IW-NET

Innovation-driven Collaborative European Inland Waterways Transport Network

D6.6 – Innovation and Data Management Initial

Lead Beneficiary: INLE

Delivery Date: 31/10/2020

Dissemination Level: Public

Type: Report

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 861377.

Document Information

Title:	Innovation-driven Collaborative European Inland Waterways Transport Network
Acronym:	IW-NET
Call:	H2020-MG-2019-TwoStages
Type of Action:	RIA
Grant Number:	861377
Start date:	01 May 2020
Duration:	36 Months
URL	www.iw-net.eu

Deliverable

Title	D6.6 – Innovation and Data Management Initial
Work Package	WP 6: Project Management
Dissemination Level	Public
Delivery Date	31/10/2020
Lead Beneficiary	INLE
Lead Author	Zisis Palaskas (INLE)

Document History

Version	Date	Modifications	Contributors
1.0	20/09/2020	First Draft	Zisis Palaskas (INLE)
1.1	25/09/2020	Links to other Deliverables, minor modifications	Patrick Specht (ISL)
1.2	28/09/2020	Minor modifications	Wiebke Duhme (ISL)
1.3	06/10/2020	Feedback	Lisa-Maria Putz (FHOO)
1.4	09/10/2020	Final edits	Jenny Rainbird (INLE)

Executive Summary

IW-NET "Innovation-driven Collaborative European Inland Waterways Transport Network" is an EU Funded research project, under the “Moving freight by Water: Sustainable Infrastructure and Innovative Vessels” topic of the Horizon 2020 research and innovation programme, grant agreement No 861377.

The IW-NET Data Management Plan (IW-NET DMP) aims to provide a detailed description of all data related activities, including data definitions, generation and capture related to the IW-NET technology development and testing in the IW-NET Application Scenarios (WP4), as well as all external data that will be used to run the IW-NET platform.

The purpose of the IW-NET DMP is to:

- comply with the Horizon 2020 Open Data Access Guidelines.
- embed the IW-NET project in the EU policy on data management which is increasingly geared towards providing open access to data funded by the EU.
- ensure that all possible data is accessible to other researchers, helping to streamline the research process from start to finish.
- enable the verification of the research results and the sustainable storage of data in the IW-NET knowledge observatory.

According to the "Guidelines on Data Management in Horizon 2020", the Data Management Plan aims to produce data so that researchers may benefit by their use directly, and / or to apply their methods based on data generated by research in Horizon 2020. The Data Management Plan governs all data generated and collected during the project, the standards that will be used, how the research data will be preserved and what parts of the datasets will be shared for verification or reuse.

Such data are typically stored in specified IW-NET architecture IT cloud infrastructure i.e. the Big Data stores and the IW-NET Knowledge Graphs. The Data Management approach covers the complete data life cycles, also including data that will be used for the IW-NET business model simulations to analyse the IWT models and their characteristics.

The IW-NET Data Management Plan is a public document, made to evolve through the IW-NET project lifespan, capable to capture and reflect evolution in the form of dataset updates and/or changes in Consortium policies.

Disclaimer

List of Abbreviations

Abbreviation	Description
AB	Advisory Board
AI	Artificial Intelligence
CA	Consortium Agreement
CoP	Council of Partners
DML	Data Management Lead
DMP	Data Management Plan
DoA	Description of Action
EC	European Commission
FAIR	Findable, Accessible, Interoperable and Reusable data
GA	Grant Agreement
GDPR	General Data Protection Regulation
IDCB	Innovation Dissemination & Commercialisation Board
IL	Innovation Lead
IoT	Internet of Things
INEA	Innovation and Networks Executive Agency
IPR	Intellectual Property Rights
IWGO	IWT Greening Officer
IWT	Inland Waterway Transport
MDM	Master Data Management
MMO	Multimodality and Modal Shift Officer
MS	Milestone
MSL	Member States Liaison Lead
ORD	Open Research Data Pilot
PM	Project Manager
PO	Project Officer
PST	Project Steering Team
QAEM	Quality Assurance and Ethics Compliance Manager
TEN-T	Trans-European Transport Network
REA	Research Executive Agency, European Commission
TL	Task Leader
TM	Technical Manager
WP	Work Package
WPL	Work Package Leader

Table of Contents

Tables

Figures

1 Introduction

1.1 Context

The IW-NET Data Management Plan (DMP) activity in the context of the Horizon 2020 initiatives seeks to accelerate research by making data *Findable, Accessible, Interoperable, Reusable* (FAIR), and effectively managed. In IW-NET, the DMP enables knowledge discovery and supports innovation, by data and knowledge integration and reuse. The main purpose of the IW-NET Data Management Plan (DMP) is to provide a single point of reference that governs the data received, generated and managed by IW-NET as well as any data sources to be made available to the public. Additionally, the DMP aims to detail the method and the relevant actions required for the preservation, enhancement and further exploitation of the data collected during the project.

Data in IW-NET is considered to play a crucial role, being essential in the digitalisation strategy of the project, helping to discover new Business Models in IWT, based on visibility due to track and trace data flows, that will be used for decision support and will be consumed at different stages, by the simulation models, and the algorithms related to Data Analytics, Data Mining and the application of Artificial Intelligence (AI) approaches in producing knowledge. Hence, IW-NET requires an efficient data management approach, as data are at the centre of all IW-NET innovations. Nevertheless, data sharing in the open domain can be restricted as a legitimate reason to protect results that can reasonably be expected to be commercially or industrially exploited. Strategies to limit such restrictions include various acts, such as anonymizing or aggregating data, or even publishing selected datasets.

To this end, the IW-NET DMP is the domain where monitored data will be constantly cleansed, integrated, and further enhanced and curated to ensure their value offered for the IW-NET scenarios, and also the IW-NET their suitability to be reused in Open Research. The DMP establishes the processes, the rules and the context, guiding the data management activities of the project, in all data creation and consumption tasks performed by the project participants. The main beneficiaries of it are the partners responsible for data collection and data exploitation in the Application Scenarios cases covering the handling of data during and after the project, the nature of data that are collected and processed, the specific methodologies that are applied and the intended way that data is shared and preserved.

IW-NET is part of the Open Research Data Pilot. The Open Research Data Pilot (ORD pilot) is an H2020 EU Pilot Programme aiming to improve and to maximise the access and the re-use of research data generated by Horizon 2020 projects. Such an initiative is required to balance between openness on one side, and protection on the other side, considering the commercialization aspects the Intellectual Property Rights (IPR), the privacy concerns and security. The ORD pilot is primarily about the data needed to validate the results presented in scientific publications. According to the "Guidelines on Data Management in Horizon 2020", a DMP has the aim to produce data so that researchers may benefit by their use directly, and / or to apply their methods based on data generated by Research in Horizon 2020 that are:

- Findable
- Accessible
- Interoperable to specific quality standards
- and to create data sets enabling reproducible and verifiable research results by others (Reusable).

In the above context, the main drivers for setting up the IW-NET DMP are:

- to comply with the Horizon 2020 Open Data Access Guidelines[1].

- to embed the IW-NET project in the EU policy on data management which is increasingly geared towards providing open access to data that is gathered with funds from the EU.
- to ensure that data that is to be part of the ODPR initiative are accessible to other researchers, helping to streamline the research process from start to finish.

The IW-NET consortium strongly believes in the concepts of open science, and in the benefits that the European innovation ecosystem and economy can draw from allowing the reuse of data at a larger scale. This document produced within the scope of the "Innovation and Data Management" task of IW-NET (T6.3), integrates the initial version of the DMP, in line with the H2020 guidelines for data management plan creation[1]. Therefore, the IW-NET DMP describes the data management life cycle for the data collected, processed, generated. Conforming to the FAIR principles and directions the IW-NET DMP considers:

- the handling of research data during and after the end of the project
- the data generated, collected, processed mainly coming from the IW-NET Application Scenarios (WP4)
- the method to applied in the data lifecycle and the related standards for supply chain and transportation data.
- the definition of data sets that are shared/made open access and
- the methods to be used for data curation and preservation after the end of the project.

The IW-NET DMP requirements are defined within the context of the Grant Agreement (GA) (Table 1)

Table 1: Deliverable's Adherence to IW-NET Objectives and Work Plan

IW-NET GA requirements	Section(s) of present deliverable addressing IW-NET GA	Description
Article 29 Dissemination of Results – Open Access – Visibility of EU Funding, Article 29.3, Open Access to Research Data[2]	Section 2.1	The IW-NET Data Management Plan (DMP) is defined within the context of the Grant Agreement. The full text of this deliverable is addressing the "Open Access to Research Data" Objective. The document describes the level of confidentiality of different data sets, defines data governance and privacy principles, and the strategy towards contributing to the Open Research Data Pilot.
ST6.3.1 Innovation Management (INLE):. This task, led by INLE with support from all partners, will determine how innovation and research data will be handled during the project and describe what data will be collected, processed or generated. Furthermore, the Innovation Manager regulates what methodologies and standards will be followed, whether and how this data will be shared and/ or made open, and how it will be curated and preserved, with emphasis on ensuring GDPR compliance. Innovation Management is strongly collaborating with the Advisory Board and the Greening manager (IGM), all innovation management reports integrate the input of both AB and the IGM.		

[1] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[2] See Annex-I of this document for References to GA.

ST6.3.2 Data Management **(INLE): Development of the DMP is aligning with the Open Research Data Pilot (ORDP) implementing FAIR processes. It is related to the information and the types of data that the project will generate and collect, the standards that will be used to represent the data during the project and how partners might exploit the data resulting from the project. The DMP will set robust management procedures that will protect personal data collected as a result of project activities, as well as client owned data, from unauthorised use or sharing, also supporting GDPR compliance.**		
D6.6 : Innovation and data management Initial [6]. Initial DMP (Data Management Plan)	Represented in this document.	Data Management Plan is intended to be a single point of reference for to govern data production, collection, use and provision of data.
D6.7 : Innovation and data management Final [36]. Final version of the DMP and Innovation management plan.	Report will elaborate on all sections of this deliverable. D6.7 is due M36.	

1.2 Approach

The IW-NET DMP integrates the Living Lab Application Scenarios data, and the data sets to be developed in research and technology development tasks (WP1-WP3), e.g. the data relating to algorithms and 'recipes' developed and stored in the IW-NET Knowledge Graphs and consumed by Big Data Analytics. The data is prepared for ORDP purposes using tools such as the Digital Curation Centre (DCC) DMP online tool[3], which is based on the DMP template matching the demands the Guidelines on FAIR Data Management in Horizon 2020(EU, 2016).

After this deliverable release in M6, there will follow focused and specific per WP discussions about the IW-NET created data sets in the consortium, including the decisions, on information confidentiality, the confidentiality levels of the different datasets used in the IW-NET Living Lab Application Scenarios.

One of the main topics for discussions about data management in the consortium, are decisions on which data will become part of an open data scheme and will become available for the Open Research Data Pilot (ORDP) initiative. In order to conform with governance rules and GDPR, mechanisms to protect identities and sensitive information will be enforced as a part of the data management actions. IW-NET is publishing no confidential data and results under Open Access, regarding all scientific publications produced along the project lifecycle. The IW-NET Open Access strategy relates to the EU "Open" paradigm for publishing project results, which foresees two possible ways of accessing the published results: *Gold Open Access*, which grants immediate access through a publisher, and *Green Open Access*.

At this early stage, a generic approach is considered, where, during the project data lifecycle, internally, the data will be treated in an organized manner in a data repository to be setup and will be functioning as a master data management facility.

[3] https://dmponline.dcc.ac.uk/

Data governance mechanisms (also, see Annex II for GDPR) will be established. These mechanisms will be active throughout the project, applying to all activities including data deployment and the application of various algorithms developed mainly in WP1 and tested in WP4 in the IW-NET Living Lab Application Scenarios, including Data Mining and Machine Learning.

IW-NET Data Management ensures that data collection and processing are to be carried out according to EU and national legislation (references [1], [2]). For this, DMP relates to and respects the *Ethics and Security* practices to be globally followed within IW-NET, which mandate that all data collection and processing is carried according to EU and National Legislation, as defined in the GA, Part B, Section 5, "Ethics and Security", and the Ethics Procedures in IW-NET (Deliverable D7.1). The Ethics and Security practices consider the relevant issues concerning Ethics, determining the framework, the rules and the availability of data, and all possible measures to ensure data are properly anonymized respecting privacy, and to ensure the open data strategy does not violate the terms and guidelines of Related EU policies.

Last and most importantly, the IW-NET Data Management incorporates the Consortium agreements on data management and is consistent with exploitation and IPR and Innovation protection, and the registered patents.

All partners' obligations and rights related to Data management will have been covered via NDAs, as necessary to protect sensitive data, linked to exploitable results to guarantee the marketing and commercial exploitation potential.

2 IW-NET Data Management Plan

2.1 IW-NET and the Open Research Data Pilot

Open Access (OA, see Figure 1) is about providing online access to 'scientific information', free of charge to the end-user and in a reusable manner. In the context of research and innovation, 'scientific information' refers to research data (data underlying publications, curated data and/or raw data).

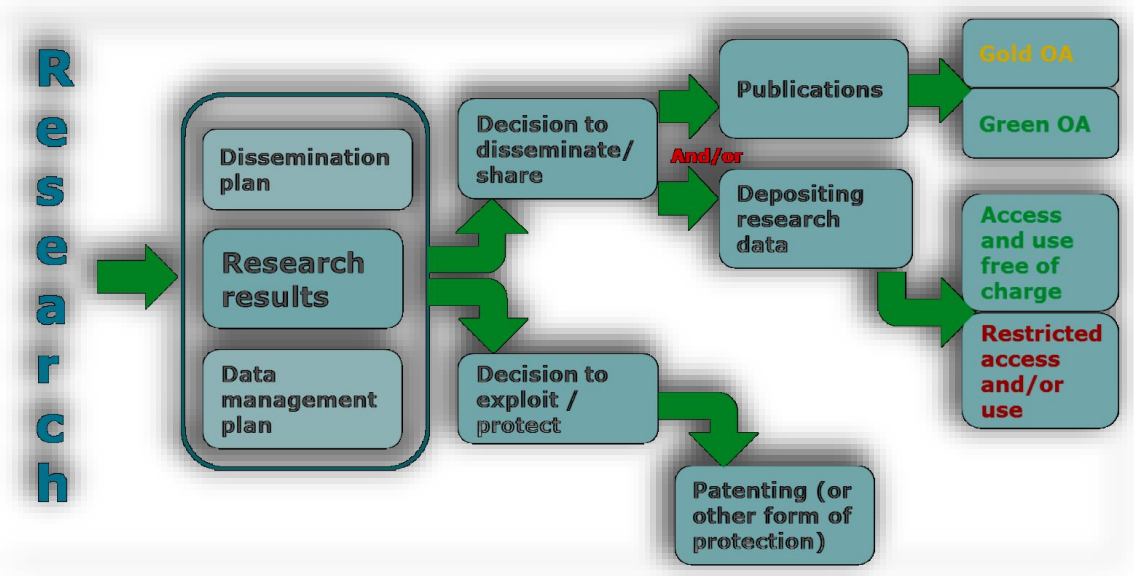

Figure 1: Open Access to Scientific Publications and Data for Dissemination and Exploitation

It is understood that 'Open Access' does not imply an obligation in IW-NET to publish its research results in open ('Green' and 'Gold' Open Access schemes as described in [3]). Publication of data within IW-NET will be carried out on a voluntary basis by the stakeholders, and in full alignment with the Intellectual Property (IP) and the patenting IW-NET activities.

The DMP of IW-NET is considering the above and aims to contribute data to the Open Research Pilot (ORDP). Data sets which are candidates for sharing will have been checked to ensure that:

- They are not confidential, that they do not include personal or commercially sensitive information according to GDPR (Annex II).
- That permission from the relevant stakeholders and/or data subjects has been obtained.
- That sharing the data does not damage exploitation or IP protection prospects.

Accordingly, datasets in IW-NET originate from the stakeholders in the Application Scenarios of the IW-NET Living Lab and the researchers in the technical work-packages, reviewed by the appointed *Data Protection Officer* (DPO) and approved before becoming candidates for contribution to the open research pilot. In that sense before publishing the data, the data stakeholders will have agreed on the possible licencing scheme if this data is made available outside the consortium, for example creative commons or public domain.

Following the internal approval, IW-NET then makes the dataset available as a link to an internally accessible data space. Where appropriate, data are embargoed to support IP protection or the exploitation timeline for its release.

2.2 Data Lifecycle

The IW-NET DMPs detail what parts of the datasets are shared for verification or reuse. The expected types of research data that will be collected or generated along the project lie in the following categories:

- Supply Chain Data from the Application Scenarios of the IW-NET Living Lab;
- Simulation Data, using the Living Lab data,
- Data extensions based on included Open Data (i.e. destinations, routes and connections), geographical data, , weather observations and predictions,
- Big Data coming from sensors, raw / and or integrated in Big Data stores (e.g. NoSQL databases), and the Knowledge Graph,
- Terminology and metadata describing information exchanges and data flows (i.e. UN/CEFACT, GS1),
- Organised semantic data, i.e. ontologies or Knowledge Graphs.

The IW-NET DMP covers the complete data life cycle (Figure 2) for all data generated or imported to IW-NET. DMPs describe the types of data that are generated or collected during the project, the standards used, and how this data will be managed, stored, enhanced, exploited and disseminated.

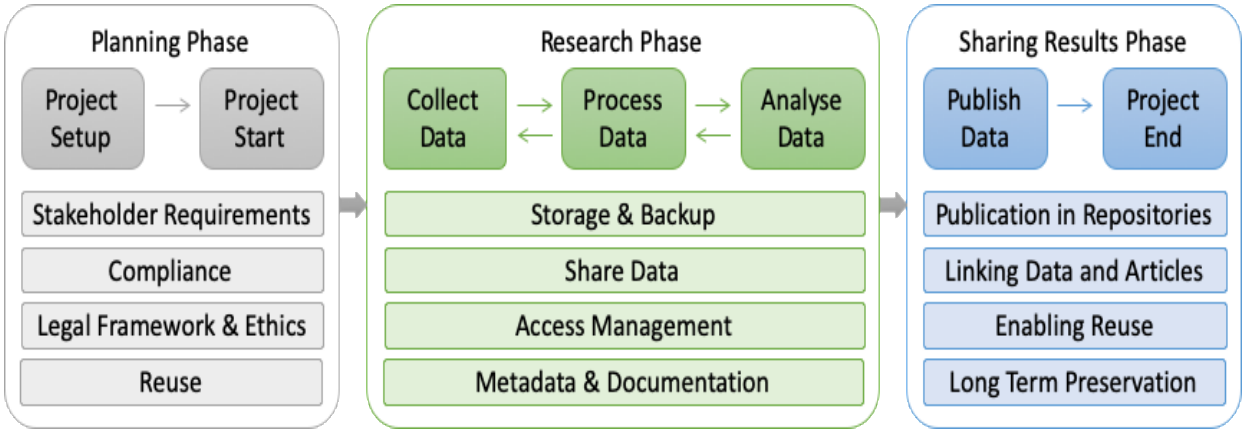

Figure 2: IW-NET Research Data Lifecycle

The IW-NET research data lifecycle can be seen as similar to the research lifecycle proposed and applied in DTU[4], which has been adapted to the IW-NET project scope and objectives, research directions, and partnerships/stakeholders, also the exploitation needs and the drive to commercialize and patent per case the results, involving the following steps:

Planning Phase

(a) The planning and the project start involves the setup of the framework for research data collection and all the project related activities, performed mainly in WP4, WP6 and the capacity building and exploitation tasks in WP5.

- The stakeholder's requirements with respect to the research data will be defined.
- At this stage, compliance with the ORDP guidelines is achieved,
- Data – Protection and Policy related activities, including the ethics considerations are defined with the project setup and start phase and are monitored continuously as the project progresses.
- Reuse is supported via the alignment to the IW-NET project objectives and the context of all research implemented. For the Knowledge Graphs, and the specific requirements in the IW-NET Application Scenarios, using Data Mining and Machine learning techniques, a scoping frame for the reuse of the project results, and research data will be set. Supporting activities also relate to the overall data standardization actions performed in WP1, especially the ones relating to the data dictionary and semantics and to IoT and blockchain development.

Research Phase

(a) Collection: Data are created in the Living Lab and in tasks that develop and demonstrate strategies and business model innovation. In the data acquisition phase, the research infrastructure collects raw data from registered sources to be stored and made accessible within the infrastructure. The data collection phase supports collecting data from back-end operational systems as well as data from IoT data flows. Data are also collected from external systems and data repositories. These data are generally assumed to be non-reproducible, provenance (particularly data source and timestamp) is considered essential. As the info includes data from RT data streams additional processing is considered, including e.g. sampling, filtering and processing, including also processes for anonymisation.

(b) Data Processing: refers to the aggregation of data, integration, cleansing, transforming and modelling, and finally, the performance of analyses using this data. Hence, the data is manipulated, leading to data derivations and transformations, useful to scientific results, and further processing.

(c) Data Analysis: involves the use of number of techniques, including statistical analysis, data mining, machine learning as well as transformations from relational data models to graph data models and the Knowledge Graphs. IW-NET performs modelling and simulation, and provides different visualization mechanisms, using the developed analytics algorithms and 'recipes' (WP1), and the cloud-based infrastructure. Further, data is consumed by the Application Scenarios in the Living Lab, which involve e.g. certain use cases that implement collaboration and are displayed in management dashboards for analytics.

- IW-NET during the research organizes data internally in a reserved area; Sharing of data towards the end of the project via the ORDP related facilities for the data sets that will be identified as sharable to the Research Community.
- Access to the data and Management infrastructure will be facilitated via a web-based facility, using all possible and relevant authorisation and authentication means. Further all data

[4] https://www.dtu.dk/english/research/research-at-dtu/research-data-management

publishing in external repositories, also considers access rights management, authentication, and authorization as implemented by the repository facilitators.
- Data sets will be documented to comply to the ORDP and to the DMP requirements and EU supported guidelines.

Results Sharing Phase

- Data Publishing which leads to and concludes with the project finalization, is promoting the discovery of the data used during the project for the research. In selected cases in IW-NET, it refers to the publishing of considerable size data sets used in the IW-NET Living Lab and the Application Scenarios. This data is initially housed in and confined within project developed resources. Selected data sets based on the IW-NET governance of data will be distributed to the Open Access Platform. The data publishing in repositories leading to the ORDP involves the use of open repositories as the OpenAIRE and Zenodo[5].
- Data Publishing includes the support of search tools for data sets discovery after their publishing based on metadata or semantics.
- Data reuse is enabled within the project as certain data is archived. For full data set access, the Big Data IW-NET infrastructure has the capacity to hold exceedingly large volumes of structured data in the IW-NET scalable infrastructure solution.
- Some data cease to be useful (e.g. raw data streams of sensors) as they will be transformed in some other value adding form or become inactive and obsolete and are destroyed. For long-term preservation of specific data sets, IW-NET considers external repositories as described above.

2.3 Data Governance and the FAIR[6] Data Principles

Data Governance deals with data usage, consumption and policies. Complying to the H2020 overall strategy for research data follows the FAIR data principles, all research data should be Findable, Accessible, Interoperable and Reusable (FAIR). This means that data should be:

- identified in a persistent manner using conventions described using sufficiently rich meta-data;
- stored in such a way that they can be accessed;
- structured in such a way that they can be combined with other data sets;
- licensed or have terms-of-use that define how they can be used.

The IW-NET Data Governance classifies the IW-NET data assets based on their usage in the Living Lab Application Scenarios and their criticality. Based on this, necessary policies around the usage and consumption of such assets can be defined. Further, Governance focuses on the data quality as IW-NET is highly dependent on data and the quality of the accessed and used information. Hence, principal governance concerns are data quality and security. Data governance in IW-NET ensures proper Data Management of important and sensitive data including information related to the Application Scenarios designs. As such, they will be appropriately managed, anonymized, encrypted and sanitized, whereas risks which should arise upon their access by third parties will be handled accordingly. A Governance strategy helps IW-NET make the best value of all data produced within the Living Lab (WP4), to leverage opportunities coming from prediction, risks management and sharing, collaboration and innovations in business models.

Thus, Data and Information Governance in IW-NET within the scope of the DMP, serves two primary purposes:

(a) provide a mechanism for controlling changes related to the data, data processes, and the data architecture of IW-NET, and more specifically to the connectivity, storage and data/information

[5] https://www.openaire.eu/ , https://zenodo.org/

[6] Mark D. Wilkinson et al. Comment: The FAIR Guiding Principles for scientific data management and stewardship

sharing IW-NET architecture components. Governance is exercised and monitored by the appointed Data Protection Officer, reporting to the IW-NET Council of Partners. All IW-NET partners are represented and have full control of how IW-NET data is managed, accessed, stored, and disseminated via the Open Data Access Initiative. Further, all changes to the data architecture and the data sets of the DMP generated by the Application Scenarios, the business model simulations and certainly while developing and testing the Innovative IW-NET Applications (WP1, WP2 and WP3), shall have to receive the approval of the appointed Data Protection Officer, before being disseminated;

(b) provide a central point of communication about all things related to the data, data processes, and data architecture of IW-NET. This includes the data definitions for information exchanges developed in WP1 and the data dictionary, the Data Management facility to track all data types and changes, any data compliance requirements in supply chain, including reporting to administrations and data related policies within EU from regulatory agencies, finally, data quality procedures and metrics.

2.4 Data Sets Definition Methodology

Datasets are collections of data corresponding to the content of a single database table, or a single statistical data matrix, where every column of the table represents a variable, and each row corresponds to a given member of the data set in question. The data set lists values for each of the variables, for each member of the data set. The data set may comprise data for one or more members, corresponding to the number of rows. The term data set may also be used more loosely, to refer to the data in a collection of closely related tables, corresponding to the IW-NET Application Scenarios of WP4 (the Living Lab).

Conforming to the EU guidelines (see [1] and [2]), IW-NET provides information for every dataset submitted to the ORDP in a disciplined manner, following a well-structured method for defining and creating data sets, and for managing the data in the data sets. The DMP is aligned with the European Commission Guidelines for Horizon 2020 for research projects (ref. [2] and [3]) and presents in a structured manner the meta-information captured for all datasets produced in the project. Consequently, the IW-NET Initial DMP addresses the following points on a dataset by dataset basis, as presented in the following paragraphs.

The data sets definition compliance to FAIR implies that the following detailed FAIR principles hold [7]:

FINDABLE:

F1. (meta)data are assigned a globally unique and eternally persistent identifier.
F2. data are described with rich metadata.
F3. (meta)data are registered or indexed in a searchable resource.
F4. Metadata specify the data identifier.

ACCESSIBLE:

A1. (meta)data are retrievable by their identifier using a standardized communications protocol.
    A1.1. The protocol is open, free, and universally implementable.
    A1.2. the protocol allows for authentication and authorization, where necessary.
A2. metadata are accessible, even when the data are no longer available.

[7] https://www.force11.org/fairprinciples

INTEROPERABLE:

I1. (meta)data use a formal, accessible, shared, and broadly applicable scheme for knowledge representation.

I2. (meta)data use vocabularies that follow FAIR principles.

I3. (meta)data include qualified references to other (meta)data.

RE-USABLE:

R1. meta(data) have a plurality of accurate and relevant attributes.

R1.1. (meta)data are released with a clear and accessible data usage license.

R1.2. (meta)data are associated with their provenance.

R1.3. (meta)data meet domain-relevant community standards.

2.4.1 Data Set Reference and Name

The teams working on the IW-NET Application Scenarios development will identify the required set of data that is useful for enabling the successful outcome of the project within a series of interviews with different industry partners. Each Application Scenario provides one or more use cases, thus the data sets required for their implementation will be different in nature. Standard naming approach will be followed in the application scenarios, using UN/CEFACT, GS1 and other relevant standards naming schemes, which are currently developing also in activities of the DTLF[8].

2.4.2 Data Set Description

Every data set that are generated or collected will be described with respect to its origin (in case it is collected), nature and scale and to whom it could be useful, and whether it underpins a scientific publication. This includes information on the existence (or not) of similar data and the possibilities for integration and reuse.

Standards and Metadata

Where possible references to existing standards of the discipline will be made. If these do not exist, metadata will provide an extensive outline on how and what metadata is created. The IW-NET project is related to different sets of data, i.e. not only standardized transportation and logistics data, but also geospatial data, nautical data on inland waterways and raw data related to IoT. Therefore, several standards exist beyond the ones covered by standards like UN/CEFACT, GS1 etc., making imperative the need to provide an extended metamodel covering data interoperability, adaptability and dynamicity on each of the specific sub-domain. Raw data generated or used by the project must contain at least the following metadata, derived from the metadata available from each data source:

- Any URL for automated retrieval of the data, contact and email of administrator/owner
- Description, internal or external
- A timestamp at which the data is created
- Information about the entity (organization, individual, etc.) supplying the data
- Information about any licensing terms that may apply to the data and visibility
- Sources and version
- This subsection presents the standards that are considered for the project to produce aligned data structures and data exchange services

[8] https://www.dtlf.eu/

2.5 Data Sharing

This involves the description of how data is shared, including access procedures, outlines of technical mechanisms for dissemination and necessary software and other tools for enabling re-use, and definition of whether access is widely open or restricted to specific groups. Identification of the repository where data is stored, if already existing and identified, indicating the type of repository (institutional, standard repository for the discipline, etc.). In case the dataset cannot be shared, the reasons for this should be mentioned (e.g. ethical, rules of personal data, intellectual property, commercial, privacy-related, security-related).

2.5.1 Access Procedures

The IW-NET project applies methods that emphasize good field access, extended contact and trust building with participants, and they are also sensitive to ethical concerns in doing scientific research among respondents in conflict-affected areas. Due to the sensitive nature of some of the topics that are discussed, data security is of vital importance and an important aspect to consider is who can access the data. In case where some of the datasets should not be publicly accessible to everyone, a control mechanism must be established with some of the below mentioned features:

- Authentication systems that limit real access only to authorized users.
- Procedures to monitor and evaluate, all the access requests. The user must complete a request form stating the purpose for which they intend to use the data.
- Adoption of a data transfer agreement that outlines conditions for access and use of the data.

Each time a new dataset is deposited, the consortium decides on who can access the data. Anonymised and aggregated data can be made freely available to everyone, whereas sensitive and confidential data is only accessed by specific authorized users undersigned disclosure agreements.

2.5.2 Methods for Data Sharing

Raw data or processed data that are governed by any IPRs or confidentiality issues will where possible be uploaded to a central data repository. The internal, intra-project data repository will in due time be selected, properly setup under IW-NET governance and be made available to all partners. This will have the form of a cloud-based facility and will be provided by one of the research project-partners.

An additional raw-data collection issue is the provision of data required during the Application Scenarios use cases, such as basic data required for each use-case. This kind of data are expected to be uploaded to the specific IW-NET platform demonstrator storage components either manually by the user, or in batches using the defined system interfaces.

Either way, the confidentiality and integrity of these data will be protected and guaranteed by the application of security encryption schemes that are applied matching and conforming to the non-functional requirements of the IW-NET platform.

On the other hand, there will be specific data that will be selected and curated as eligible for public distribution, disseminated through:

- Scientific papers in conferences and journals
- Interest groups created by the partners of the project
- Dissemination though the dissemination and exploitation channels of the project to attract more interested parties

Appropriate repositories will be considered for storing the results of the project and providing access to the scientific community, such as OpenAIRE[9] and Zenodo[10].

The data sharing for public access will occur in a timely fashion, i.e. data resulting from the research conducted in the project will become available towards the end of the project.

Data in this respect, will be controlled and secure, including those initially not meant to be distributed to the public either due to participant confidentiality concerns, third-party licensing or use of agreements that prohibit redistribution. For the latter kind a full analysis will be performed towards the end of the project to potentially result subsets of this the data, appropriate for the ORDP.

2.6 Data Storage, Archiving and Preservation.

IW-NET will put in place procedures for long-term preservation of the data, providing indication of how long the data should be preserved, what is its approximated end volume, what the associated costs are and how these are planned to be covered.

At the time of this first version of the DMP (D6.6), the Data Repository does not contain any data. Plans for archiving the situation as described within this report are thus preliminary and fluid. Only data that will initially be used and accessed by IW-NET will be archived and curated in the first 12 months of the project (M12 being a control Time point), including data to be produced in all technical research tasks (WP1-WP3) and in the initial steps of the Living Lab (WP4) of IW-NET.

However, based on those data, for the ORDP an immutable version of the data gathered will potentially be prepared to be made available to several researchers on request towards the later stages of the project (After M18). To ensure high-quality long-term management and maintenance of these datasets, the consortium implements GDPR compliant procedures to protect information over time.

These procedures permit a broad range of users to easily obtain, share, and properly interpret both active and archived information, and they will ensure that information is kept up to date in content and format, so they remain easily accessible and usable.

IW-NET will organize and store data internally an open access repository (as explained in section 2.5), transforming the data to knowledge assets, further disseminated for capacity building. Such data will available in different formats depending on the tools deployed, the resources available and the most appropriate way to organize the information. The raw data captured and recorded as data flows from IoT streams are stored in a Hadoop filesystem (HDFS) node, and NoSQL – Graph Database, using the standard IW-NET infrastructure developed in WP1.

According to the IW-NET DMP policies, raw, generated or meta-data from the project shall be preserved and archived. In the case of raw data collected from industrial partners in a predefined way (file format, fields, etc.) these are stored in a NoSQL database facility and or a Graph database implemented in WP1. IW-NET develops a knowledge graphs technology and the IW-NET developments for the Knowledge Repository developed in WP1. Hence, the entire storage data set is archived in the IW-NET storage facility created in WP1, at least until the end of the project. The files containing the datasets are usually versioned over time. Also, the datasets will be automatically backed up on a frequent (weekly and monthly) basis.

[9] https://www.openaire.eu/
[10] https://zenodo.org/

2.7 IW-NET Privacy Principles

Data confidentiality is an overriding concern throughout the IW-NET project and beyond, as the tools developed in IW-NET will continue to be used afterwards and even rolled-out to future applications, to this end IW-NET is (aims to be) fully GDPR compliant (see Annex II).

IW-NET partners are fully concerned, and take concrete measures, towards prohibiting to the best extent possible unauthorized access to their IW-NET-related data through both technical and legal means. This is applicable both upon IW-NET partners that collect the data as well as on partners that will be provided with access or processed data on behalf of others.

Project participants are already covered by a Consortium Agreement which encompasses Non-Disclosure clauses as well as their Contract with the EC which itself includes Special Clause 15 on the treatment of data. However, NDAs are implemented to cover future users, as well as through the implementation of security measures in their processing systems (such as the design of IW-NET nodes) aimed at a level of protection, according also to the principle of proportionality, which should be at least the same as that provided to their own confidential information.

2.7.1 Commercial Data

The exchange of information at such rate as implied by the IW-NET project invites considerations of confidentiality and trade secrets. The IW-NET platform is fed with information, for instance on employees, contractors, collaborators, clients, etc. that may be of critical importance to the partners that release them. If correlated, they may reveal business methods, pricing, payment terms or other business-sensitive information.

While data exchange is important for the project objectives to be accomplished, a lack of a duty to confidentiality would leave the information exchanged unprotected – something that by itself could challenge the Project's success because partners would hesitate to use the IW-NET community nodes to share supply chain information.

The issue of confidentiality is therefore of critical importance to the success of the IW-NET project. An obligation to confidentiality should cover in particular:

- Data exchanges undertaken in Living Lab pilot projects;
- Data transmitted through or uploaded to the IW-NET platform;
- Data exchanged (on a bilateral basis) between IW-NET partners;

It should be noted that the above duty to confidentiality does not cover only personal data. Quite on the contrary, personal information is protected under basic data protection legislation. Here it is particularly technical and other proprietary information that are placed within the scope of protection. This information may have intellectual property rights protection over it (for instance, in the event that it qualifies for copyright or patent protection), but it may well be the case that it is unprotected raw data, that however still possesses business value for the disclosing party.

The preferred means through which to protect confidential information exchanged during execution of the IW-NET project are (NDAs) and these are included in the present Consortium Agreement which has been signed by all partners. However, after the end of the research project, when results will be rolled-out to organizations which are not partners in IW-NET and therefore not covered by the present Consortium Agreement, it is essential that comprehensive NDAs are signed prior to any disclosure of information. Such agreements should be drafted by the Project Coordinator and entered whenever deemed important before confidential information exchanges.

2.7.2 Personal Data

Data collection forms part of personal data "processing", according to Article 2 of Directive 95/46 [4] (" 'processing' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"). In the IW-NET project context, collection of personal data may take place through:

(a) interaction with individuals that may provide personal information (interviews or evaluation sessions), and

(b) collection of data regarding supply-chains, including, for instance, the kind and volume of goods transported, their source and destination, and the transportation means used, evidently whenever personal information is inserted in the relevant fields.

With respect to (a), obtaining of lawful consent by the individuals concerned, for it to constitute the relevant legal basis for the processing, is imperative. Participants in interviews or other activities must be asked to sign a relevant form, for their consent to be demonstrable in writing. The form must be composed in accordance with legal requirements, i.e., among others to describe how the information is used, how the person concerned may review or amend them, etc. [11]

With respect to (b) Personal data may be shared among partners for IW-NET project purposes. According to the project's Description of Work collection is undertaken by certain project partners. The outcome of this process may be made available to others in order to execute the relevant processing. The same is the case in WP4 (the Living Lab): among all IW-NET partners participating in a Living Lab Application Scenario personal data may be made available to others for business reasons, regardless of the "point of entry" (IW-NET partner that collected the data). Consequently, data are distinguished between data of IW-NET partners that:

(a) process personal data by way of collection,

(b) process personal data by way of data transfer,

(c) do not undertake any personal data processing under the Project.

In this context, it is recommended that all IW-NET partners under points (a) and (b) above are instructed to undertake relevant data protection measures.

These may include, depending on each particular case, either collection of consent forms by the individuals concerned and/or registration with the appropriate (according to the place of establishment) Data Protection Authority and/or adherence to the IW-NET project privacy policy. It is also essential to consider that the project is being undertaken under a contract with the EC which includes Special Clause 15.

Therefore, all partners who collect personal data must inform the Research Executive Agency (REA) in writing, prior to any data being collected, that they have received favourable opinions from all the relevant ethics committees and, if applicable, the regulatory approvals of the competent national or local authorities in the countries where the research is going to be carried out. This is not necessary if parties already collect or receive such information as part of their existing business operations since it is assumed that they already comply with the relevant legal and data protection rules.

[11] The detailed procedures to guarantee informed consent are described in D7.1.

Since this may impose a significant additional burden, it is a key objective of IW-NET that systems be designed so as to limit actual or potential access to personal data to only those parties that need to access or process data, encrypting, securing or masking data so that it is not visible to parties which are not authorized, or which do not strictly require it.

Personal data shall not be transmitted to non-EU countries and consequently cloud computing infrastructure will be based in an EU country.

2.8 IPRs and Privacy Issues, IW-NET Data Protection and Privacy policy

Data access and sharing activities has been rigorously implemented in compliance with the privacy and data collection rules and regulations, as they are applied nationally and, in the EU, as well as with the H2020 rules. Raw data collected through sources external to the consortium may be available to the whole consortium or specific partners upon authorization of the owners. This kind of data are not meant to be available to the public.

Concerning the results of the project, these will have become publicly available based on the IPRs as described in the Consortium Agreement. The following describes the IW-NET Data Protection and Privacy Policy as it applies to Data created within IW-NET.

Article 1. Introduction. The Data Protection and Privacy Policy refers to EU Project [IW-NET, 861377], (the "**Project**") and applies to the project website, the document server and in general covers the data created within IW-NET project for research purposes and will have been uploaded to the IW-NET website or Public Registries:

This Personal Data Protection and Privacy Policy (the "**Policy**") aims at providing details of the processing, and related methods of use, of personal data referred to users/visitors (the "**User(s)**") of the IW-NET website that can be reached at the address [https://www.iw-net.eu] (the "**Website**"), also to data uploaded to Publicly Accessible Research Data Registries.

Users must be informed of this Privacy Policy at all personal information entry points before filling electronic forms posted on this website or sending information. Such information is given in accordance with applicable EU data protection law, the EU General Data Protection Regulation, and the EU applicable Privacy laws.

Article 2. Scope. This Policy covers the Website and the research data uploaded to EU Open Research Data Registries as described in Article 1. No other personal data processing under the Project or any other websites owned or run in any manner by the Controller or Project Partners is covered, unless specifically described in an Article of this Policy and/or within a specific IW-NET project Deliverable. All data under this Policy before being made publicly available i.e. uploaded to the Website or to the Public Registries for ORDP purposes, will have been cleansed and anonymized using all GDPR practices and policies applying to IW-NET.

Article 3. Policy application and information notices. The IW-NET site is designed with the main function of providing information on the activities of the Project. Therefore, in most cases, the collection of the user's personal data is not required. In certain instances, such as the "newsletter" section and to allow the transmission of the IW-NET newsletter, the interested user is required to fill out a data collection form. In these cases, the user is always free to provide his/her own data and consent to relevant processing. It is recommended that Users read this Policy before providing the data. In addition, should it be necessary in limited cases to collect personal information for other purposes, this will be clearly shown in the information privacy notices required by law, to enable transparency and user awareness. Consent forms and other documentation will be used each time, as appropriate. The above information aims to define limits and methods of personal data processing of

each service, according to which the visitor can freely express his consent and eventually allow the collection of data and its subsequent use.

Article 4. Optional supply of personal information. The supply of personal data required from a user of the Website, unless otherwise noted, is optional.

Article 5. Controller. The Controller is the actual data owner per data case and it is expected to be a IW-NET partner that has full ownership or is the creator of a data set in the case such information is accessible via the IW-NET website or it has been deposited in a free accessible Registry for the Open Research Data Programme as described in Article 1.

Article 6. Scope of data flow and dissemination. The data may be used by the Controller and/or the Project Partners as well as by third parties who perform operating activities on behalf of them and who act as data processors, to fulfil contractual obligations with regard to the IW-NET Project. Personal data are not disseminated to unspecified recipients. Detailed information on the names of the data processors can be requested by writing to the project coordinator.

Article 7. Traffic data. The computer systems and software procedures used to operate the Website might acquire, during their normal operation, personal data whose transmission is implicit in the use of Internet communication protocols. Such data are parameters regarding the user's operating system and computer environment, e.g. IP addresses, browser type, operating system, domain name and website addresses from which Users are logged in or out, the information on pages visited by users within the site, the time of access, time users stay on a single page, the internal path analysis etc. This kind of technical set of data is collected and used only in an aggregated and not immediately identifiable manner. This data can be released to public authorities per authority request for investigation.

Article 8. Redirects to other websites. From the IW-NET website, users may connect through special links to other websites of Project Partners within the Project, or of third parties as applicable each time. Controller hereby assumes no responsibility regarding the possible processing of personal data by third-party sites and in respect of the management of authentication credentials provided by third parties.

Article 9. Purposes of processing and data retention. The processing of personal data is carried out mainly by using electronic procedures and media for the time strictly necessary to achieve the purposes for which the data will be collected. The User, however, has the right to obtain the cancellation of his data for legitimate reasons.

Article 10. Place of personal data processing. Data processing related to web services of this website takes place, unless otherwise expressly stated, at Controller’s establishment, which provides for the corresponding server management. Personal data are only handled by technical personnel of the Controller, specifically in charge of processing, or others charged with occasional maintenance operations.

Article 11. Data protection rights. With regard to the processing of personal data, a user has the right to obtain confirmation of whether or not such data exist and, in this case, to have it communicated to him/her in an intelligible format per request. Users also have the right to know the content and the origin of the data, to check its accuracy or to ask that it be integrated, updated or adjusted. Finally, Users have the right to ask that the data be deleted or made anonymous or to request the blocking of data processed in violation of the law; moreover, they may oppose the processing of the data for legitimate reasons. Requests should be addressed to the project coordinator.

Article 12. Policy updating. The possible entry into force of new laws, as well as the evolution and updating of User services or developments in the Project could make it necessary to vary the method

of processing of personal data. It is therefore possible that our policy may be modified over time and therefore visitors are periodically invited visit this page.

A summary follows of the general approach to categorise and enforce full confidentially of different categories of data (Table 2):

Table 2: Data Sets in Full Confidentiality

Category	Sub-Category	Examples
Commercial Data handled by IW-NET technical systems. Commercial Data handled by IW-NET technical systems, constitutes valuable business information for the IW-NET partners concerned. Out of their processing useful information may be derived on preferred routes, preferred partners and collaborators, client relationships, billing and collection etc. This information constitutes valuable business secrets and if unauthorized access is granted to them it may cause serious damage to IW-NET partners. Therefore, as a general principle: This data is not to be shared outside the consortium and access within the consortium and is strictly limited to only those parties agreed by the data owner. Some information may also concern third parties such as customers or subcontractors and thus must be stored and processed in accordance with appropriate data protection rules.	Supply chain related data.	These referred e.g. to data shared only with commercial parties on basis of existing commercial agreements. The design teams have access to develop software systems. No other consortium members to have access unless explicitly agreed Invoices. • Purchase orders • Inventory levels • Sales data
	Delivery related information. [Note this may include personal information]	Personal information to be redacted or encrypted if not necessary for functioning of the system • Locations • Times of pickups/Drop offs. • Customer names • Customer addresses • Cargo details
	Real time position information. [Note this may reveal personal information]	• GPS locations • AIS locations • Shipment status information • Booking status • Vessels schedules • Container Information
	Customs related information, usually having legal restrictions	• Manifest. • Customs declaration summary information.
	Data provided by commercial services, which are less sensitive than the above category, however access is also restricted	• AIS/RIS information • Traffic information

Performance related data produced by IW-NET. This data represents aggregated derived statistics about the overall performance of a living lab or technical system. • Technical data related to performance of innovative systems developed within IW-NET may be shared provided it does not compromise commercialisation prospects • Key performance indicators and aggregated results related to the Living Lab (WP4) may be shared with the consent of the appropriate parties provided it is not commercially sensitive. • Key performance indicators and aggregated results related to third parties are generally not shared without being anonymised and/or with consent to publish being given.	Technical data related to performance of systems developed in IW-NET, considering all relevant restrictions w.r.t. Ethics, commercialisation and Patents pending, etc.	• Performance of Big Data analytics system. • Performance publish subscribe system.
	Key performance indicators and aggregated results related to the Living Lab. Data in this category require the agreement of all commercial parties related, to eliminate sensitive information	• Quantified benefits of operational changes (e.g. fuel consumption per barge, cost structures). • Aggregated data –
	Key performance indicators and aggregated results related to third parties. To minimise the possibility of any damage caused to 3rd parties, all data are anonymised as appropriate, and consent of all affected parties is sought.	• Performance related data
Interviews and surveys Participants in interviews or other activities must be asked to sign a relevant form, in order for their consent to be demonstrable in writing. The form must be composed in accordance with legal requirements, i.e. among others to describe how the information is used, how the person concerned may review or amend them.	Results stakeholder consultations and their consent to record and/or publish required before gathering information.	• Responses to surveys • Expert interviews • Participation of individuals in trials or workshops

3 Data sets in IW-NET and the IW-NET Application Scenarios

The Living Lab of IW-NET comprises of different Application Scenarios and use cases that can be considered as the user-centred, open-innovation best practices for the systematic exploration, experimentation and evaluation of innovative ideas, scenarios, concepts and related technological artefacts in real life use cases which involve user communities and thus various data sources.

Being in the initial phase of the project, not enough data are already available or generated e.g. the communication and navigation connectivity sub-systems which are systems that convey real-time information and as such have not yet been setup. The same applies for generated datasets included performance data for hybrid satellite-terrestrial communications systems and for the content based publish subscribe system and data gathered via connectivity interfaces utilized publicly available AIS data. The initial datasets will include simulated data used for testing purposes.

3.1 IW-NET Data Management Plans for ORDP

In the direction to ORDP, the section here provides an indicative Data Management template which will apply to all data to be collected, following the FAIR guidelines, using a web available tool facility[12] to support the creation of FAIR compliant DMPs. All data sets to be published in IW-NET for ORDP will potentially have a corresponding DMP template filled.

Data Collection

What data will you collect or create? A brief description of the data, including any existing data or third-party sources that will be used, in each case noting its content, type and coverage. Outline and justify your choice of format and consider the implications of data format and data volumes in terms of storage, backup and access.
Indicative text… *All data for the xxx application in IW-NET Application Scenario xx, Use Case yy is about the current transport status of a container in the form of a status code which is calculated based on the collection of data from various systems. The Data involve Barges Routes, connecting Trains and Routes, Terminals and Containers.* **Data Volume:** The volume of data is 10k - 100k of textual data records. **Data Format:** The data collected are in Excel (.xls or .csv) format which enables the long-term access and sharing of data. **Data Description:** Data represent historical data collected from legacy systems (years 2018-2020) Container Data include the container registration string and basic information stored including the weight of the empty container, its length and its GPS location with the latest tracking date, truck and the train number, train departure date. Trip details include the start/terminus stations information (name and GPS location), intermediate stops of the train with the station name, GPS location, arrival date and departure date, and the last station (name and GPS location) with the datetime that the train arrived at the last station.
How will the data be collected or created? Outline of how the data are collected/created and which community data standards (if relevant) will be used. Description of how data is organized during the project, naming conventions, version control and folder structures. Description of how the consistency and quality of data collection will be controlled and documented, including processes such as calibration, repeat samples or measurements, standardized data capture or recording, data entry validation, peer review of data or representation with controlled vocabularies.
The container's GPS location and tracking date are generally quite often updated as well as its status according to the information received. When the container is loaded the weight of its contents is filled in and then the transport details are gradually received. At first the destination of the Barge and the Barge IMO identification number, vessel departure date and start, ports departures and arrivals, ETAs and ETD, (name and GPS location) is filled in. UNLOCODES data for Locations, Dangerous Goods and product classification schemes (HSCodes, GS1). During the transport information about the intermediate stops of the barges is added including the port name, GPS location, arrival date and departure date. Details regarding the last station are also stored (name and GPS location) as well as the date that the barge arrived at the last Inland port.

[12]Inserted/Maintained using the online tool/facility at https://dmponline.dcc.ac.uk/plans/39569

The data will be collected from the Operational Systems, exported via a script to the excel format presented, and they will be cleansed and integrated for analysis.

Documentation and Metadata

What documentation and metadata will accompany the data? Refer to the types of documentation that accompany the data to help secondary users to understand and reuse it. Include names of the data creators and contributors to the data, data title, creation date of data and under what conditions data can be accessed.

Document if possible, the methodology used, analytical and procedural information, definitions of variables, vocabularies, units of measurement, any assumptions made, and the format and file type of the data. Consider how you will capture this information and where it will be recorded. Identify related standards if exist.

Indicative text…

A data model for the data is included in the form of a UML diagram. The data in the Application Scenarios conform to the definitions of the UN/CEFACT Core Components Dictionary, which provides the metadata definitions for Supply Chain and Transportation terms.

All datasets used in the experiment will be considered as openly available from the moment they will have been published to an openly accessible repository (e.g. on Zenodo).
As all published data are stored in Excel and CSV file format (Comma Separated Values), they can be opened and manipulated using any text editor or workbooks/sheets such as Excel, or Google Sheets. Based on that, data are sufficiently documented for display and access.

Ethics and Legal Compliance

How will you manage any ethical issues? Ethical issues affecting storage, access including who see/use data and how long data is kept have been addressed. Managing ethical concerns includes anonymization of data; referral to departmental or institutional ethics committees; and formal consent agreements.

Indicative text…

The IW-NET DMP as applied in the Application Scenarios of the Living Lab of IW-NET, relates to the “Ethics and Security” practices of the project , which mandate that all data collection and processing is carried according to EU and National Legislation, as defined in the GA, Part B, Section 5, “Ethics and Security”, where relevant issues concerning Ethics will be considered, determining the framework, the rules and the availability of data, and all possible measures to ensure data are properly anonymized respecting privacy, and to ensure the open data strategy does not violate the terms and guidelines of Related EU policies.

All data sets for sharing will have been checked to ensure that:

- They are not confidential, that they do not include personal or commercially sensitive information. All confidential information or GDPR related data will have been removed, anonymized and/or encrypted.
- That permission from the relevant stakeholders and/or data subjects has been obtained.
- That sharing the data does not damage exploitation or IP protection prospects.

How will you manage copyright and Intellectual Property Rights (IPR) issues? Addressing who will own the copyright and IPR of any data, along with the license(s) for its use and reuse. IPR ownership is covered by a consortium agreement also considering the permissions to reuse third-party data and any restrictions needed on data sharing for the ORDP.

Indicative text…

The IW-NET Data Management incorporates the any Consortium agreements on data management and is consistent with exploitation and IPR and Innovation protection, and the registered patents.

All partners' obligations related to Data management will have been covered via NDAs, as necessary to protect sensitive data, linked to exploitable results to guarantee the marketing and commercial exploitation potential.

Storage and Backup

How will the data be stored and backed up during the research? Consider data back-up policy and storage locations. The use of robust, managed storage provided by university IT teams is preferable.

Indicative text…

Data in IW-NET for all Application Scenarios of the IW-NET Living Lab will be stored in a central Big Data storage facility and the Knowledge Graph, during the project. Also, all Data are stored in a web-based registry, access is provided to all IW-NET partners. During the Living Lab operation, automatic backup services (as opposed to manual backups) provided by the used cloud facility will be applied.

The data for the ORDP will be stored to a repository (e.g. the Zenodo repository), which is an open-access repository before the project Finish accompanied by a DOI citation (Digital Object Identifier).

The IW-NET Application Scenario xxx data are being published in an open repository, and are associated with their metadata and documentation available, DOI cited and indexed.

How will you manage access and security? Consider data confidentiality (e.g. personal data not already in the public domain, confidential information or trade secrets), and outline any appropriate security measures and any applicable standards e.g. ISO 27001.

Indicative text…

IW-NET protects the important and sensitive data and information from the Living Lab (WP4) design and configuration of applications, to be appropriately managed, anonymized, encrypted and sanitized, managing risks which could arise upon their access by third parties.

IW-NET application design considers access to data using Identity Access Management of an OpenStack variant architecture to implement the IW-NET Infrastructure Security, and to only those parties that need to access or process data, encrypting, securing or masking data so that it is not visible to parties which are not authorized, or which do not strictly require it. Security in IW-NET covers Authentication, Authorization, Audit, and Identity Management.

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved? Consider how the data may be reused e.g. to validate research findings, conduct new studies, or for teaching. Decide which data to keep and for how long. This could be based on any obligations to retain certain data, the potential reuse value, economic viability, and any additional effort required to prepare the data for data sharing and preservation.

Indicative text…

The data set of Application Scenario xxx, and Use Case yyy are utilized for Estimated Time of Arrival (ETA) prediction using various techniques and algorithms, and for other relevant Transportation and Logistics uses.

The dataset used will be up-to date until the final 6 months of the project, however, for research reasons and for the algorithm specifications for Big Data analytics, the periods covered (two years) are considered sufficient.
What is the long-term preservation plan for the dataset? Consider how datasets that have long-term value will be preserved and curated beyond the project lifetime. Outline the plans for preparing and documenting data for sharing and archiving. The DMP should demonstrate that data will be made available beyond the lifetime of the project, in the case a public repository is used.
Indicative text… With the end of IW-NET the data will be deposited on a public repository, so, after the end of the project, an unalterable version of the data in the repository will continue to be available to researchers. To ensure high-quality long-term management and maintenance of the dataset. IW-NET procedures comply to the ORDP requirements, permitting a broad range of users to obtain, share, and properly interpret both active and archived information which is at the appropriate format to remain easily accessible and usable.

Data Sharing

How will you share the data? Consider where, how, and to whom data with acknowledged long-term value should be made available. The methods used to share data will be dependent on a number of factors such as the type, size, complexity and sensitivity of data. If possible, mention earlier examples to show a track record of effective data sharing. Consider how people might acknowledge the reuse of your data.
Indicative text… Used data for the Living Lab Application Scenarios are reusable by third parties as they are valid CSV files with well-described metadata. Besides publishing data, it will be available and reusable as long as it still reserved and indexed on the repository.
Are any restrictions on data sharing required? Outline any expected difficulties in sharing data with acknowledged long-term value, along with causes and possible measures to overcome these. Restrictions may be due to confidentiality, lack of consent agreements or IPR, for example. Consider whether a non-disclosure agreement would provide sufficient protection for confidential data.
Indicative text… Generated data from the IW-NET Living Lab are to be licensed under Creative Commons Attribution 4.0 International License. The CC license applies to the data available for re-use and sharing by the time these are published and cited on the Open Data Repository (such as Zenodo).

Responsibilities and Resources

Who will be responsible for data management? Outline the roles and responsibilities for all activities e.g. data capture, metadata production, data quality, storage and backup, data archiving & data sharing. Consider who will be responsible for ensuring relevant policies will be respected. Individuals should be named where possible.
Indicative text… Throughout the IW-NET project lifetime, a Data Protection Officer has been appointed for all data related to the Data Management Plan.
What resources will you require to deliver your plan? Carefully consider any resources needed to deliver the plan, e.g. software, hardware, technical expertise, etc. Where dedicated resources are needed, these should be outlined and justified.

Indicative text…

The resources and costs for the Data Management Plan and the ORDP contribution will have been foreseen and included in the IW-NET project workplan in WP6, Task 6.3.

3.2 Living Lab Data Sets

In the development of the Living Lab Application Scenarios (AS) use-cases and demonstrators, several data sources will have been identified and as the project evolves additional ones will be included aiming at enhancing the overall DMP. In the following, a short description of identified data generated per Living Lab Application Scenario is inserted. As soon as the tasks progress and the Application Scenarios will become better defined including volumes, sources, and their updating schedules, the data per Application Scenario will properly be defined, mapped and managed under the DMP. The tables inserted are a very first outline of the relevant data types per Application Scenario.

3.2.1 AS1: IWT Digitalisation

AS1 investigates the application and benefits of digitalisation for barge operators (to optimally plan services and operations) in three representative IW corridors:

- **AS1A transportation of goods** into dense urban areas (Brussels-Antwerp-Brussels-Courtrai-Lille-Tournai-Valenciennes); enabling predictive **demand routing** on a **pallet** first and last legs within the urban area network, with explicit integration of different categories of **customers**, major stakeholder is Blue Line Logistics.
- **AS1B** focusing on investigating data driven optimisation of barge operations in Danube axis with specific focus to address variable navigability in uncertain water conditions and obtain data to drive design of new types of barges optimised for Danube navigability conditions.

Applying revenue management optimization AS1 will produce reactive decision support systems for intermodal transportation. The main objective of the AS1 is to increase competitiveness of IWT services and to improve transportation network efficiency enabling modal shift and GHG reduction by:

Improving flexibility, speed, and availability of transportation services offered on the network, making use of accurate real-time tracking of freight flows and by monitoring and forecasting incoming & outgoing flows, resources availability and goods' conditions.

Advancing the ability of SMEs to participate and collaborate through improved coordination of tactical service planning, operations management, (e.g. waiting time reduction, last mile seamless modes integration, efficient application of consolidation best practices), and flexible resource shar ing, based on an overall profitability assessment with aligned contractual agreements and risk sharing mechanisms.

Sustainable, closer cooperation between waterway actors and their supply chain partners through revenue management based smart contracting, booking and hierarchical decision making for service planning and demand routing

Performance optimization, by (a) reducing congestion and streamline flows, (b) ensuring an efficient allocation of human and material resources, (c) planning transport activities and managing reservations on the network, including last-mile deliveries and (d) decision-making that integrates flows anticipation and the opportunistic use of residual capacities, market conditions and contingencies.

Table 3: AS1A Data Use Case

Stakeholder	Data Description	Data Type	Data Format	Records	Collected Period	Volume
BLL	**Barge Inland Terminal Visits**	Historical Data, Legacy System	Excel		2018	
	Barge Details					
	Start of Operations					
	End of Operations					
	Operator Details					
	ETA					
PoB	**Barge Deep Sea Terminal Visits**	Historical Data, Legacy System	Excel			
	Barge Details					
	Operator Details					
	Vessel Type					
	Start / End of Operations					
	ETA					
	Weather Conditions	Historical Data	CSV			
	Wind Speed & Direction					

3.2.2 AS2: Intelligent IWT Traffic Flow Management

The major focus of AS2 is on solutions that enable sustainable infrastructure and traffic flow management on inland waterways. Geographically, the Application Scenario will focus the hinterland connections of Bremerhaven via the River Weser and the Mittelland Canal. Along this corridor, the ports of Bremen, Minden, Hannover and Brunswick form important intermodal hubs. From a TEN-T perspective, the Application Scenario supports the development of the "North-Sea-Baltic" as well as the "Orient-East-Med" network.

The Application Scenario will counter these challenges by conceptualizing, developing and implementing intelligent and cost-effective solutions for infrastructure and traffic flow management and showing the potential of integrating of lock scheduling forecasts and dynamic berth allocation. Specifically:

AS2A: Locks forecasting and planning and Traffic forecasts

- Lock forecasting River Weser/Mittelland Canal: reducing uncertainty in vessel voyage planning for larger inland vessels for the Bremerhaven hinterland transport.
- Lock Planning Bremen Oslebshausen/industrial harbour: development of a demonstrator app for lock requests and announcements of vessels arriving from Bremerhaven along the River Weser heading towards the Bremen industrial harbour, development of a planning tool for optimized lock operation.
- Traffic forecasts for new IWT scenarios, e.g. opening the new RegioPort in Minden, a greenfield intermodal facility at the Mittelland Canal and vessel types.

AS2B: Management of fairway sections and Berth Planning

- ICT supported management of fairway sections where encounters are prohibited.
- Berth planning in relation with (mandatory) shore power supply, fresh water supply, other ship supply services (i.e. food and spare parts) for barges including invoicing, part of demonstrator application.

Table 4: AS2 Data Use Case

Stakeholder	Data Description	Data Type	Data Format	Records	Collected Period	Volume
bremenports	**Lock Infrastructure Data**	Historical Data, Legacy System				
bremenports	**Lock Schedule Data**					
bremenports/dbh (external)	**Port Call Data**					
WSV (external)	Infrastructure Network Data	Master Data				
WSV (external)	Network Traffic Data	Historical Data				
WSV (external)	River water level data	Historical Data				
bremenports	**Berth Infrastructure Data**	Historical Data, Legacy System				
Barge operators	Port Call announcement					
Barge operators	Shore power booking request					
bremenports	Invoice data (Energy)					

3.2.3 AS3 Innovative Vessels

AS3 investigates the potential use of innovative vessels to increase the efficiency, competitiveness and reliability of inland waterway transport. Innovative vessel technologies comprise a set of functionalities and related services. Besides advancements in vessel intelligence such as automation and locational awareness technologies, solutions for improved connectivity, navigability and optimized capacity will be developed and tested in order to meet the industrial requirements of users within this application scenario.

AS3A focusing on the development of an innovative IW vessel fleet with a high degree of automation for urban distribution utilizing the East Flanders-Ghent Testing Area.

AS3B conceptualizes a new type of barge that is designed to be used at low and or high-water levels and allows for optimized loading capacities for the barges of push boats. The design will be driven by a business case for the corridor from Port of Enns (Austria) to Giurgiu (Romania).

AS3C aims the enabling of the use of GALILEO services for advanced driver assistant functionalities like a guidance assistant, bridge height warning system and an automatic entering of an inland waterway lock. These functionalities will be implemented and tested on existing vessels in the digital testbed on the Spree – Oder Waterway in the vicinity of Berlin.

In the application scenarios:

- the economic and ecological impact of using the new barges on a round-trip or providing 'on-demand' services will be assessed.
- based on the specifications (e.g., size, capacity, speed) of the new barges, a simulation-based service design will be produced incorporating integration in multimodal chains and specifying fleet size and travel times.
- the benefits of using GALILEO Services for highly automated vessels will be assessed

Table 5: AS3 Data Use Case

Stakeholder	Data Description	Data Type	Data Format	Records	Collected Period	Volume
KUL	**Barges Model Data**	Historical Data,	Excel			
	IoT data					
	GIS data					
DLR	GIS data					
	River Data					
ALB	**Satellite Data**	Historical Data,	Excel			
	Infrastructure Location Data					
NAV						
TTS	**Barges Itineraries**	Historical Data	CSV			
	Navigation Data					

4 Innovation Management Plan

IW-NET considering the financial contribution to the project from public (EU) funding, recognizes a responsibility to:

- protect the Strategic IP - and keep the EC's competitive advantage "within Europe"
- help the EC improve its patent output in the EC's "strategic areas" and improve EC's competitive position on a global stage as a world leader in Innovation
- see increased success/commercialisation from EU projects, and to prioritise innovation and patent resources in ways that incite, help, support the EU SME sector towards economic outputs
- incentivise IP filing decisions towards supporting actors who aim to commercialise the IP, thus prioritizing industry and economic impact (i.e. not to patent/protect innovation that will "sit on a shelf")
- find a responsible balance between "Open" and "Protection" - such that peers/colleagues across Europe can leverage, build on, benefit and prosper from our work (and to discourage stealth patent filings)

In support of the above, IW-NET Innovation Management will seek patent protection in strategic areas, ultimately giving freedom of use and exploitation of the inventive concepts and steps to the consortium and its commercializing actors, unimpeded by competitors outside of Europe.

With formal protection at EUPO and USPTO, a patent will represent a grant of a property right to the owner of the patent, formalised in a detailed document comprising dozens of pages of background, context, specification, diagrams, and patent claims.

This property right conferred is "exclusionary" and is one that excludes others from making, using, offering for sale, or importing a product that practices the invention (the term of a Patent's protection is generally 20 years from earliest filing date). Moreover, protecting the IW-NET commercially strategic innovation supports the European Commission is keeping commercial and economic advantages and associated opportunities within Europe, whilst also helping to improve the EU's reputation on a worldwide stage for research excellence.

4.1 IP Ownership

In line with H2020 best practices, results shall be owned by the project partner carrying out the respective work. If any result is created jointly by at least two project partners and it is not possible to distinguish between the contribution of each of the project partners, such work will be jointly owned by the contributing project partners. In order to further the competitiveness of the EU market, and to enhance exploitation of the consortium results, each contributing party to jointly created IP shall have full freedom of action to independently exploit the jointly created results as it wishes while protecting and assuring Access Rights in accordance with the IW-NET Consortium Agreement.

4.2 Patent Filing Context

All members of the IW-NET consortium will be encouraged to submit compelling innovation propositions for patent protection, in an open and unbiased competition, with the assurance that their ideas will be professionally managed, discussed and deliberated in an open and transparent way, and scored in conjunction with all of the other innovations put forward in a structured framework. As previously indicated, priority of the IP resources will be aligned with intentions to exploit and intentions to commercialise, as well as protecting strategic innovation within Europe, thus giving the commercializing actors within the consortium a competitive advantage and incentive to both commercialise and exploit their innovation.

Confirmed patent filings are thus both tactically and strategically advantageous to the IW-NET partners, and also help influence perceived business value of the solution and the technology, in turn raising the profile of the actors holding the patents.

In respecting EU and US patent law, the IW-NET innovation management methodology recognises that inventions must meet the following criteria and will thus be interrogated from these criteria:

- be “patentable subject matter”
- meet the criteria of being “new or novel” (not invented before)
- meet the criteria of not being publicly disclosed prior to application
- have a “Useful”, substantial and credible use and application
- be operative, i.e. must operate to perform the intended purpose
- be “Non-obvious” - i.e. must not be apparent to one of ordinary skill in the relevant arts
- be “Implementable” – i.e. sufficient detail needs to be provided at filing time to demonstrate that implementation of the invention is both practical and possible

Likewise, within IW-NET the Patentable Concepts that will be supported and guided by the project innovation framework will be in compliance with EU and US law, and thus will fall in to one of the following “legal” invention categories:

- processes, machines, manufacture, composition of matter or improvements thereof
- process: process, act, or method computer programs implementing processes and methods
- machines: “ordinary dictionary meaning” – artefacts that transmit forces, motion, energy
- manufacture: object constructed by application of a manufacturing process
- composition of matter: compounds or mixtures

The IW-NET consortium comprises prominent researchers and industry experts in the fields of Transport & Logistics, Inland Waterways, Shipping construction, Modelling & Simulation, Software Development, IT Infrastructure and commercialisation.

On the basis that the IW-NET project estimated for patent filings, the innovation management approach will involve a combination of technical, business, research and industry actors in support of a collaborative adjudication effort of project-wide decisions for prioritising the available resources.

Such a heterogeneous panel is deemed as an essential ingredient to ensuring fairness, best practice, best decisions, diligence and eliminating any possibility of bias in all aspects of adjudication.

4.3 Identification and Prioritisation of Patents

The innovation management process that IW-NET uses for identifying, selecting and managing inventions is collaborative (involving all partners) as well as iterative. Inventors' inputs are collected through focused sessions, where a panel of experts from across the broader consortium will periodically work together to discern what is collectively agreed as the more strategic and commercially significant innovation.

While questionnaire-based approaches represent an option to gather ideas for inventions across the consortium, such approaches require the inventor to understand key legal subtleties such as non-obviousness, inventive step, patentability, claim sets, reduction to practice, utility, etc. Typically, researchers, engineers and managers would not have such expertise and such approaches can lead to disappointment and loss of time/productivity. Consequently, IW-NET aims to follow a model where technical, business, research and IP expertise work closely together in focused innovation deep-dive meetings, in turn bringing the correct expertise together to collaboratively deliberate and decide innovations from the project that are deemed to have the more significant business, technical and research value and their respective suitability for patent protection. Appropriate checkpoints will be established during the project's lifecycle that brings this expertise together, with the end goal of a well-formed panel of experts collectively paying attention to identifying and protecting the innovation that is deemed to be the most strategic to the project.

The innovation management scoring process works as a collaborative process that will pay attention to, at a minimum, Non-obviousness (for an invention to be non-obvious, the invention must go further than what would have been obvious to one of ordinary skill in the art when properly reviewing the relevant universe of prior art), Utility (be applicable in industry), and Novelty (invention must involve an inventive step). Scores for non-obviousness and novelty represent go or no-go decisions, while utilisation has a more subjective weighting. The no-go decision can be easily made because the obvious or not novel invention has no IP value and cannot be protected. These requirements are further substantiated as follows:

- Inventive step (Non-Obviousness) - An invention is considered to involve an inventive step if, having regard to the "state of the art", it is not obvious to a person with average knowledge of that particular technical field. It is meant that the invention must differ significantly from what is already known. This implies that new ways of combining known methods or objects are not necessarily patentable, hence the question as to whether there is an "inventive step" only arises if there is novelty. The "inventive step" requirement conveys the idea that it is not enough that the claimed invention is new (i.e. different from what exists in the state of the art), but that this difference must have two characteristics – a) it must be "inventive" and the result of a creative idea, and it must be a step that is noticeable. There must be a clearly identifiable difference between the state of the art and the claimed invention.
- Industrial Applicability (Utility) - An invention is industrially applicable or has industrial utility if it can be made or used in any kind of industry. If the invention is intended to be a product or part of a product then someone must be able to make that product. If the invention is for a process or part of a process, then it must be possible to carry out that process in practice.
- Novelty - An invention is novel if it does not form part of the state of the art i.e. the invention cannot be known. The state of the art includes any publicly available description of the invention from anywhere in the world, before the filing of a patent application, and it is known as "prior art". There must be clear that the claimed invention is novel.

In respecting the above patent legislative framework, the expertise and support available within the consortium can focus efforts and resources towards progressing those innovations which have the greatest potential for patent filling success and commercialisation.

The IW-NET consortium will also leverage best practices and experience identifying and focusing the relevant innovation areas for scoring and measurement of innovation which will be based on pre-established KPIs that collectively fall in to three categories of measurement:

- Alignment to EC priorities and objectives – thus ensuring that IP resources are managed in a way that aligned with the EC's strategic priorities and, in turn, securing IP protection in areas that are deemed both significant and important to Europe with the project's living labs as a useful and relevant calibration point
- Alignment with patent laws (EU, US) – which includes overcoming the tests for novelty thus ensuring that filed patents meet the patent office tests for uniqueness and extending the background art in new and non-obvious ways, in turn steering a path for filed patents to be successfully granted (at issuance stage) with approval from the respective patent offices. Ease of discoverability assessments will also be performed, taking the perspective that there is limited commercial use and value in filing strategic IP in situations where it not possible to reasonably demonstrate that a third party may have infringed at some future point down the road. Ease of avoidance will also be factored in to the KPI scoring (see Figure 3), thus applying a weighting that measures the extent to which a third party could circumvent the inventive step(s) through an alternative or modified claim set or through implementing the inventive step in a different way and thus limiting the potential value and commercial significance of the invention.
- Commercial Value - of most significance is the application of an exploitation weighting to the inventions scored, to reduce the potential for innovation to "sit on the shelf" and not be exploited by the consortium's partners, thus incentivizing commitments to use and exploit the innovation commercially and, consequently, giving the commercializing actors a competitive advantage (as well as a valuable asset). Likewise, the background art and prior art landscape will be assessed, to understand the nature of the invention space, taking the view that well invented spaces have limited IP value potential and prioritizing IP resources in areas that will maximize he commercial value of patents granted at the patent office at issuance time. Other aspects such as IP revenue potential shall also be reflected in the scoring, allowing for the prioritisation of decisions where evidence of potential licencing, assignment and divesture values are deemed significant. Last, a final measurement in the scoring will pay attention to the innovation and its alignment with the projects broader commercial vision as expressed by the project's commercialisation plan.

As mentioned, identification, selection and prioritising of IW-NET inventions will be a collaborative process, managed under confidentiality guidelines, open to all actors, and involving commercial, IP, research and business experts from the consortium, guiding an organic free-flowing exchange of ideas and questions. The methodological framework allows these actors to have a naturally flowing conversation with the inventors while at the same time keeping the meeting focused on the goal of prioritising and discerning the more compelling innovations for patent protection, with discussions focused on: (1) supporting data to define the specific measure, dimension and grain of the score; (2) further questions relevant to substantiating score; (3) appropriate actions or decisions to be taken.

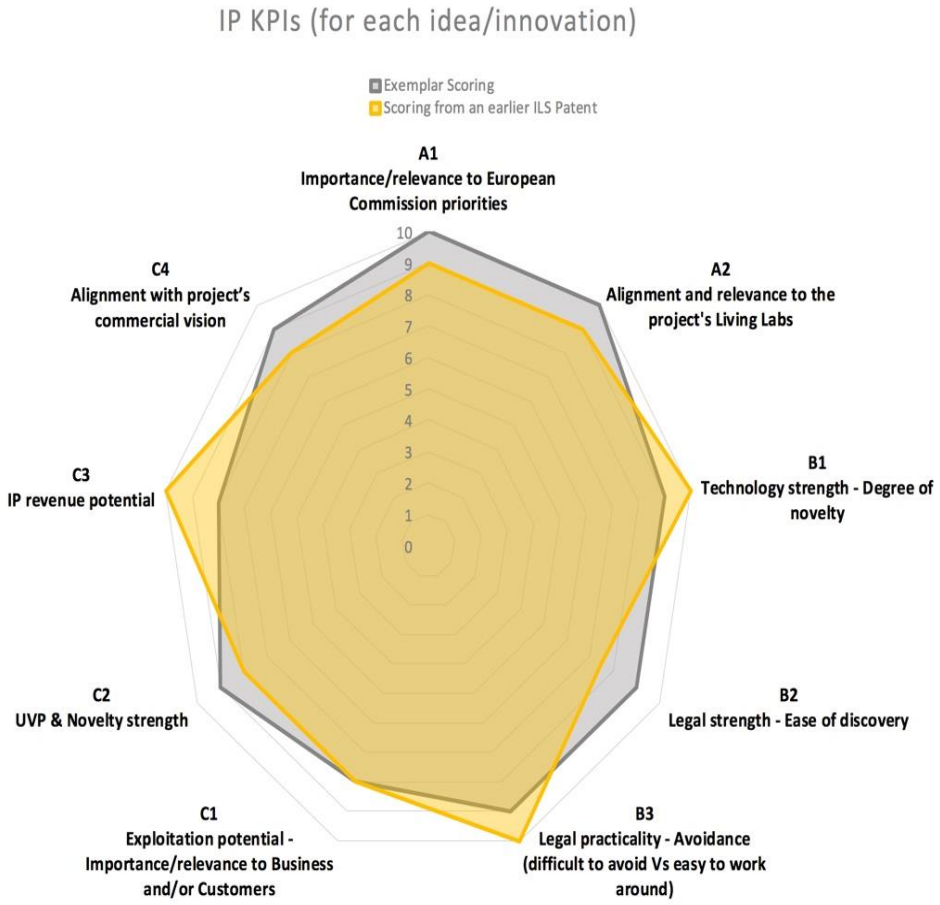

Figure 3 : Innovation Management Framework - KPIs

Frequently, to calculate a KPI score (see Figure 3), along one or more dimensions, one needs to aggregate data from a multiplicity of sources. The goal is to ensure that all attributes that create a score for the stated values and their KPIs are captured and are validated for each given dimension. The term KPI metrics refers to a direct numerical measure that represents a piece of data in the relationship of one or more dimensions. An example would be: "importance to business and/or customers" from the perspective of market coverage. In this case, the measure would be euros (value) and the dimension would be territory (state). For a given measure, one may also wish to see the values across different hierarchies within a dimension. For instance, seeing value by city, region, or state would show the measured euros (value) by different hierarchies (cities, regions, and states) within the territory dimension. Making the association of a measure with a specific hierarchal level within a dimension refers to the overall grain of the metric. Looking at a measure across more than one dimension such as market value by territory (market coverage) and time is called multi-dimensional analysis.

Generally, KPI scorecards leverage multi-dimensional analysis in a limited and static way versus some of the more dynamic "slice-and-dice" tools that exist in the business intelligence market. In practical

scoring terms, IW-NET will use scores agreed in one or multi-dimensional analyses. More specifically, the IW-NET innovation potential KPIs represent a metric tied to a target with a stated KPI representing how far a metric is above or below of such pre-determined target. Scorecards in this context can be used to help align operational execution with innovation strategy with the goal of keeping the innovation focused on a common strategic plan. The primary measurement used will hence be scored KPI value indicators. These indicators will represent a composite of several metrics that measure the innovation ability against a strategic objective.

An example of such a metric would be an indicator named "importance to customers/others" that combines quantitative/ weighted measure such as new customer acquisition with qualitative measure such as customer satisfaction with value proposition (quantitatively measurable with e.g. number of repeated product-purchasing when applicable). By aligning KPIs and scoring with the IW-NET business plan (Task 5.4.1) the importance of the score and separate the "must-have" from the "nice-to-have" inventions are validated, thus prioritising commercial relevance.

The IW-NET consortium will apply best practice in IP value creation to discern a small number of targeted patent assets, applying a spider diagram of KPI (see Figure 3), weighting aiming for high quality and high value patents.

The Innovation Management approach in IW-NET aims to see performance metrics that prioritise strong patents aligned with the IW-NET project goals with IP management guided as a knowledge management process involving many expert stakeholders that collectively comprise a common body of critical information and knowledge that is needed to discern the more strategic and commercially strategic innovation that aligns with the EC's brief, the objectives of the project and which incentivises the commercial ambitions of the project. This work will be done in close alignment with the project commercialisation work task (T5.4.1), where the innovation management methodology and associated decisions will be guided by and informed by progress in this task anticipates the more commercially relevant and commercially strategic innovation.

4.4 IW-NET Patent Filing Process

IW-NET has foreseen the potential of 3 patents which will necessitate the identification and appointment of specialised law recourses for this work, in line with the EC's public procurement guidelines and associated best practices.

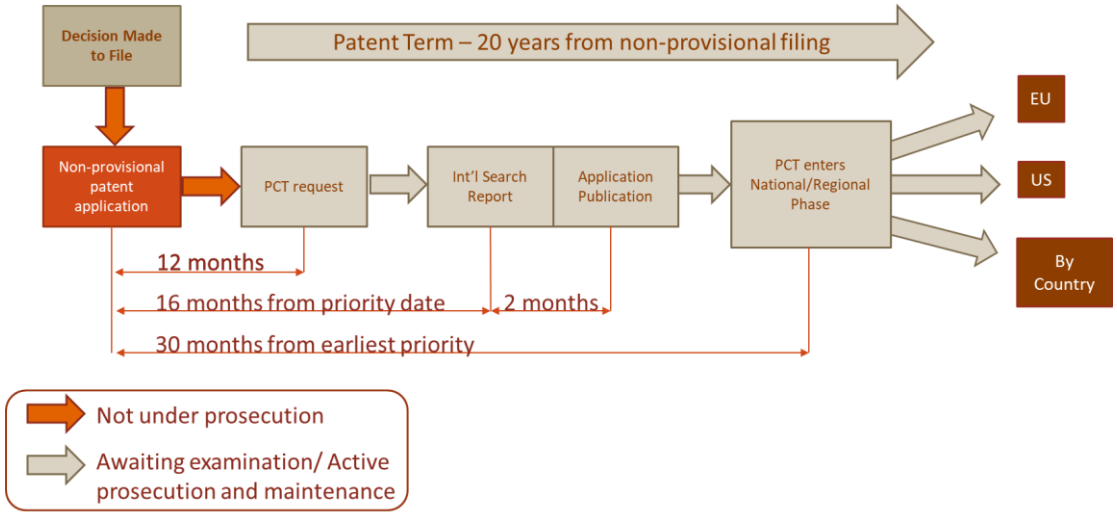

Figure 4: Patent Filing Process

The IW-NET Patent Filing process is abstracted in Figure 4 and is a well-known, predetermined process that starts with Non-provisional Patent Application after which a PCT requests (Patent Cooperation Treaty) assists applicants in seeking patent protection internationally and enables the patent Office to assist with their patent granting decisions, in turn facilitating public access to a wealth of technical information relating to those inventions. By filing one international patent application under the PCT, applicants can simultaneously seek protection for an invention in a very large number of countries. The PCT is an international treaty with more than 145 Contracting States.

4.5 IPR and Patent Training for IW-NET Consortium

The initial IPR training session and workshop will be held the first quarter of 2021, with two key aims: firstly, to create a solid foundation in the basic concepts of IPR protection and secondly, to clarify the IW-NET partners business ambitions commercial vision. In this first session partners with commercial interests will present their current business ambitions in relation to IW-NET.

5 Conclusions

This document is the initial version of the IW-NET DMP, describing the overall management principles on data, including rules of access and sharing, IPR, and the security and privacy of data reflecting the current state of the Consortium agreements on data management. Hence, the DMP aims to be consistent with capacity building and IPR actions, Dissemination and Exploitation (WP5). The DMP is conforming to the EU directives and initiatives to promote research via the Open Access to Data.

The main purpose of the IW-NET Data Management Plan (DMP) is to provide a single point of reference on the policy that governs the data received, generated and managed by IW-NET as well as any data sources to be made available to the public. Additionally, the DMP aims to detail the method and the relevant actions required for the preservation, enhancement and further exploitation of the data collected during the project.

The Data Management approach covers the full data lifecycle as described in section 2.2, also including data that will be used for research and publications and for the IW-NET business models' simulations contributing to the development of the IW Roadmap (WP5).

The IW-NET DMP methodology covers all data generated and collected during the project, the standards used, how the research data are preserved and what parts of the datasets will be shared for verification or reuse, it incorporates the data definitions, and describes the data generation processes and the data captures of the IW-NET Living Lab (WP4), as well as all external data that will be used in the running of the IW-NET platform.

The IW-NET DMP data governance integrates the FAIR principles, and it is in full compliance with the GDPR guidelines. The IW-NET data covered under the DMP are expected to be stored in specified IW-NET components, e.g. the connectivity components (temporary storage), in the Big Data stores and the IW-NET Knowledge Graphs. Further to the storage and maintenance of the data internally in the project, research data under the ORDP are stored externally in open repositories (OpenAIRE, Zenodo).

The IW-NET DMP is made with the prevision to evolve through the IW-NET project lifespan and afterwards, capable to capture and reflect evolution in the form of dataset updates and/or changes in Consortium policies.

The document also includes the description of the IW-NET Innovation Management methodology. Though the task has not already started, the outline of the approach to Innovation Management and the Patenting process has been included, so that as early as M9 of the project innovation management activities will start.

References

[1] Data Management, Participant Portal H2020 Online Manual, Cross Cutting Issues and Data Management, http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

[2] H2020 Programme, Guidelines on FAIR Data Management in Horizon 2020, Version 3.0, 26 July 2016, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[3] H2020 Programme, Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020 Version 3.2, 21March 2017, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

[4] 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). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[5] Wilkinson et al., "The FAIR Guiding Principles for scientific data management and stewardship", 2016, Scientific Data 3:160018, https://doi.org/10.1038/sdata.2016.18

[6] EU GDPR Website, GDPR portal: https://www.eugdpr.org/.

Annex I: Data Management Plan Context

1. **References to the Grant Agreement** 861377**— IW-NET**
   a. **Article 29.3**

29.3 Open access to research data

*Regarding the digital research data generated in the action ('**data**'), the beneficiaries must:*

(a) deposit in a research data repository and take measures to make it possible for third parties to access, mine, exploit, reproduce and disseminate — free of charge for any user — the following:

(i) the data, including associated metadata, needed to validate the results presented in scientific publications as soon as possible;

*(ii) other data, including associated metadata, as specified and within the deadlines laid down in the '**data management plan**' (see Annex 1);*

(b) provide information — via the repository — about tools and instruments at the disposal of the beneficiaries and necessary for validating the results (and — where possible — provide the tools and instruments themselves).

This does not change the obligation to protect results in Article 27, the confidentiality obligations in Article 36, the security obligations in Article 37 or the obligations to protect personal data in Article 39, all of which still apply.

As an exception, the beneficiaries do not have to ensure open access to specific parts of their research data if the achievement of the action's main objective, as described in Annex 1, would be jeopardised by making those specific parts of the research data openly accessible. In this case, the data management plan must contain the reasons for not giving access.

(See footnote for Annex 1 referenced in Article 29.3 [13])

The most important reasons for setting a Data Management plan are:

• The EU policy on data management is increasingly geared towards providing open access to data that is gathered with funds from the EU. The rationale is that the Horizon 2020 grant consists of public money and therefore the data should be accessible to other researchers;

• Stimulating the reuse of research data by other researchers;

• Helping to streamline the research process from start to finish. A data management plan clarifies in advance the required data expertise and facilities to store data.

[13] Annex 1 to the Grand Agreement is the "Description of the Action"

Annex II: Global Data Protection Policies and IW-NET

This Global Data Protection Policies in the context of IW-NET should be applied individually by all Partners so to:

- Comply with the policy and legal requirements of the EU General Data Protection Regulation (Regulation EU 2016/679, the "**GDPR**"), as in effect since 25 May 2018;
- Comply with all other applicable national and EU regulations and guidelines on personal data processing;
- Comply with applicable regulations and best practices with regard to research projects within the EU H2020 Research Programme;
- Raise awareness and improve knowledge among the Project Coordinator, the Project Partners, as well as their employees and/or agents and/or contractors (collectively, the "**Policy Recipients**").

Because the field of data protection is a dynamic legal field of constant change, new developments, in the form of new regulations, official reports and/or guidelines, are issued by EU and national legislators, as well as, competent national authorities at a constant pace. In this context, Policies may need to be periodically updated in order to remain relevant to legislative change. Accordingly, Policy Recipients will be duly informed, and will be asked to provide their renewed consent upon any such updates.

1. Definitions

The GDPR definitions, as set in the GDPR Article 4[14], apply. In addition,

"**Personal data**" in IW-NET means any information relating to an identified or identifiable natural person that is processed by any Project Partner and Policy Recipient during execution of the IW-NET Project. Further information is provided in section 0 "Personal data" of this Annex.

"**Controller**" means the owner of the data (usually the creator of the data itself), unless otherwise expressly clarified in e.g. Project deliverables and reports. Further information for the use of the term "Controller" complying to GDPR is provided in section 0 of this Annex.

"**Processor**" means each Project Partner, referring mainly the technical partners participating into the IW-NET consortium, unless otherwise expressly clarified in this Policy or elsewhere in Project deliverables and reports. Further information for the use of the term "Processor" complying to GDPR is provided in section **Fehler! Verweisquelle konnte nicht gefunden werden.**0 of this Annex.

"**Consent**" of the data subject means any freely given, specific, informed, unambiguous and **in writing** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"**Supervisory authority**" means the competent Data Protection Authorities within the Project Partners' jurisdictions.

2. Policy scope

IW-NET leaves the GDPR compliance to the Controllers and Processors consortium members. The Controller determines in advance what is the law applicable to the processing of personal data in a particular case, considering that according to EU law such determination comes from legal principles and cannot be derogated by the parties.

[14] http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm

3. Establishment

Each Project Partner is established on the territory of EU Member States. In the event of any change in establishment, the respective Project Partner shall notify the Project Coordinator duly and in writing. Unless otherwise expressly specified, each Project Partner is considered the controller in that Member State.

Processor outside the EU

In the event of any subcontracting to an organization not established on EU territory (such as subsidiaries pertaining to the same corporate group) that processes personal data of people staying on EU territory, on behalf of a Project Partner, that organization qualifies as Processor and ensures the fulfilment of the obligations imposed by the GDPR for that specific part of processing.

4. Personal data processing

Personal data

Personal data means any information relating to natural persons, that is or can be identified, even indirectly, by reference to any other information including a personal 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.

Special categories of data

Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation as well as the processing of genetic data and biometric data for the purpose of uniquely identifying an individual. In the event of such processing the Controller and/or Processor respectively comply with specific rules related to the processing of such data of special categories, as collecting specific informed consent from data subject and applying stricter safeguards. When the Controller and/or Processor relies on data subject's consent as a legal ground for processing special categories of data, it will meet all legal consent requirements; otherwise, they are only processed if and to the extent it is based on one of the legal grounds listed in the GDPR for the processing of such data.

Newsletters, social media and other dissemination material

Unless otherwise expressly specified in Project contract, Controller shall be responsible for the personal data processing carried out for Project dissemination purposes. To this end, Controller shall:

- Collect and keep all relevant personal data (including lists of contact details), or copies thereof;
- Monitor relevant communications;
- Address to Project Partners instructions and guidelines on Project dissemination activities (including any EU or other state guidelines, whenever available);
- Inform Project Partners of any policy or legal requirements reviews and changes.

Data processing

Data processing means any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organization, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data whether the latter are contained or not in data bank. European Union data protection law set forth the following specific principles for legitimate data processing.

Pertinence and necessity - The Controller should implement management practices to fulfil the obligation to collect only relevant and necessary data for a specified purpose.

Purpose limitation - Personal data is collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The Controller has a clear overview of

all purposes for which personal data is processed. Personal data is not processed for purposes besides the original purposes, unless the (secondary) use is compatible.

Data minimization - Personal data collected by the Controller must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and further processed; if the same purposes can be realized in a less data intensive way a preference is given to that method.

Data update - Personal data is accurate, and, where necessary, kept up to date. Every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Data retention - Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The Controller and/or Processing concerned should have processes and policies in place to:

a) determine what the applicable (minimum and maximum) retention periods are for the personal data that is being processed;
b) ensure that relevant retention periods are monitored.

Data anonymisation

Whenever possible, including non-detrimental to Project execution purposes, Controller and Project Partners shall undertake efforts to keep personal data processed by them for Project purposes anonymous or pseudonymous. According to the GDPR, “anonymous information” is information which does not relate to an identified or identifiable natural person, or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In this context, the GDPR does not apply to the processing of such anonymous information, including for statistical or research purposes. Similarly, “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.

5. Data protection legal roles

Controller

By determining the purposes and means of the processing of personal data, unless otherwise expressly specified in this Policy, the Controller is considered by law as the “Controller” and it is the primary target of the provisions of the law.

Identification

The data controller previously identifies itself as such and ensures an effective implementation of data protection measures in order to comply with the principle that personal data are processed fairly and lawfully. The legal role of controller implies specific responsibilities because provisions setting conditions for lawful processing are essentially addressed to the controller.

i. Accountability

The GDPR provides full accountability of the company/controller regarding the compliance of its processing of personal data with the law. To ensure the effectiveness of that obligation, it prompts the Controller to follow an overall approach, achieving a genuine system of control and management of its pertinent information. So, accountability and compliance system are elements of the framework for the protection of personal data, in the cause / effect relationship: to be compliant and able to prove it (accountability), the Controller needs to put in place a comprehensive compliance system.

ii. Data protection by design

The Controller considers data protection issues from the outset and from the design of the Project, within the whole lifecycle of processing, to manage the issues in a proactive way, to reduce costs and improve efficiency.

iii. Data protection by default

The Controller standardizes data protection principles in personal data processing, products and services. The measures adopted ensure that

- personal data is processed for purposes not different from the original purposes,
- only data necessary for these purposes are collected, and
- data are not disclosed without human intervention.

Joint controller

In the event that at any time during Project execution the Controller processes personal data in conjunction with a third party, by jointly determining the purposes and means of the processing, they both act as joint controller. Both joint controllers determine the mutual responsibilities with a specific arrangement.

Processor

Unless otherwise specified expressly in this Policy, all Project Partners act as Processors during Project execution. A processor processes personal data on behalf of the Controller – that is, the Controller delegates all or part of the processing activities to them. In such event the Project contract assumes the role of the relevant required written agreement as per GDPR requirements.

The processor warrants that it shall provide sufficient guarantees to ensure compliance with the GDPR, has implemented appropriate controls to meet data protection requirements defined by the agreement, instructions and/or legal requirements and ensures the protection of the rights of data subjects.

Auditing

The Controller ensures the commitment of the Processor(s) to enable and contribute to any review activities, including inspections, carried out by the Controller or other (EU authorities') auditors and/or reviewers, as appropriate.

Security

Each Project Partner undertakes that it adopts appropriate security measures to ensure the security, integrity and confidentiality of personal information and electronic communications at an adequate level with regard to Project purposes, and at any event at no lower lever than processing of similar data within its own organisation.

Data Protection Officer (DPO)

Whenever required, following applicable GDPR and Member State respective legal requirements, the Controller and each Processor, may designate a data protection officer ("DPO") for assistance in monitoring internal compliance with GDPR.

i. Identification

Each Processor appoints a DPO in accordance with the criteria and the requirements set forth in the GDPR, as applicable to it. In such event, it shall notify the Controller in writing accordingly.

ii. Designation compulsory vs. voluntary

Each Processor documents the reasons supporting the designation of the DPO or, rather, the reasons why such designation is deemed not necessary. This documentation forms part of the data protection documentation system of that Processor.

iii. Professional requirements

The DPO has sufficient authority, professional qualities and independence to ensure success in his role, according to the GDPR provisions.

Tasks, Notification to Supervisory Authority

The organization assigns to the DPO at least the tasks listed in the GDPR. Whenever a DPO is appointed the organization notifies the Supervisory Authority of such designation and publishes DPO's contact details.

i. People in charge of processing

Individuals who process personal data under the authority of the Controllers or Processor(s) must receive specific formal instructions. Hence, the Controller gives specific instructions, relating also to the implementation of security measures and safeguards, to all of its personnel in charge of processing personal data.

ii. Training and awareness

All Project Partners' employees should be well informed and aware of data protection implications and be able to carry out their obligations in their work. A data protection education and communication program should be in place and supported by a monitoring system that confirms all employees and/or contractors are appropriately trained on their data protection responsibilities.

iii. Policies and procedures

Data protection policies and procedures exist, are documented in writing, are formally approved by management, implemented, reviewed, updated and approved when there are changes to applicable laws and regulations.

All Project Partners understand, and the Controller may ask them to overview all their personal data processing, the data protection risks and the applicable rules and procedures. In such event, they shall provide it with all requested information to the best of their ability without undue delay.

6. Notice and consent

Notice

Each Controller and/or Processor, as appropriate, provides the information required by law to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

The data protection notice informs data subjects about the processing of personal data relating to them, even when the personal data is not collected from them as well as of their rights, in order to let them verify in particular the accuracy of the data and the lawfulness of the processing.

Free and informed consent

Personal data is processed if and to the extent that the data subject has given valid consent to the processing for one or more specific purposes, or another legal basis for processing exists.

Systems or applications are able to document the explicit consent of the data subject so that it can be evidenced at any time.

Other legal grounds for a legitimate personal data processing are the following:

1. performance of a contract;
2. legal obligation;
3. vital interest of data subject;
4. public interest;
5. legitimate interest of the controller or third party.

If "legitimate interest" is used as a basis, the interests that have preceded to the decision, need to be documented as well as any possible mitigating measures which will be taken to be able to proceed with personal data processing based on the defined interests.

Withdrawal of consent

Data subject's consent can be withdrawn at any time; even though it will not affect the lawfulness of processing based on consent before its withdrawal.

7. Rights of data subjects

The individual whom the data refers to (data subject) is entitled with specific rights set forth by the law. The GDPR requires that each Controller and/or Processor, as appropriate, must facilitate the exercise of the data subject's rights, take action on the request within a specific time frame and must communicate the information requested in an intelligible and easy to access form.

Right of access

Any individual must be able to exercise the right of access to data relating to him which are being processed.

Right to rectification

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request rectification of their personal data. The procedure specifies in which cases rectification is legitimate.

If a data subject's request for rectification is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

Right to erasure

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request erasure of their personal data. The procedure specifies in which cases erasure is legitimate.

If a data subject's request for erasure is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

Right to restriction of processing

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request restriction of processing of their personal data. The procedure specifies in which cases restriction is legitimate.

If a data subject's request for restriction of processing is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

Right to data portability

Each Controller and/or Processor, as appropriate, determines which processes are subject to the right of data portability as well as when the requirements for such right are met.

Data subject can request the organization to receive a machine-readable copy of the personal data the organization holds about them and where possible, enable the transfer of this data to another data controller.

Portability right can be exercised when:

1. processing operations are based on data subject's consent or on contract
2. personal data concerns the data subject and are the same that the latter has provided to the organization
3. the right does not adversely affect rights and freedoms of others
4. the processing is carried out by automated means.

Each Controller and/or Processor, as appropriate, implements appropriate measures and procedures to provide data subject, who is entitled to, with a structured, commonly used and machine-readable copy of the personal data it holds about him and where possible, to enable the transfer of this data to another data controller indicated by data subject.

Right to object

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subjects have the right to object on grounds relating to their particular situation (unless the processing is necessary for the performance of a task carried out for reasons of public interest). The right to object is explicitly brought to the attention of the data subject at the latest at the time of the first communication with the data subject, presented clearly and separately from any other information. Measures should be in place to assess such objections and to ensure that such processing ceases when the request is legitimate and needs to be respected.

Data subjects have right to object, on request and free of charge, to the processing of personal data relating to them for purposes of direct marketing.

Automated decision making

Data subject has the right to object to any automatic decision-making (including profiling).

Each Controller and/or Processor, as appropriate, will have determined which processes entail automated decision-making (including profiling) and will have established measures to allow data subjects to object to such automated decision making and profiling. Suitable measures are in place to safeguard the data subject's rights and freedoms and legitimate interest, at least the right to obtain human intervention on the part of the Company/controller, to express his or her point of view and to contest the decision.

Timely response to exercise of rights

Each Controller and/or Processor, as appropriate, must confirm to data subjects without delay whether data relating to them are processed and communicate the data to them in an intelligible form. Each Controller and/or Processor, as appropriate, should implement internal procedures in order to be able to provide a timely response to the requests of data subject for the exercise of his rights.

Measures have to be implemented in a way that effectively allows an individual to exercise his or her right to personal data, and that enables Each Controller and/or Processor, as appropriate, to respond to such request appropriately within the required timeframes.

Notification to recipients

In case of a legitimate exercise of rights to rectification, erasure or restriction of processing recipients of the personal data should be informed of the rectification, erasure of that data or of the restriction of processing.

Each Controller and/or Processor, as appropriate, should have a procedure in place for communicating any rectification or erasure of personal data or restriction of processing to the recipients to whom the personal data has been disclosed and for disclosing these recipients to the data subject, if so requested.

8. Data protection documentation system

Register of processing

Each Controller and/or Processor, as appropriate, with regard to their processing activities must set up a relevant record, maintained in writing (including in electronic form) and made available easily and swiftly to the supervisory authority on request, as per applicable legal requirements within their respective Member States. The record of processing activities shall contain all the information required by GDPR.

Consequently, the Controller shall have an up-to-date overview of all personal data processing activities and shall maintain records within the Project, that meet the legal requirements posed by the GDPR. By so doing, the Controller will be able to demonstrate compliance to any Supervisory Authority or other state or EU authority concerned.

For the avoidance of doubt, each Project Partner carries the same responsibility above within its own respective organisation.

Register of data breaches

A specific register where the breaches have to be recorded together with other information specified by the law, must be maintained by the Controller and shown to the Supervisory Authority upon request. This register is an important element of the data protection documentation system.

Project Partners need to notify immediately and in writing the Controller of any personal data breach within their respective organisations that affects execution of the Project in any way, and to cooperate with the Controller while applying relevant GDPR legal requirements.

9. Data protection assessment

Assessment

In the event that a Data Protection Impact Assessment ("**DPIA**") is carried out under the Project, the Controller shall ensure that personal data receives the appropriate level of protection in accordance with the assessed data protection risk.

The decision whether to carry out a DPIA under the Project, unless undertaken in respective Project contract, will be made by the Controller upon prior written consultation with the Project Partners.

i. Adequacy of protection

The Controller, assisted by Project Partners, should have a process in place in order to assess for all processing the risks of varying likelihood and severity for the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of personal data processing.

ii. Impact assessment in case of high risk (DPIA)

When the preliminary assessment highlights that processing represents high risks, a formal and documented DPIA is carried out by ascertaining possible impact on data subject.

DPIA is conducted in such a way to meet all the requirements set forth by the GDPR (art. 35) in order to confirm the quality and validity of the findings.

iii. Prior consultation to Supervisory Authority

The Controller has a process in place and roles are assigned in order to ensure that when a DPIA determines that the processing represents high risks, the competent Supervisory Authority is consulted prior to the processing.

Technical and organizational measures

The Controller and each Project Partner, as appropriate, adopts appropriate technical and organisational measures with regard to Project execution (the "**Measures**"), and reviews and updates them where necessary, to ensure and to be able to demonstrate that processing is in compliance with GDPR.

Each Project Partner shall notify relevant Measures to the Controller in writing. In the event of any queries or further requests by the Controller, each Project Partner undertakes to address them duly and in writing.

In the event that any Project Partner has notified the Measures to its competent Supervisory Authority, it shall inform the Controller thereof, and shall provide respective copies thereof.

Data breach

According to GDPR, the Controller and/or Processor, as appropriate, has to implement adequate Measures in order to prevent personal data breaches.

In addition, the Measures should be able to minimize the adverse effects, in case a security breach to personal data relating in any manner to the Project occurs anyhow.

Should a data breach occur, GDPR sets forth that the Controller and/or Processor, as appropriate, has to notify it to the Supervisory Authority providing specific information, without undue delay and in any case no later than 72 hours from the time of knowledge.

When the breach leads to significant risk of serious adverse effects on the data subject(s) or serious adverse consequences for the protection of personal data, also the latter must be informed without undue delay.

Data transfers to third countries

No international transfers of personal data are expected to take place under the Project.

In the event that any Project Partner wishes to carry out such personal data processing, it shall notify the Controller in writing and in advance. Unless otherwise expressly specified, any international data transfers carried out by any Project Partner for any reason during Project execution take place at its own exclusive liability and responsibility; same Project Partner shall hold all other Project Partners (including the Controller) harmless from any legal or other claims arising for such personal data processing.

Sanctions and damages

In case of violation of data protection principles and rules, each Project Partner (including the Controller) is responsible for damages and is subject to sanctions. Possible violations may involve civil liability and sanctions in order to ensure that any relevant damage is compensated.

The Project Partner (including the Controller) that is liable for said damages and/or sanctions shall hold all other Project Partners harmless from any claims, costs, and expenses arising from relevant GDPR infringement.