition, a short summary of how IPR are addressed through the ORCHESTRA Grant Agreement is given. For relevant ethical aspects the report references D1.3 *Ethics, Security, and Gender Balance Plan*.

Lastly, the report is a living document and will be updated several times during the implementation phase of the project in accordance to the inserted timeline.

Table of Contents

About ORCHESTRA ... **2**

Legal disclaimer ... 2

Acknowledgment of EU funding ... 2

Executive Summary ... **3**

List of Abbreviations ... **7**

List of Definitions ... **8**

1 About this Deliverable ... **9**

1.1 Why would I want to read this deliverable? ... 9

1.2 Intended readership/users ... 9

1.3 Structure ... 9

2 Data Management in ORCHESTRA ... **10**

2.1 Data Summary ... 10

2.1.1 Purpose of data collection ... 10

2.1.2 Data types and formats ... 10

2.1.2.1 Specific status of personal data ... 10

2.1.2.2 Data categories ... 11

2.1.2.3 Data types & file formats ... 12

2.1.2.4 Updates ... 13

2.1.3 Re-use of data ... 13

2.1.4 Data origin ... 13

2.1.5 Size ... 13

2.1.6 Data utility ... 13

2.2 Implementation of the FAIR principle ... 13

2.2.1 Making data findable ... 13

2.2.1.1 Data storage solution during ORCHESTRA ... 13

2.2.1.2 Naming & Identification ... 14

2.2.1.3 Version numbers ... 14

2.2.1.4 Metadata ... 14

2.2.2 Making data openly accessible ... 14

2.2.2.1 Legal requirements regarding open access to research data ... 14

2.2.2.2 Zenodo repository ... 15

2.2.2.3 Public & confidential deliverables ... 15

2.2.2.4 Open Research Europe ... 16

2.2.3 Making data interoperable ... 16

2.2.4 Data re-use 17
2.3 Allocation of resources 17
3 Safety & Security of Data 18
3.1 Legal requirements for personal data (GDPR) 18
3.1.1 Applicability of GDPR requirements 18
3.1.2 GDPR principles 18
3.1.3 Consent form 18
3.1.4 GDPR and research projects 19
3.1.5 GDPR & Cybersecurity 21
3.1.6 Secure storage during the project 22
3.1.7 Secure storage after the project 22
3.1.8 Roles of responsibility 22
3.1.9 Consequences for publication activities 23
3.2 Cybersecurity Act 23
4 Intellectual Property Rights 25
4.1 Overview: IPR and Research Data 25
4.1.1 Trade secrets 25
4.1.2 Copyrights 25
4.1.3 Special database rights 25
4.1.4 Patents 26
4.1.5 Waiver and licensing of rights 26
4.1.6 Terms of use and other contractual agreements 26
4.2 IPR within the ORCHESTRA Grant Agreement and the ORCHESTRA Consortium Agreement 26
4.2.1 Access Rights for beneficiaries (Art. 25 and 31 GA, Art. 9 CA) 27
4.2.2 Ownership of results (Art. 26 GA, Section 8.1 and 8.2 CA) 27
4.2.3 Protection of results (Art. 27 GA) 27
4.3 Consequences for publication activities 28
5 Ethical aspects 30
6 Timeline – Date Management Updates 31
7 Conclusions 32
8 References 33
8.1 Primary Sources 33
8.2 Secondary sources 33
9 Annexes 35
9.1 Annex 1: Data Management Questionnaire 35

Members of the ORCHESTRA consortium 38

List of Tables

Table 1: List of abbreviations 7
Table 2: List of definitions 8
Table 3: DMP - Updates 31

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

List of Abbreviations

Table 1: List of abbreviations

Abbreviation	Explanation
CA	Consortium Agreement
DMP	Data Management Plan
DOI	Digital Object Identifier
EC	European Commission
GA	Grant Agreement
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System[1]
IP	Intellectual Property
IPR	Intellectual Property Rights

[1] Examples include GPS, GLONASS, Galileo and BeiDou

List of Definitions

Table 2: List of definitions

Definition	**Explanation**
FAIR	Is a common term used to describe principles for managing data. The data should be Findable, Accessible, Interoperable and Re-usable (FAIR)

1 About this Deliverable

1.1 Why would I want to read this deliverable?

The Data Management Plan (DMP) aims at describing the management of research data within ORCHESTRA. It describes the research data generated, collected, processed and analysed within the project, as well as the data flow and exchange within the project consortium.

The DMP also focuses on management of data gathered from the project's Living Labs. Moreover, it provides the internal procedures for dealing with the collection and handling of data, whereas the goal of FAIR data will be implemented. The DMP will focus on establishing the secure use of personal data, privacy requirements, cybersecurity, intellectual property rights, and access of all project partners to all relevant project data, breaking down the GDPR as well as further EU legislation to practical requirements and proceedings for the project.

The DMP is a living document. It will be updated continuously throughout the project (cf. timeline, Section 6).

1.2 Intended readership/users

To monitor the implementation of the DMP, and administer the list and repository of relevant research data, the role of a **Data Manager** (Anne Freiberger/IKEM) has been established. The Data Manager can refer to this deliverable for its tasks.

Moreover, consortium partners responsible for **Research data management (Task 6.4)** have to manage the data received from work package (WP) 5 according to the DMP. They can refer to this deliverable to keep track of research data generated, processed and analysed throughout the project.

All consortium members can refer to this plan for information on open access and legal issues regarding the handling of data during the duration of the ORCHESTRA project.

1.3 Structure

This document comprises of seven chapters. Following the introduction, the second chapter addresses the topic of Data Management in ORCHESTRA. It will provide a summary of the data collected and processed (Section 2.1) and the implementation of the FAIR principle (Section 2.2) according to the DMP Template provided by the EC's H2020 Online Manual.[2]

The third chapter introduces safety and security measures for data in ORCHESTA. It will notably describe the legal requirement arising from the General Data Protection Regulation (GDPR) for personal data.

The fourth chapter develops an Intellectual Property (IPR) strategy according to the ORCHESTRA Grant Agreement and Consortium Agreement.

For ethical aspects, chapter five refers to the Ethics, Security and Gender Balance Plan (D1.3).

Chapter six will develop a time plan for the updates of the DMP, followed by conclusions (Chapter 7).

[2] available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm.

2 Data Management in ORCHESTRA

This DMP will address the relevant aspects of making the research data generated during ORCHESTRA **FAIR, i.e. findable, accessible, interoperable and re-usable**. It is based on the DMP Template provided by the EC's H2020 Online Manual.[3] All partners have been asked to provide information about their use of data throughout the project using a questionnaire that has been distributed to the respective work package leaders. The information gathered from this procedure have been analysed and incorporated into the Plan. The main aspects of the analysis that are going to be identified are the following:

- What data is going to be collected, processed, and analysed throughout ORCHESTRA project?
- How is the data going to be collected and processed throughout ORCHESTRA project?
- Which data is going to be provided as open access and which is not (confidential)?

The DMP is a **living document**. It will be updated continuously. Notably, once the work packages have progressed, the characterisation of data that is going to be collected, processed, and analysed is expected to be extended (cf. timeline, Section 6).

The DMP will also establish the secure use of personal data, privacy requirements, and cybersecurity, breaking down the GDPR and related EU legislation. It will take into consideration data ownership, privacy and security.

2.1 Data Summary

This section provides the data summary for research data in ORCHESTRA.

2.1.1 Purpose of data collection

The ORCHESTRA project, seeking to develop a Multimodal Traffic Management Ecosystem (MTME), will generate, collect, and process vast amounts of data in order to coordinate and synchronise transport management and optimise transport networks.

Data will be collected to gather information on barriers and enablers for MTMEs, to develop/understand needs and activities, and to develop an enabling toolkit and architecture for MTMEs. It shall also serve to design 2030 and 2050 visions of multimodal traffic orchestration.

2.1.2 Data types and formats

This section gives an overview of data types and formats generated, processed and analysed.

2.1.2.1 Specific status of personal data

Regulations applicable to the processing of data distinguish between personal and non-personal data. Personal data is defined under the **General Data Protection Regulation (GDPR)** as "any information relating to an identified or identifiable natural person ('data subject')", Art. 4(1) GDPR. For instance, identifying characteristics such as name, address and date of birth, external characteristics (gender, eye colour, height and weight), but also internal characteristics (opinions, convictions, wishes etc.), communication and relationship are personal data.[4]

[3] available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm.

[4] BeckOK DatenschutzR/Schild, DS-GVO Art. 4 pt. 3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

During the ORCHESTRA project, personal data will be collected and processed from:

- project partners;
- stakeholders.

The personal data collected includes:

- names
- addresses
- signed consent forms
- email addresses
- telephone numbers
- video material and photographs
- institutions/companies that individuals work for
- opinions of academics and other stakeholders

The collection and processing of this data must comply with the requirements set out in the GDPR (cf. Section 4.1).

Stricter conditions for processing apply to **special categories of personal data**, i.e. data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, data concerning a natural person's sex life or sexual orientation, Art. 9 GDPR.

2.1.2.2 Data categories

In order to develop an overview of the research data that will be collected, generated, and processed within ORCHESTRA, six different data categories have been defined. These six different data categories are the ones most crucial for the project activities. The data collection approaches of each of the six data categories differ from each other.

- **CONSORTIUM DATA:**

The first category is consortium data, which comprises data from project partners. Consortium data involves data related to administration and management within the consortium. It will involve technical & innovation management throughout ORCHESTRA. This data will mostly be collected in WP1 "Coordination and Innovation Management" and in WP7 "Outreach".

- **LEGISLATIVE DATA:**

The second category is legislative data, which comprises of legal aspects within ORCHESTRA. Legislative data acts as an integration between the consortium data and legal aspects such as GDPR guidelines, cybersecurity law and so on. This data will mostly be collected while addressing issues of ethics and data management in WP1 "Coordination and Innovation Management."

- **STAKEHOLDER DATA:**

The third category is stakeholder data. Stakeholder data includes data collected from stakeholders involved in the ORCHESTRA project. These stakeholders include experts, interview partners and so on. This data will mostly be collected in WP2 "Target vision and scenarios", WP3 "Polycentric traffic management design" WP4 "Enabling toolkit organizational and business models, WP5 "Living labs trials and simulations", WP6 "Evaluations and lesson learned", WP7 "Outreach".

- **SIMULATION DATA:**

The fourth category is simulation data. Simulation data involves data collected for simulation and design of polycentric traffic management ecosystem. It deals with addressing the functionalities of resilience, arbitration, flexibility, safety and security. This data will be collected in WP3 “Polycentric traffic management design” and WP6 “Evaluation and lessons learned”.

- **TOOLKIT DATA:**

The fifth category is toolkit data. Toolkit data involves data collected for developing technical tools and assessment methodology. Also, it will be collected from the simulations carried out in Living Labs. This data will mostly be collected, generated or analysed in WP4 “Enabling toolkit, organizational and business models” and WP6 “Evaluations and lesson learned”.

- **TRAFFIC DATA:**

The sixth category is traffic data. Traffic data involves data collected from living labs. This data helps in improving simulation, methods and training materials. This data will also help in integrating traffic management across all modes of transport. It will be mainly collected from the WP5 “Living labs trials and simulations”.

2.1.2.3 Data types & file formats

The data falling into the categories outlined above will belong to the following data types and file formats:

Data type	File format	Data category
Video Recordings	.mp4	Stakeholder data
Protocols	.docx	Stakeholder data
Images	.jpg	Stakeholder data
List of participants	.xlsx	Consortium data
Reports	.docx	Consortium data
Presentations	.pptx	Consortium data
Minutes (from interviews)	.odt	Stakeholder data
GNSS data	.lat / .lon	Toolkit data
Minutes (from workshops)	.docx	Stakeholder data
Audio recordings	.mp3	Stakeholder data
Images of posters	.jpg	Stakeholder data
GNSS locations of vehicles and goods (cargo, consignment etc.)	JSON	Traffic data

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

2.1.2.4 Updates

The data summary will be updated throughout the course of the project (cf. timeline, Section 6).

2.1.3 Re-use of data

Data produced by some project partners will partially be re-used by other beneficiaries. For instance, WP3 might re-use data produced in WP2.

2.1.4 Data origin

At the current state of the project, data will be gathered from interviews conducted with stakeholders, during workshops and internal project meetings.

Positioning data (GNSS) data will be collected through sensors and IoT devices from connected vehicles.

2.1.5 Size

to be updated.

2.1.6 Data utility

The data collected might be useful for other ORCHESTRA partners in the development of traffic management systems and, after publication, scientists in the field, the EU and national institutions.

GNSS data collected could be useful for third parties, such as fleet operators.

2.2 Implementation of the FAIR principle

ORCHESTRA will provide FAIR data as described in “Guidelines on FAIR Data Management in Horizon 2020”. The FAIR principle aims at making data findable, accessible, interoperable and reusable to ensure it is soundly managed.[5]

2.2.1 Making data findable

This section deals with required management steps in order to make data findable.

2.2.1.1 Data storage solution during ORCHESTRA

For **non-sensitive data** detailed above, communication purposes and cooperation, ORCHESTRA beneficiaries will use the ORCHESTRA MS Teams channel as a storage and file sharing solution.[6]

Sensitive data collected and processed by the beneficiaries will, for the time being, be secured locally according to the data protection and data security policy of the respective beneficiary. Should sharing features for sensible data be necessitated for the purposes of ORCHESTRA, the DMP will be adapted accordingly. Bdrive has been envisioned as an appropriate data storage and sharing solution for sensible data.

[5] H2020 Online Manual, Open access & Data management, available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm.

[6] Cf. ORCHESTRA, D1.1 (Project Management Handbook).

Concerning the process of code development, a development platform (e.g. GitHub, GitLab) will be used to foster collaborative work. Between beneficiaries.

2.2.1.2 *Naming & Identification*

The following naming convention shall apply:

- for deliverables: Dx.y
- for other files (if suitable): YYYYMMDD_[Task n°]_[content description].[file format]
  - e.g. 20211020_T2.1_Minutes.docx

Filenames should not include version information since MS teams' version tracking function will be used.

Zenodo, which will be used as repository after the end of the project (cf. Section 2.2.2.2), assigns a digital object identifier (**DOI**) to every published record to ensure that research datasets and research findings stored in the repository are easily to find and uniquely citable. Data as well as the metadata will include the DOI.

2.2.1.3 *Version numbers*

Each deliverable will be assigned a Release Number to make its identification possible. MS Teams will be used for automatically keeping track of file versions.[7] Filenames should not include version information.

Upon publication in Zenodo, data files will be versioned automatically.

2.2.1.4 *Metadata*

Metadata, documentation, and code produced during ORCHESTRA will be deposited to Zenodo. Metadata will be licensed under CC0, except for email addresses. JSON-format will apply according to a defined JSON schema.

2.2.2 Making data openly accessible

This section provides information on how to make research data of ORCHESTRA openly accessible.

2.2.2.1 *Legal requirements regarding open access to research data*

According to the ORCHESTRA Grant Agreement, the beneficiaries must ensure open, free-of-charge access to **digital research data** generated in the action (**Art. 29.3 GA**).

According to the H2020 Annotated Model Grant Agreement "Open access to digital research data means taking measures to make it possible for end-users to access, mine, exploit, reproduce and disseminate the data via a **research data repository** without any charges for them."

The open access obligation covers all data (and associated metadata) generated in the course of the action or reused digitally in the action, i.e.

- the data needed to validate the results presented in scientific publications and associated metadata (i.e. data describing the deposited research data) and

[7] Cf. ORCHESTRA, D1.1 *Project Management Handbook*, p. 38.

- other data and associated metadata, as specified by the beneficiaries themselves in their data management plan.[8]

  Examples: statistics, results of experiments, measurements, observations resulting from fieldwork, survey results, interview recordings and images.

Exception: The beneficiary does not have to ensure open access to specific parts of the research data if the action's main objective (see Annex 1 to the GA) would be jeopardised. The DMP will contain the reasons for not giving access.

Currently, the following reasons for **restricting access** can be foreseen:

- Some confidential data relating to data measurements made in restricted parts of the use case sites may not be published (to be decided with the site owners);
- Personal data to which consent to publication has not been given.

2.2.2.2 Zenodo repository

To this end, ORCHESTRA will deposit data in **Zenodo**[9], which is a European scientific repository compliant with the European OpenAIRE program. Its scope encompasses all fields of research and all types of research artifacts.

All data file formats can be uploaded on Zenodo.

The file size limit in Zenodo is 50GB. Should higher quotas be necessary for individual project partners, the Data Manager should be contacted, and a request filed on his behalf with Zenodo (costs may arise).

The Zenodo repository was selected amongst alternatives because it offers a practical online service that allows researchers, scientists, EU projects, and institutions to showcase, share, and preserve multidisciplinary research results (data and publications), that are not part of the existing institutional or subject-based repositories of the research communities.

Zenodo provides the possibility to deposit data objects under closed, open, or embargoed access. Closed files will be protected against unauthorized access.

2.2.2.3 Public & confidential deliverables

To comply with the ORCHESTRA Grant Agreement, deliverables classified as "**public**" in Annex 1 will be made available to the public. Before publication they will be submitted for approval to the European Commission (EC) by the project coordinator. All deliverables approved by the EC will be uploaded to the ORCHESTRA project-website as digital copies. They will also be deposited on Zenodo under open access conditions.

A separate procedure will apply to **confidential** deliverables intended for dissemination to specific external parties with restricted access only. These deliverables or specific parts of them will be designated by the ORCHESTRA consortium. The consortium will also appoint the authorised parties upon request. A separate section of the project website will be dedicated to the digital publication of such deliverables.

[8] H2020 Annotated Model Grant Agreement.

[9] Zenodo repository, www.zenodo.org.

In Annex I of the GA the following deliverables have been defined as “confidential” and shall thus not be subject to open access:

- D1.1 *Project Management Plan & Handbook* – only for members of the consortium (including the Commission Services)
- D1.4 *Innovation strategy and process* – only for members of the consortium (including the Commission Services)
- D4.1 *Initial version of technical tools* – only for members of the consortium (including the Commission Services)
- D4.2 *Final version of technical tools for multimodal traffic management* – only for members of the consortium (including the Commission Services)
- D5.2 *Simulator* – only for members of the consortium (including the Commission Services)
- D8.1 *H – Requirement No. 1* – only for members of the consortium (including the Commission Services)
- D8.1 *POPS – Requirement No. 2* – only for members of the consortium (including the Commission Services)
- D8.3 *NEC – Requirement No. 3* – only for members of the consortium (including the Commission Services)
- D8.4 *EPQ – Requirement No. 4* – only for members of the consortium (including the Commission Services)

2.2.2.4 Open Research Europe

Additionally, ORCHESTRA beneficiaries can publish (public) project results on **Open Research Europe**. With Open Research Europe[10], the European Union has developed an open access online publishing platform whose objective is precisely to facilitate Horizon 2020 beneficiaries’ data deposition in accordance with their funding terms. To this end, authors can submit their research online: https://open-research-europe.ec.europa.eu/for-authors/publish-your-research.

Each submission will be checked by an in-house editorial team and published under a CC BY licence (or CC0 licence for data) before being opened to peer review by independent experts. An individual digital object identifier (DOI)[11] will be assigned to each article, its versions, peer reviews and some datasets. The CrossMark Identification Service™ provides a summary of all work associated with an article assuring that multiple article versions, updated peer reviews and linked articles are workable.

Open Research Europe offers a tailor-made and easy-to-handle online platform which makes publications from Horizon 2020 projects findable, accessible, and re-usable.

2.2.3 Making data interoperable

Zenodo provides for the interoperability of (meta)data. It uses a formal, accessible, shared, and broadly applicable language for knowledge representation and vocabularies that follow FAIR principles.[12]

[10] Open Research Europe, https://open-research-europe.ec.europa.eu/.

[11] According to the International DOI Foundation Handbook “[a] DOI name is permanently assigned to an object to provide a resolvable persistent network link to current information about that object, including where the object, or information about it, can be found on the Internet. While information about an object can change over time, its DOI name will not change.”, available at: https://www.doi.org/hb.html.

[12] https://about.zenodo.org/principles/.

2.2.4 Data re-use

Zenodo also ensures the reusability of ORCHESTRA data. (Meta)data will be assigned multiple accurate and relevant attributes using DataCite’s mandatory terms and released with a clear and accessible data usage license.[13]

2.3 Allocation of resources

Currently, it is not foreseeable that costs will be incurred for making data FAIR in ORCHESTRA. Zenodo is a free of charge repository for specific data sizes. All Open Access costs, as well as article processing charges or publication fees are eligible.

[13] https://about.zenodo.org/principles/.

3 Safety & Security of Data

This section covers aspects on safety and security of data.

3.1 Legal requirements for personal data (GDPR)

Data collected, processed and published within ORCHESTRA shall comply with the existing data safety and security provisions.

3.1.1 Applicability of GDPR requirements

Personal Data: The GDPR lays down rules for the protection of personal data (cf. Section 2.1.2.1).

Processing: These rules must be observed by all ORCHESTRA beneficiaries when they process personal data of data subjects established in the EU. Processing is defined by Art. 4(2) GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means". Examples include 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.

3.1.2 GDPR principles

Art. 5 GDPR establishes seven principles relating to processing of personal data which shall be satisfied by the ORCHESTRA project partners. These are:

1. **lawfulness, fairness and transparency** in relation to the data subject (Art. 5(1) lit. a)
2. **purpose limitation** – data shall only be collected for specified, explicit and legitimate purposes and not in a way, that is incompatible with these purposes (Art. 5(1) lit. b)
3. **data minimisation** – data collection shall be adequate, relevant and limited to the necessary (Art. 5(1) lit. c)
4. **accuracy** – data shall be accurate and kept up to date (Art. 5(1) lit. d)
5. **storage limitation** – data shall be kept in a form which permits identification of subjects for no longer than is necessary (Art. 5(1) lit. e)
6. **integrity and confidentiality** – data shall be processed in a way that ensure appropriate security of the personal data (Art. 5(1) lit. f)
7. **accountability** – the controller shall be responsible for following the above principles (Art. 5(2))

3.1.3 Consent form

The processing of all personal data is subject to consent by the data subject (**principle of consent**), Art. 6(1) lit. 1, 7 GDPR. The data subject shall be provided all information laid down in Art. 13 and 14 GDPR at the time when the data are obtained.

The legal ground for personal data processing will be **informed consent** by the data subject. Therefore, ORCHESTRA project partners will provide an Informed Consent form to all data subjects whose data will be processed during their research. This Consent form will include:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the purposes of the processing for which the personal data are intended;

- the legal basis of the processing which will be the consent given in the form;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.

Cf. Art. 13 and 14 GDPR for further details.

3.1.4 GDPR and research projects

Taking due account of the fundamental right of freedom of research[14], the GDPR allows for eased requirements regarding the processing of personal data for scientific research:

- **Relaxed purpose limitation and further processing**: If data that has already been collected for a specified purpose is further processed for research purposes, the processing is deemed compatible with the initial purpose and may, therefore, take place, Art. 5(1) lit. b GDPR. Nevertheless, an independent legal basis is required for secondary processing for research purposes. Data controllers cannot simply rely on the legal basis of the primary purpose.

- **"Broad consent"**: In deviation from the principle of specific consent, data subjects can give their broad consent to certain areas of scientific research, cf. recital 33 GDPR. This allows for the processing of data although precise preliminary research questions and objectives are commonly lacking.[15] Broad consent is only valid if its use is absolutely necessary; recital 33 does not replace the requirement of specific consent altogether.[16] Furthermore, the research project, the framework conditions, explicitly not yet defined purposes, possible risks and specific security measures must be described as precisely as possible in order to meet the basic data minimisation, anonymisation, data security and transparency requirements of the GDPR.[17] For this purpose, it is advisable to prepare a comprehensive research plan available for data subjects to take note of before they consent.[18] For special categories of data (Art. 9 GDPR) stricter requirements may apply.[19] The recognised ethical standards of scientific research[20] as well as other requirements for consent (voluntary, informed, unambiguous, see Art. 7 GDPR) must also continue to be met.

[14] Art. 13 GRCh.

[15] Recital 33 GDPR; Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz", 2. Edition, 2020, S. 21.

[16] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en, para. 156; BeckOK Datenschutzrecht/Eichler, DSGVO Art. 89, Rn. 2.1.

[17] BeckOK Datenschutzrecht/Eichler, DSGVO Art. 89, Rn. 2.1.

[18] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en, para. 162.

[19] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en, para. 157.

[20] Recital 33 GDPR.

- **Exception to the principle of storage limitation**: Research data may be stored for longer, although not indefinitely, 5(1) lit. e GDPR. This preserves the proper functioning of research.[21]

- **Exception to the prohibition of the processing of special categories of personal data**[22]: As a matter of principle special categories of personal data (cf. Section 3.2) may not be processed, Art. 9(1) GDPR. If the processing is defined as necessary for scientific purposes by national or EU law, it may nonetheless be lawful, Art. 9(2) lit. j. However, the essence of the right to data protection and specific measures to safeguard fundamental rights must be respected.

- **No legal duty to inform**: Where personal data have not been obtained from the data subject but the fulfilment of the legal duty to inform proves impossible, would involve a disproportionate effort, or would render impossible or seriously impair the achievement of the research purposes, there is no obligation to provide the data subject with the information, Art. 14(5) lit. b.

- **No right to be forgotten**: The duty to erase personal data upon request without undue delay is also excluded to the extent that processing is necessary for scientific research purposes, 17(2) lit. d.

Data processing for research purposes is, in all cases, subject to the **conditions and safeguards set out in Article 89(1)** of the GDPR: Appropriate measures must be taken for the rights and freedoms of data subjects, the appropriateness of which depends on the specific case, notably which personal data are processed and who is involved in the process.[23] In particular, the principle of data minimisation must be respected by taking appropriate technical and organisational measures (such as pseudonymisation[24] or anonymisation[25] of data). However, the measures should not frustrate the achievement of the research purposes. Appropriate measures could consist of the encryption of data during transmission, confidentiality agreements, the selection and concrete design of data access (guest researcher workstation, download or remote access).[26]

According to Art. 89(2) GDPR the Union or national legislature can adopt further derogations to the rights in Art. 15, 16, 17 and 21 GDPR. These exemptions are, again, subject to the conditions and safeguards of Art. 89(1) GDPR being met. They are justified only insofar as the rights under Art. 15, 16, 18 and 21 GDPR are likely to frustrate or seriously prejudice the achievement of the research purposes and such exemptions are necessary for the fulfilment of those purposes.

[21] BeckOK DatenschutzR/Schantz, DSGVO Art. 5, Rn. 34.

[22] Special categories of personal data comprise all 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, Art. 9 GDPR.

[23] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz", 2. Edition, 2020, S. 23.

[24] Vgl. Art 89 Abs. 1, S. 3 i.V.m. Art. 4 Nr. 5 DSGVO.

[25] Vgl. Art 89 Abs. 1, S. 4 DSGVO.

[26] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz", 2. Edition, 2020, S. 23.

These derogations only apply to **data processed for scientific research purposes**. According to the EDPB, "'scientific research' […] means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice."[27]

3.1.5 GDPR & Cybersecurity

Security of personal data is one of the core obligations arising from the GDPR. It is mandated in Art. 5 and concretised in Art. 32 GDPR.

According to Art. 32 GDPR the controller and the processor shall "ensure a level of security appropriate to the risk". The GDPR follows a **risk-based approach**, i.e., the higher the risk, the more rigorous the measures that have to be taken in terms of data protection. Data controllers and processors must reflect the risks of their respective processing and take the measures adequate to the risk to achieve the highest possible level of security.[28]

To this end, certain measures may have to be taken (Art. 32 GDPR):

- Pseudonomysation: dissolving the personal reference of data to such an extent that it is only possible to draw conclusions about a specific person by consulting additional information;[29]
- Encryption: the personal reference is retained in principle, but cannot be read without a suitable key;[30]
- Confidentiality: information must be protected against unauthorized disclosure and sensitive data must be made accessible only to authorized persons;[31]
- Integrity: the manipulation of data is prevented, i.e., information is protected from undergoing unauthorized modification;[32]
- Availability: the system actually performs as required, which in the case of data storage can also mean that the data is not available due to data protection requirements;[33]
- Resilience of systems and services processing personal data: the system must be able to cope with hazardous situations, in particular not to fail in the event of disruptions but to maintain its performance;[34]
- Ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

ORCHESTRA project partners will be engaged in adopting the appropriate security measures for the protection of personal data in compliance with the GDPR. They will employ all possible organisational and technical security measures instrumental in achieving this objective.

[27] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en, para. 153.
[28] Paal/Pauly/Martini, 3. Edition, 2021, DS-GVO Art. 32 Rn. 3.
[29] Ibid. Art. 32 Rn. 33.
[30] Ibid. Art. 32 Rn. 34.
[31] Ibid. Art. 32 Rn. 35d.
[32] Ibid. Art. 32 Rn. 36
[33] Ibid. Art. 32 Rn. 38.
[34] Ibid. Art. 32 Rn. 39.

Such security measures may include:

- A register of the IT resources used for the processing of personal data (hardware, software, and network), including type (server, workstation, …) and location;
- communication and awareness of the responsibilities and obligations related to the processing of personal data;
- an access control system and authentication mechanism for all users accessing the IT system using complex passwords;
- implementation of security settings, such as anti-virus applications, use of authorised software applications, session time-outs when the user has not been active for a certain time period, regular security updated;
- encrypted communication through the Internet (TLS/SSL);
- backup and data restore procedures;
- appropriate management of mobile/portable devices;
- software based overwriting prior to media disposal (alternatively, physical destruction);
- physical access to the IT system only by authorised personnel.[35]

3.1.6 Secure storage during the project

See section 2.2.1.1 on this question.

3.1.7 Secure storage after the project

Research data generated and re-used during the project will be stored on Zenodo after the finalisation of ORCHESTRA (cf. Section 2.2.2.2).

3.1.8 Roles of responsibility

The responsibilities arising from the GDPR are directed at the **controller** which is the "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Art. 4(7) GDPR). In the case of legal entities, this is the managing director or the board of directors.[36]

Joint control occurs when two or more controllers jointly determine the (respective or joint) purposes and means of processing (Art. 26(1) GDPR). They must jointly determine which of them fulfils which obligations under the GDPR and are liable for this to the data subject. The essence of the arrangement shall be made available to the data subject. Controllers have the legal obligation to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR as well as to *pre-emptively* implement data-protection policies (especially by means of „data protection by design" and „data protection by default", Art. 24, 25 GDPR). The measures taken must be reviewed and updated regularly. Violations are sanctioned with a fine and may lead to claims for damages by affected persons. Self-regulatory mechanisms like codes of conduct or certifications may be useful to demonstrate compliance.

Processor is the "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Art. 4 Nr. 8 GDPR). He is only responsible for the technical execution of the decisions taken, while the controller is authorised to give instructions and has the

[35] ENISA, "Guidelines for SMEs on the security of personal data processing", December 2016.

[36] BeckOK DatenschutzR/Schild, DS-GVO, Art. 4, para. 89.

power to decide on the purposes and means of the processing.[37] However, he has his own duty of documentation (Art. 30(2) GDPR). He shall be jointly and severally liable with the controller for damage suffered by the data subject (Art. 82).[38]

The research partners involved in the research activities of WP2 concerning stakeholder involvement through workshops and interviews may be regarded as joint controllers in accordance to Art. 26 (1) GDPR. Therefore, they are obliged to follow an internal agreement on how responsibilities concerning data subject's rights are implemented. The most important responsibilities are:

- Consent in accordance to Art. 6 GDPR
- Information in accordance to Art. 13 and 14 GDPR
- Rights of Research participants Art. 12 to 23 GDPR
- Responsibility of Controllers Art. 24 GDPR
- Data security Art. 32 GDPR
- Notification of personal data breach Art. 33 GDPR

The responsibilities are shared to the extent, that each beneficiary who is undertaking the interviews with stakeholders is obliged to fulfil the GDPR requirements in regard of the specific interviews.

Moreover, in regard of the workshop the specific host beneficiary is responsible for the implementation of the GDPR requirements.

3.1.9 Consequences for publication activities

The processing of anonymous data, including for research purposes, is not covered by data protection law. Therefore, research results should preferably be published anonymously.

Insofar as personal data, i.e., information relating to an identified or identifiable natural person, are to be published, the processing is only lawful if the data subject has given consent to this (Art. 6(1) lit. a GDPR). Consent shall be specific to the publishing for scientific purposes. (Broad consent for research purposes is also admissible - but only to the extent that a specification is not possible, see above.)

More information on this topic can be found in D8.1 *H - Requirement No. 1.*

3.2 Cybersecurity Act

The Cybersecurity Act[39] broadens the EU Agency for cybersecurity (ENISA) mandate, its resources and tasks. ENISA shall assist Member States and Union with cybersecurity strategies and awareness. To this end, it shall, inter alia, set up and maintain an EU-wide common cybersecurity certification framework for information and communications technology (ICT) products, services and processes as well as its technical grounds. Accordingly, in May 2021, based on Art. 48.2 of the Cybersecurity

[37] CJEU, C-210/16 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH); EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725", available at: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf, 34f (including check-lists for the identification of controller and processor).

[38] BeckOK DatenschutzR/Schild, DS-GVO, Art. 4, para. 97.

[39] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L 151/15.

Act, ENISA has published the Common Criteria based European candidate cybersecurity certification scheme (EUCC) scheme, an Ad Hoc Working Group to support the preparation of a candidate EU cybersecurity certification scheme.[40] The EUCC scheme shall serve as a reference point for cybersecurity functionalities of ICT products, services and processes, in the interest of internet users and consumers.[41] Although the proposed EUCC label and associated mark may be useful in identifying suitable products and services for the secure processing of data in the future, the Cyberspace Act is of no relevance to the management of data in ORCHESTRA. Should ORCHESTRA produce information and communication technology products the requirement laid down in the EUCC scheme shall be fulfilled.

[40] See ENISA, Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 [2021], available at Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 — ENISA (europa.eu).

[41] ENISA, Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 [2021], available at Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 — ENISA (europa.eu), p. 9.

4 Intellectual Property Rights

This section deals with the topic of Intellectual Property Rights (IPR).

4.1 Overview: IPR and Research Data

ORCHESTRA beneficiaries must respect all IPR attached to intellectual goods. Especially IPR on data may play a significant role in the research conducted during the project.

Different legal rights can be attached to data:

4.1.1 Trade secrets

Trade secrets (also “proprietary” or “confidential” information) are all information which are subject to secrecy measures and derive their economic value from not being generally known or readily ascertainable.[42] This definition may include non-published research data. Trade secrets generated within the scope of an employment are owned by the employer.

4.1.2 Copyrights

Copyrights apply to original works of authorship. Only the author(s), i.e. the person(s) making the creative or editorial decisions about how ideas and facts are expressed, have the exclusive right to reproduce the work, to publicly distribute copies, to display, publicly perform, or otherwise communicate the work to the public, and to make adaptations to it.[43] They are the owners of the rights. In principle, data are not protected by copyrights since they are facts which are part of the public domain. They can be copied, shared, and reused freely. In contrast, some datasets may be subject to copyrights when they have an element of originality, and a discretionary choice was exercised. This is the case for creative decisions regarding the selection of data, their arrangement and visualisations (i.e. in excel spreadsheets), annotations, or other forms of metadata. However, the underlying data can still be used, renamed and re-organised.[44]

4.1.3 Special database rights

For databases created or maintained and used within the EU the EU Database Directive[45] applies. It protects databases that require a “substantial investment” to assemble or maintain, i.e. in the **procurance of the data** (not data creation), for a period of 15 years against the extraction or reutilisation of its substantial parts and against the frequent extraction of its insubstantial parts.[46] Research data, in general, meets the “substantial investment” requirement, but a **limitation** applies for non-commercial research to which special database rights do not apply. The person or entity making the substantial investment is the owner of the right.

[42] Carroll, Sharing Research Data and Intellectual Property Law: A Primer, available at: Sharing Research Data and Intellectual Property Law: A Primer (plos.org).

[43] Ibid.

[44] Ibid., Cornell University, “Introduction to intellectual property rights in data management”, available at: Introduction to intellectual property rights in data management | Research Data Management Service Group (cornell.edu).

[45] Carroll, Sharing Research Data and Intellectual Property Law: A Primer, available at: Sharing Research Data and Intellectual Property Law: A Primer (plos.org).

[46] Ibid.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

4.1.4 Patents

Patents are "exclusive rights in inventions that are new, useful and demonstrate an inventive step in comparison to what is already known within the relevant field of knowledge"[47]. They must be applied for and granted by a national public authority and apply only within national borders. Since most research data does not fall within the term "inventions" patents do not play an important role for research.[48]

4.1.5 Waiver and licensing of rights

Copyright and special database rights can be waived by the owner. This is possible, for example, by means of the Creative Commons[49] **CC0 waiver**.

A clear permission to reuse the data can also be given in form of a **license**. Such copyright licenses exist under the Creative Commons Framework. The broadest license is CC-BY under which the user must provide only an attribution to the work as directed by the licensor. Other licenses add different conditions to the attribution requirement:

- CC BY-SA: the user must license under the same license;
- CC BY-NC: the license is limited to non-commercial uses:
- CC BY-ND: only copy-paste reuse is allowed, not the creation of derivative works

When uploading data and results to Zenodo, ORCHESTRA members must specify the license for the data files according to their dissemination level (public/confidential).

Art. 30 GA, Art. 8.3 CA – "Licensing of results": Each beneficiary may transfer ownership of its results but must ensure that the obligations on joint and agency ownership, protection of results, exploitation, and dissemination, continue to apply. The beneficiary may give 45 days advance notice to the other beneficiaries that have or may request access rights (not waived under Art. 8.3.2 CA). Each beneficiary may also grant licenses to its results.

4.1.6 Terms of use and other contractual agreements

Finally, where no underlying IPR exists, "terms of use" may apply to the site from which the data is downloaded. These "terms of use" are enforceable in courts. However, their use is widely limited by the EU Database Directive which excludes any additional restrictions to those provided for in the Directive.

Non-Disclosure Agreements (NDAs), too, constitute contractual agreements that must be respected by the parties. They apply to factual data as well as data protected under copyright law or database rights.

4.2 IPR within the ORCHESTRA Grant Agreement and the ORCHESTRA Consortium Agreement

The Grant Agreement (GA) and the Consortium Agreement (CA) set out specifications as to access rights for background and results (5.2.1) and ownership of results of ORCHESTRA (5.2.2)

[47] Carroll, Sharing Research Data and Intellectual Property Law: A Primer, available at: Sharing Research Data and Intellectual Property Law: A Primer (plos.org).
[48] Ibid.
[49] See creativecommons.org.

4.2.1 Access Rights for beneficiaries (Art. 25 and 31 GA, Art. 9 CA)

Some participants have a number of rights to access results or background of the action.

Access rights to background for action exist, under certain conditions,

- for beneficiaries, where needed to
    - implement their own tasks under the action (25.2): royalty-free, without administrative transfer costs
    - exploit their own results (25.3): under fair and reasonable conditions;
- for affiliated entities (under fair and reasonable conditions, 25.4).

Fair and reasonable conditions can comprise financial terms or royalty-free conditions, taking into account the specific circumstances of the request for access.

The background for action, including intellectual property rights held by the beneficiaries, has been defined and agreed on by the ORCHESTRA beneficiaries before they acceded to the Agreement or needed to implement the action or exploit its results (so called "agreement in background", Art. 24 GA). The parties to the GA have done so in Attachment 1 of the ORCHESTRA CA: Sintef AS, CertX, SEA have identified a background.

Art. 31 GA defines similar **access rights to results** for other beneficiaries, affiliated entities, EU institutions, bodies, offices or agencies. Access rights to results shall be granted on Fair and Reasonable conditions and, in case of results for internal research, on a royalty-free basis. A request can be made up to twelve months after the end of the Project or after the termination of the requestion party's participation.

All requests for access rights shall be made in writing and shown to be necessary (Art. 9.2.6 and 9.2.7 CA).

4.2.2 Ownership of results (Art. 26 GA, Section 8.1 and 8.2 CA)

Results, such as data, knowledge or information that is generated in the action, and the attached IPR, are owned by the beneficiary that generates them. The Innovation Manager (Alessandra Tedeschi) will maintain a list of ownership of results.

Where the respective contributions cannot be discerned or results cannot be separated, several beneficiaries can have **joint ownership** which must be defined in a "joint ownership agreement". Each joint owner is entitled to

- use the results for *non-commercial* research activities without consent and on a royalty-free basis or
- *otherwise* exploit the results and grant non-exclusive licenses if the other joint owner is given 45 days advance notice and fair and reasonable compensation (Art. 8.2 CA).

If the owner does not protect the results/stops protecting them, the Agency may assume ownership under the conditions laid down in Art. 26.4.2 GA.

4.2.3 Protection of results (Art. 27 GA)

Each beneficiary has the obligation to protect its results. It must take the necessary measures to protect them if they can "reasonably be expected to be commercially or industrially exploited and if protecting them is possible, reasonable and justified". In case the beneficiary does not do so, the Agency can assume ownership. Applications must, in principle, include a reference to EU Horizon 2020 funding.[50]

4.3 Consequences for publication activities

According to Art. 29.1 GA and Section 9 CA, the beneficiaries have the obligation to disseminate their own results, including in scientific publications (in any medium).

Procedure (Art. 29.1 GA)

Advance notice of at least 45 days must be given to the other beneficiaries, together with sufficient information on the results disseminated.

The other beneficiaries have a **right to objection** (within 30 days) where they have a legitimate interest in relation to the results or background that would be significantly harmed; that is, where:

- protection of the objecting party's results or background would be adversely affected;
- the objecting party's legitimate interests in relation to the results or background would be significantly harmed.

Objection must be given in writing to the Coordinator and the party/parties proposing the dissemination. It must include a precise request for necessary modifications. The objecting party can request a publication delay of max. 90 calendar days.

Dissemination can still take place if appropriate steps are taken to protect the objecting party's interests.

Exception: Advance notice is not necessary where the publication is solely based on own results and other scientific sources already published (Art. 8.4.2.1 CA)

Open access (Art. 29.2)

The publication must be made under open access conditions to all peer-reviewed scientific publications. In particular, the publication must be deposited in a **repository** for scientific publications, which shall also be Zenodo (cf. Section 2.2.2).

The publication deposited in a repository must include:

- The research and other data (including associated metadata) and information about tools and instruments at the disposal of the beneficiaries necessary for validating the results as specified in Section 2.1 of this plan.
- The bibliographic metadata: in standard format, including
  - o the terms "European Union (EU)" and "Horizon 2020"
  - o the name of action, acronym and grant number: 953618
  - o the publication date, length of embargo period if applicable (the need for embargoes is not foreseeable yet)
  - o a persistent identifier which will be the DOI automatically assigned by Zenodo
- where possible, the tools and instruments necessary for validating the results themselves.

[50] "The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618".

Open access must be ensured:

- on publication, if an electronic version is available for free via the publisher, or
- within six months of the publication in any other case (12 months for social sciences and humanities).

<u>Formalities:</u>

- The publication must display the EU emblem (appropriate prominence). Approval by the Agency is not needed.
- It must include the following text: *"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618"*.
- It must indicate that it reflects only the author's view and that the Agency is not responsible for any use that may be made of the information it contains.

The beneficiary must still protect the results (Art. 27 GA) and meet its confidentiality obligations and obligations to protect personal data (Art. 36, 39 GA)

The breach of any of these obligations may lead to a reduction of the grant or other measures.

Another Party's unpublished results or background may only be disseminated with prior written approval.

5 Ethical aspects

Ethical aspects of ORCHESTRA will be analysed in the Ethics, Security, and Gender Balance Plan (D1.3).

6 Timeline – Date Management Updates

The DMP is a "living document". This means, that the DMP will be updated throughout the duration of the project. The updates are needed whenever significant changes arise. These changes might compromise "new data, changes in consortium policies (e.g., new innovation potential, decision to file for a patent)."[51]

Due to ORCHESTRA's project duration of 36 months and the expected regular creation and flow of new data, IKEM will update the DMP in M8, M14, M20, M26, M32, and M36. To this end, the Data Management Questionnaire in Annex 1 will be circulated regularly.

Table 3: DMP - Updates

Updates (e.g., new data, new innovation potential, copyright actions)	Project month:
1st update	M8
2nd update	M14
3rd update	M20
4th update	M26
5th update	M32
6th update	M36

[51] European Commission, "H2020 – Online Manual, Data Management" <https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm>.

7 Conclusions

The DMP contributes to the goal of making research data findable, accessible, interoperable, and re-usable by establishing necessary management steps. The beneficiaries may refer to the DMP in case that organisational or legal question in regard to the handling of research data arise.

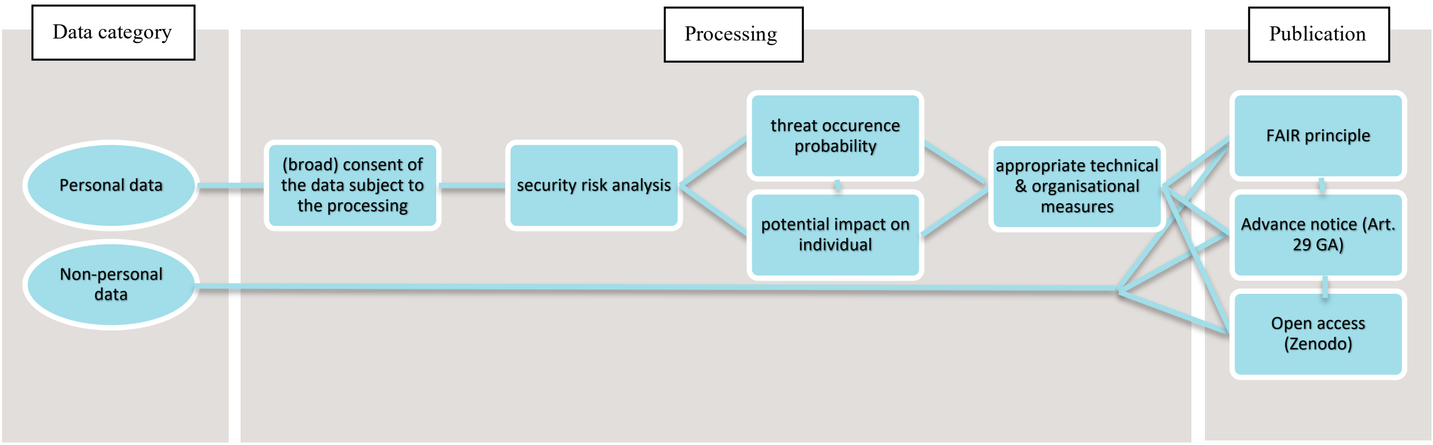
The DMP is a living document and will be updated regularly with new information in regard to the data summary and the implementation of the FAIR principle. Different requirements for the storage of the research data during the implementation of the project and afterwards have been defined.

During the implementation of ORCHESTRA a suitable development platform will be used for the code development. Moreover, sensitive data collected and processed by the beneficiaries will initially be secured locally according to the data protection and security policy of the respective beneficiary. In case that sharing features will be necessary, the DMP will include additional solutions.

After the project has finished, relevant research data generated, processed, or analysed in Orchestra will be inserted in Zenodo, as practical online service, which helps to guarantee the accessibility of the research data.

Moreover, the open access obligation covers all data (and associated metadata) generated in the course of the action or reused digitally. However, in some cases reasons not to publish data might be applicable. Those reasons will be included in the DMP.

The following graph provides an illustrated summary on what to look out for regarding data categories, processing steps, and publication activities:


Data category
Processing
Publication
Personal data
Non-personal data
(broad) consent of the data subject to the processing
security risk analysis
threat occurence probability
potential impact on individual
appropriate technical & organisational measures
FAIR principle
Advance notice (Art. 29 GA)
Open access (Zenodo)

The findings are relevant with respect to the following objectives of the ORCHESTRA project:

- *(O3) Support MTME realisation and deployments, through provisions of tools, models and guidelines.* The DMP implements the principle of FAIR data for project results, which helps further realisation and deployment.
- *(O5) Maximise outreach and uptake of project results.* The implementation of the DMP fosters the outreach of the data generated, processed and analysed within ORCHESTRA.

8 References

8.1 Primary Sources

EU primary law

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

EU case law

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH (C-210/16) [2018], CJEU, ECLI:EU:C:2018:388.

EU secondary law

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) [2016] OJ L 119.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L 151/15.

8.2 Secondary sources

Articles

Carroll, "Sharing Research Data and Intellectual Property Law: A Primer", available at: https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.1002235#references [2015].

Books

Paal/Pauly (ed.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3rd edition, 2021.

Wolff/Brinck (ed.), BeckOK Datenschutzrecht, 37th edition, 2021.

Websites

Cornell University, "Introduction to intellectual property rights in data management", available at: https://data.research.cornell.edu/content/intellectual-property, accessed 12.10.2021.

Creative Commons Organisation, creativecommons.org.

DOI Foundation, International DOI Foundation Handbook, available at: https://www.doi.org/hb.html, last accessed 20.09.2021.

European Commission, “Horizon 2020 Online Manual – Data management”, available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm , last accessed 20.10.2021.

European Commission, Open Research Europe, https://open-research-europe.ec.europa.eu/, last accessed 20.10.2021.

Zenodo, https://www.zenodo.org/, last accessed 20.10.2021.

Others

Horizon 2020 Annotated Model Grant Agreement

EDPS, “Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725“.

ENISA, “Cybersecurity Certification: Candidate EUCC Scheme V1.1.1” [2021].

ENISA, “Guidelines for SMEs on the security of personal data processing” [2016].

European Data Protection Board (EDPB), “Guidelines 05/2020 on consent under Regulation 2016/679”, 05/2020.

Rat für Sozial- und Wirtschaftsdaten (RatSWD), „Handreichung Datenschutz“, 2. Edition, 2020.

9 Annexes

9.1 Annex 1: Data Management Questionnaire

Data Management Questionnaire (M6)

The aim of this questionnaire is to get an overview of the data collection and processing in the ORCHESTRA project and to adapt the data management accordingly. For this purpose, we ask you to provide the information on data you possess at the current status of the project or information that you can already provide on future data activities.
Your answers will be used to complement the Data Management Plan (DMP). The DMP is a living document. It will be updated continuously during the project. New insights into data collection and processing can therefore be provided at later points in time. Thus, if you do not know the answer to a question yet, feel free to leave it open.

1. DATA SUMMARY

1.1 What is the purpose of the data collection/generation and its relation to the objectives of the ORCHESTRA project?

1.2 What is the intended use of data which you've collected? Is it pertaining to research work or any other form of external activites?

1.3 What types and formats of data will you generate/collect?

1.4 Will you generate/collect any personal data, i.e. data relating to an identified or identifiable natural person (e.g., identifying characteristics such as name, address and date of birth, external characteristics (gender, eye colour, height and weight), but also internal characteristics (opinions, convictions, wishes etc.), communication and relationship)?

1.5 Will you re-use any existing data and how?

1.6 What is the origin of the data (e.g. interviews, audio recording, video recording, transcript…)?

1.7 What is the expected size of the data?

1.8 To whom might it be useful (within and outside of ORCHESTRA)?

2. FAIR DATA

2.1 Are you intending to use standard identification mechanisms to make the data you produce or use in the project discoverable with metadata, identifiable and locatable (e.g. persistent and unique identifiers such as Digital Object Identifiers)? If yes, how?

2.3 What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

2.4 Do you believe an embargo will be needed for specific data? If yes, for which data, for which reasons (i.e. time to publish or seek patents) and for what period?

2.5 Will data produced or used in the project be useable by third parties?

2.7 What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?

2.8 Will you be using standard vocabularies for all data types present in your data set, to allow inter-disciplinary interoperability? In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?

2.9 Is specific software needed to access the data included (e.g. Word; Excel; PDF-reader, data analysis tools…)?

2.10 In exceptional cases, where the achievement of the ORCHESTRA project's main objective (as described in Annex 1 to the Grant Agreement) would be jeopardized, specific parts of the research data do not have to be published under open access conditions (Article 29.3 GA). The Data Management Plan must contain the reasons for not giving access. At the current state of your research, do you see any reasons for data not to be published under open access conditions?

Members of the ORCHESTRA consortium

ITS Norway c/o Tekna – Teknisk-naturvitenskapelig forening Postboks 2312 Solli NO-0201 Oslo Norway its-norway.no	**Project Coordinator:** Runar Søråsen runar.sorasen@its-norway.no **Dissemination Manager:** Jenny Simonsen jenny.simonsen@its-norway.no
SINTEF AS NO-7465 Trondheim Norway www.sintef.com	**Technical Manager:** Marit Natvig Marit.K.Natvig@sintef.no
Technische Universiteit Delft Stevinweg 1 2628 CN Delft The Netherlands	**Evaluation Manager:** Alexei Sharpanskykh O.A.Sharpanskykh@tudelft.nl
ROSAS Center Fribourg Passage de Cardinal 13B Halle bleue CH-1700 Fribourg Switzerland info@rosas.center	**Contact:** Lucio Truaisch lucio.truaisch@rosas.center
CERTX AG Route de l'Ancienne Papeterie 106 CH-1723 Marly Switzerland	**Contact:** Samuel Rieder samuel.rieder@certx.com
Institut Fur Klimaschutz Energie Und Mobilitat-Recht, Okonomie Und Politik Ev (IKEM) Magazinstraße 15-16 10179 Berlin Germany	**Data Manager / Legal, Privacy and Policy Issues Officer (LEPPI) officer:** Anne Freiberger anne.freiberger@ikem.de
IOTA Foundation c/o Nextland Straßburger Straße 55 10405 Berlin Germany	**Contact:** Michele Nati michele@iota.org Siddhant Ghongadi siddhant.ghongadi@iota.org
Societa Per Azioni Esercizi Aeroportuali Sea (SEA) Presso Aeroporto Linate 20090 Segrate MI Italy	**Contact:** Massimo Corradi massimo.corradi@seamilano.eu

deepblue consulting & research	**Deep Blue Srl** Via Ennio Quirino Visconti, 8 00193 Roma Italy	**Innovation Manager:** Alessandra Tedeschi alessandra.tedeschi@dblue.it
RÉPUBLIQUE FRANÇAISE Cerema	**Cerema** 25 Avenue François Mitterrand 69500 Bron France	**Contact:** Sylvain Belloche Sylvain.Belloche@cerema.fr
FS TECHNOLOGY GRUPPO FERROVIE DELLO STATO ITALIANE	**FSTechnology SpA** Piazza della Croce Rossa, 1 00161 Roma RM Italy	**Contact:** Jessica Bonanno jessica.bonanno@it.ey.com
Information Sharing Company	**Information Sharing Company Srl (ISC)** Via di Tor Pagnotta, 94/95 00143 Roma Italy	**Contact:** Antonio Martino a.martino@gruppoisc.com
APPLIED AUTONOMY	**Applied Autonomy AS** Kirkegardsveien 45 NO-3601 Kongsberg Norway	**Contact:** Olav Madland olav.madland@appliedautonomy.no
HERØYA INDUSTRIPARK www.heroya-industripark.no	**Herøya Industripark AS** Hydrovegen 55 NO-3936 Porsgrunn Norway	**Contact:** Tone Rabe tone.rabe@hipark.no
enav	**ENAV SpA** Via Salaria, 716 00138 Roma Italy	**Contact:** Patrizia Criscuolo Patrizia.Criscuolo@technosky.it
Statens vegvesen Norwegian Public Roads Administration	**Statens vegvesen** Rynsengfaret 6A NO-0667 Oslo Norway	**Contact:** Elisabeth Skuggevik elisabeth.skuggevik@vegvesen.no