NEXT GENERATION INTERNET

Grant Agreement No.: 957216
Call: H2020-ICT-2018-2020

Topic: ICT-56-2020
Type of action: RIA

iNGenious

D7.1 DATA MANAGEMENT PLAN

Revision: v.1.0

Work package	WP7 Dissemination, standardisation and exploitation
Task	T7.1
Due date	31/03/2021
Submission date	26/03/2021
Deliverable lead	NXW
Version	1.0
Authors	Erin Seder (NXW), Giacomo Bernini (NXW), Efstathios Katranaras (SEQ), Guillaume Vivier (SEQ), Ignacio Garcia Zuazola (NOK), José Luis Cárcel Cervera (FV), Alexandr Tardo (CNIT), Christos Politis (SES)
Reviewers	David Gomez-Barquero (UPV), Nuria Molner (UPV)

Abstract	This Data Management Plan (DMP) describes the management life cycle for the data to be collected, processed, and generated by the iNGENIOUS project. This document also includes information on the data format, dissemination, and preservation plans in line with the FAIR (Findable, Accessible, Interoperable and Reusable) Data Management Protocols.
Keywords	data management

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	26/03/2021	Final version submitted to the EC	E. Seder (NXW)

DISCLAIMER

This iNGENIOUS D7.1 deliverable is not yet approved nor rejected, neither financially nor content-wise by the European Commission. The approval/rejection decision of work and resources will take place at the Mid-Term Review Meeting planned in June 2022, after the monitoring process involving experts has come to an end.

The information, documentation and figures available in this deliverable are written by the "Next-Generation IoT solutions for the universal supply chain" (iNGENIOUS) project's consortium under EC grant agreement 957216 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

COPYRIGHT NOTICE

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	OTHER (ORDP: Open Research Data Pilot)	
Dissemination Level		
PU	Public, fully open, e.g. web	✓
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to iNGENIOUS project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

EXECUTIVE SUMMARY

The iNGENIOUS project is a Horizon 2020 action expected to have open-access exportable data. This deliverable, the Data Management Plan (DMP), explains the project's action plan pertaining to data management; describing the main elements of the data management policy that will be used by iNGENIOUS project.

The topics that will be presented include:

· DMP structure;

· Data types and modes of preservation;

· Ethics to be followed;

· Intellectual Property Rights.

The DMP is an Open Research Data Pilot document that will be updated from its creation to the end of the iNGENIOUS project. Any changes to the Data Management Plan will also be included in the deliverables D7.2, Mid-term dissemination, standardisation and exploitation report, and D7.3, Final dissemination, standardisation and exploitation report.

OBJECTIVE OF THE DOCUMENT

The document covers the topics of exploitation of research data generated (and collected) within the project, and the dissemination of the public scientific results which are created by the project.

The scope of the current DMP is to make the iNGENIOUS public data easily:

· Discoverable;

· Accessible;

· Usable.

The document also covers data ethics and security for sensitive data, as well as project guidelines for intellectual properties.

STRUCTURE OF THE DOCUMENT

This document is divided into 4 sections. Section 1 provides the principle and structure of the management life-cycle of produced data, following FAIR (Findable, Accessible, Interoperable and Reusable) data management protocols. Sections 2 and 3 address data security/ethics, and intellectual property rights, respectively. Lastly, Section 4 outlines the detailed data management for each use case and proof of concept.

TABLE OF CONTENTS

Co-funded by the Horizon 2020
Framework Programme of the European Union

LIST OF FIGURES

Co-funded by the Horizon 2020
Framework Programme of the European Union

LIST OF TABLES

ABBREVIATIONS

AGV	Automated Guided Vehicle
API	Application Programming Interface
COM	COMmunication port
DBMS	Database Management System
DMP	Data Management Plan
DLT	Distributed Ledger Technologies
DLV	Data Virtualisation Layer
DMP	Data Management Plan
DPO	Data Protection Officer
FAIR	Findable, Accessible, Interoperable, Reusable
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GMS	Google Mobile Services
IE	Innovation Elements
iNGENIOUS	Next-GENeration IoT sOlutions for the Universal Supply chain
IoT	Internet of Things
IPR	Intellectual Property Right
M2M	Machine-to-Machine
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
ML	Machine Learning
MMC	MultiMediaCard
MR	Mixed Reality
OTA	Over-The-Air
PoC	Proof of Concept
SD	Secure Digital
SD-MAC	Software-Defined Medium Access Control
SDN	Software-Defined Network
SD-PHY	Software-Defined PHYsical layer
SNR	Signal-to-Noise Ratio
UC	Use Case
WP	Work Package

Co-funded by the Horizon 2020
Framework Programme of the European Union

1 DATA MANAGEMENT

Data management is an important component of the responsible conduct of any research initiative. Thus, there is a need to describe how data will be collected, stored and preserved, as well as managed and shared. This document, which serves this purpose, is a Data Management Plan (DMP).
All Horizon 2020 projects are required to export open-access data, meaning end users should be able to have free-of-charge online access to project scientific information and outcomes. More specifically, the information that will be offered under the iNGENIOUS project includes:

1) peer-reviewed scientific research articles (published in scholarly journals);
2) research data (data underlying publications, curated data and/or raw data);
3) results to be incorporated into standards.

The iNGENIOUS DMP follows the template recommended by the European Commission [1]. The template includes the 4 guiding principles of FAIR data [2]:

To Be Findable	**F1**. (meta)data are assigned a globally unique and persistent identifier **F2**. data are described with rich metadata (defined by R1 below) **F3**. metadata clearly and explicitly include the identifier of the data it describes **F4**. (meta)data are registered or indexed in a searchable resource
To Be 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 an authentication and authorization procedure, where necessary **A2.** metadata are accessible, even when the data are no longer available
To Be Interoperable	**I1**. (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation. **I2**. (meta)data use vocabularies that follow FAIR principles **I3**. (meta)data include qualified references to other (meta)data
To Be Reusable	**R1**. meta(data) are richly described with 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 detailed provenance **R1.3**. (meta)data meet domain-relevant community standards

TABLE 1: GUIDING PRINCIPLES OF FAIR DATA [2]

1.1 FINDABLE DATA

The data generated in the framework of the iNGENIOUS project will have unique identifiers so as to be easily discoverable by research communities. The identifier format is:

INGENIOUS_[Name]_[Type]_[Date]_[Owner]

where

· [Name] is a short and characteristic name for the data;
· [Type] is the type of data (code, publication, measured data);
· [Date] is the date when data was produced (format: DDMMYYYY);
· [Owner] is the owner (or owners) of the data (if exist);
· _ (underscore) is used as the separator between the fields;

For example, the following identifier:
INGENIOUS_PlatformConfiguration_code_23012021_NXW
indicates that the generated data is a code which is used to configure the platform. The configuration was completed on 23-01-2021 by NXW, which is the owner of the configuration.

In addition to the unique name identifier, the data set description is also important. The data set description is organized as metadata. Metadata is used to give information such which data are generated by the project and which are collected and used. The metadata identifier is formed in a similar way to the data identifier but with more details and, depending on the file format, will be either incorporated as a part of the file or as a separate file e.x. text format.

The metadata identifier format is:

INGENIOUS_[Name]_[Type]_[Date]_[Owner]_METADATA

where

· [Name] is a short and characteristic name for the data
· [Type] is the type of data (code, publication, measured data)
· [Date] is the date when data was produced (format: DDMMYYYY)
· [Owner] is the owner (or owners) of the data (if exist)
· _ (underscore) is used as the separator between the fields

1.2 ACCESSIBLE DATA

The public access to the project data is ensured with the development of the project website, https://ingenious-iot.eu:

Co-funded by the Horizon 2020
Framework Programme of the European Union

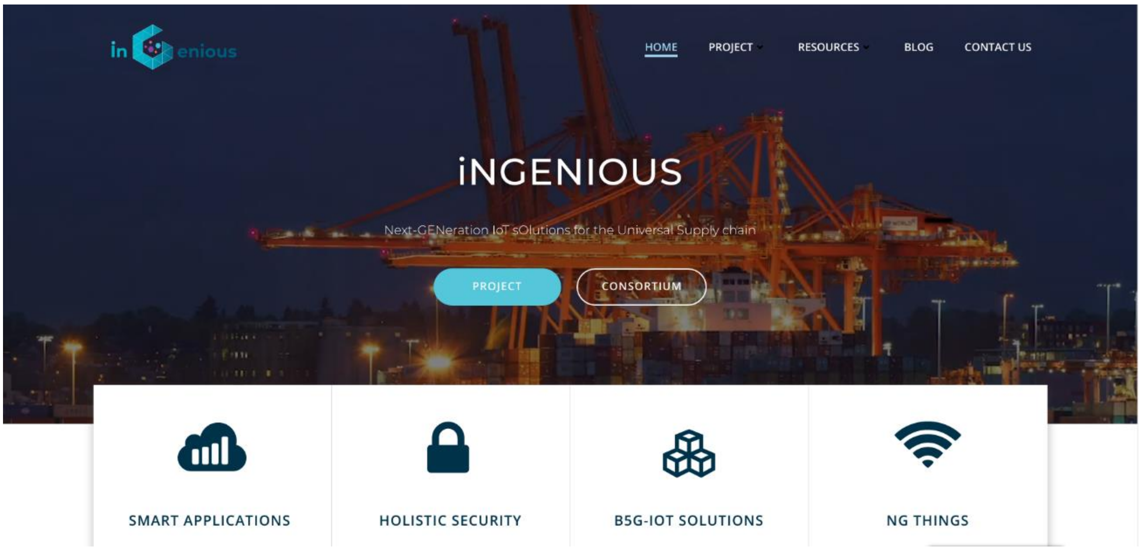
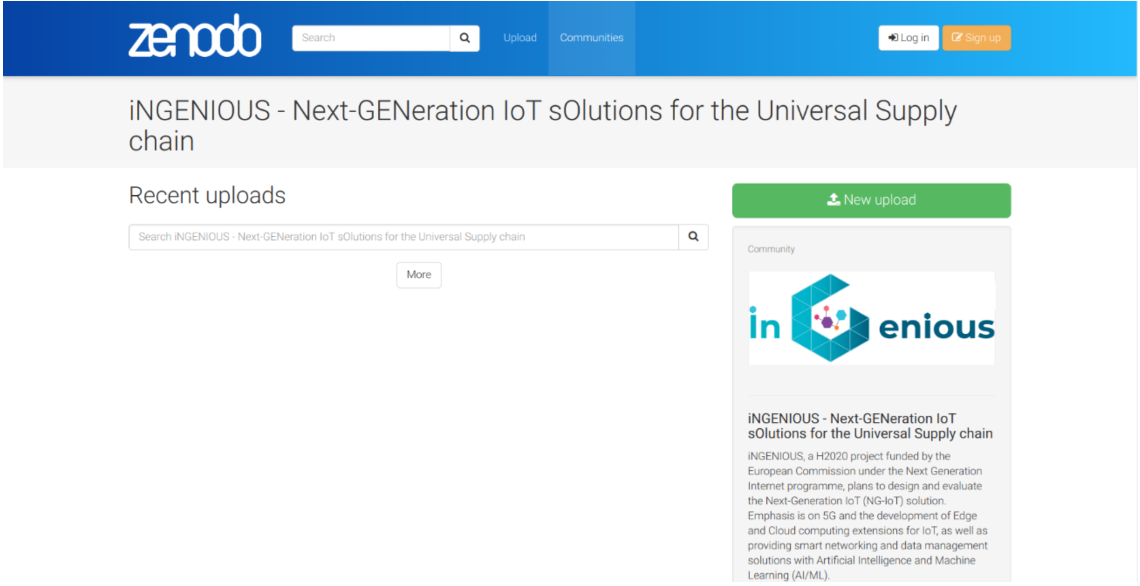


FIGURE 1: INGENIOUS PUBLIC WEBSITE

The website permits easy and convenient access for users and research collaborators to the project's research data. Additionally, a Zenodo repository will be used for storing the project's public data. Zenodo is an open-access repository developed under the European OpenAIRE program. It allows for the dissemination of research papers, data sets, research software, reports, and any other research related digital artifacts [3]. The project has a Zenodo Community page, https://zenodo.org/communities/ingenious-iot/ where the available data will be displayed and accessible:



iNGENIOUS - Next-GENeration IoT sOlutions for the Universal Supply chain

iNGENIOUS - Next-GENeration IoT sOlutions for the Universal Supply chain

iNGENIOUS, a H2020 project funded by the European Commission under the Next Generation Internet programme, plans to design and evaluate the Next-Generation IoT (NG-IoT) solution. Emphasis is on 5G and the development of Edge and Cloud computing extensions for IoT, as well as providing smart networking and data management solutions with Artificial Intelligence and Machine Learning (AI/ML).

FIGURE 2: INGENIOUS ZENODOO COMMUNITY PAGE

A third source of public access is though the public repositories of individual partners[i]:

UNIVERSITAT POLITECNICA DE VALENCIA:
https://riunet.upv.es/

[i] Partner repositories will host those publications which are authored/co-authored by members of the hosting institution.

BARKHAUSEN INSTITUT GGMBH
https://www.barkhauseninstitut.org/ergebnisse/publikationen

TECHNISCHE UNIVERSITAET DRESDEN
https://www.vodafone-chair.org/publications

1.3 INTEROPERABLE DATA

Several data types, as detailed in Section **¡Error! No se encuentra el origen de la referencia.**, are foreseen to be generated within the project. In order to ease the procedure of data exchange the consortium partners will use a fully documented commentary on the data produced.

1.4 REUSABLE DATA

Public project data will be open access. They will be accessible through Zenodo repository, project website, and partner's open-access repositories, described above. The accessibility capability will be continued after the completion of the project through the Zenodo repository as well as the partner's open-access repositories.

For the data which cannot be openly shared, the reasons will be clearly stated and these data will be preserved in a repository in the project's Confluence site with limited access and not appear in the website of the project.

1.5 SUMMARY

A summary of the iNGENIOUS compliance with FAIR data management protocols is given in Table 2.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Principle	iNGENIOUS DMP
Findable Data	INGENIOUS_[Name]_[Type]_[Date]_[Owner] INGENIOUS_[Name]_[Type]_[Date]_[Owner]_METADATA
Accessible Data	website: https://ingenious-iot.eu Zenodo community: ingenious_iot Institutional repositories[ii]
Interoperable Data	fully documented commentary on the data produced
Reusable Data	Zenodo community: ingenious_iot (public access) iNGENIOUS Confluence site (restricted access) Institutional repositories[iii]

TABLE 2: iNGENIOUS COMPLIANCE WITH THE FAIR PRINCIPLES.

[ii] Partner repositories will host those publications which are authored/co-authored by members of the hosting institution.

Co-funded by the Horizon 2020 Framework Programme of the European Union

2 DATA ETHICS AND SECURITY

Details about data ethics and security including the project’s DPO and GDPR compliance can be found in deliverable D7.4. As stated in D7.4, the iNGENIOUS project does not foresee the collection of any personal data on external users for any use case or proof of concepts. However, in case any data will be collected, it will be done in accordance with EU regulations and according to the minimisation principle in Article 5(1)(c) of the GDPR and Article 4(1)(c) of Regulation (EU) 2018/1725, which provide that personal data must be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’.

Co-funded by the Horizon 2020
Framework Programme of the European Union

3 INTELLECTUAL PROPERTY RIGHTS

This section contains information regarding the management plan for Intellectual Property Rights or IPR(s). To this end, the IPR types, the IPR generation process and the management of background and foreground IPRs catalogue in iNGENIOUS project, in accordance with the H2020 Grant Agreement and project CA, is described.

IPRs include patents, patent applications and other statutory rights in inventions; copyrights (including without limitation copyrights in Software); registered design rights, applications for registered design rights, unregistered design rights and other statutory rights in designs; and other similar or equivalent forms of statutory protection, wherever in the world arising or available, but excluding rights in Confidential Information and/or trade secrets.

All the confidential data and IPR will be stored in a secure centralized server repository, where partners will share technical documents and data obtained from the research and testing throughout the iNGENIOUS project. WP7 is tasked to ensure that the IPR and data management strategies are well defined and coherently executed while PMT will perform the monitoring of the IPR activities and IPR work. The activity of Innovation Elements (IE) generation that can lead to IPR(s) will be actively monitored in Task 7.2. A foreground catalogue will be kept to document relevant information of each determined IE, including:

- IE id
- IE description
- IE type
- Work item(s) where IE is generated
- Background IP elements (by partner)
- Foreground IP element associated
- Partners involved
- Patent(S)
- Ownership
- Access conditions
  This catalogue will be accessible by partners in project’s Task 7.2 Confluence pages. In addition, standardization and exploitation activities may include foreground IP elements that are contributing to each specific standardization activity and to each market opportunity, respectively. Therefore, the relevant foreground IP elements will also be documented within the standardization and exploitation catalogues in the respective Task 7.2 Confluence pages.

Co-funded by the Horizon 2020
Framework Programme of the European Union

4 DETAILED DATA CATALOGUE

This section contains the data catalogue for each use case and proof of concept as a first step to ensuring the proper infrastructure is in place for compliance to the DMP. The data catalogue includes all data sets containing personal information, and in case personal data are involved, detailed information on the technical procedures for data collection, storage, protection, retention, and destruction. As the project progresses, the catalogue will be updated to include any new handling of data within the project.

Co-funded by the Horizon 2020
Framework Programme of the European Union

4.1 UC: Automated robots with heterogeneous networks (Industrial IoT)

PoC: Tactile Internet and integration with IoT networks supporting Software Defined communications (SD-PHY, SD-MAC and SDN) and adaptive networking	
Type of data	• Videos will be captured mainly to perform object detection at the MEC • Sensor data will be collected and send to the control function • Commands for steering the AGV and controlling the robot arm • Status information will be delivered to the remote operators o AGV location o Environment status (temperature, pressure, humidity) o Surveillance data to update virtual/real scene • Network statistics (e.g. packet loss, SNR) • Measurement data collected in trials
Data collection (methods, standards used)	Data collection is performed by the involved IoT devices in the PoC, such as cameras, and environmental sensors. Localization information and statistical information will be collected from network functions. Some data will be generated from applications, such as control commands.
Documentation available	Most of the data format depends on the involved commercial devices that are documented by the manufacturers. Customized data format created within the use case will be gradually documented for internal use.
Storage and backup	Some of the data will be stored for a short term to perform offline performance analysis or to be used for ML training. No personal data will be stored.
Access and security	Network measurement data will be shared with partners in Work Package 3 and Work Package 4.
Ethical issues	None.
IPRs (data ownership, licensing, etc.)	None.
Planned use (documentation, validation, analytics, etc.)	Some data will be used for research and analysis purposes within the period of the project.
Data sharing (public, partners only, selected personal, etc.)	Partners only.
Preservation (delete-after-project, archive, etc.)	Delete-after-project

TABLE 3: DATA CATALOGUE: AUTOMATED ROBOTS WITH HETEROGENEOUS NETWORKS (INDUSTRIAL IOT)

Co-funded by the Horizon 2020
Framework Programme of the European Union

4.2 UC: Transportation Platform Health Monitoring

Type of data	• GPS Positioning Data (Railway Freight Carriages) • Speed Data (Railway Freight Carriages) • Loading Condition (Railway Freight Carriages) • Vibro-Acoustic Data – Wheels & Bearings
Data collection (methods, standards used)	Data collection is done by GMS connected edge devices and data edge loggers
Documentation available	Measurement data is stored binary or hex. COM data is TLS1.2 encrypted
Storage and backup	Data will be stored on MMC or SD card or transferred via TLS1.2 to partner middleware
Access and security	Data logging equipment and/or data will be provided to partners upon request
Ethical issues	None.
IPRs (data ownership, licensing, etc.)	The Data is Stakeholder specific and therefore not available for public use.
Planned use (documentation, validation, analytics, etc.)	The data will be used for iNGENIOUS research and analytic purposes.
Data sharing (public, partners only, selected personal, etc.)	Data logging equipment and/or data will be provided to partners upon request with confidentiality obligation.
Preservation (delete-after-project, archive, etc.)	Partners shall delete after iNGENIOUS project completion

TABLE 4: DATA CATALOGUE: TRANSPORTATION PLATFORM HEALTH MONITORING

4.3 UC: Situational Understanding and Predictive Models in Smart Logistics Scenarios

Type of data	Data related to operational processes carried out at the Port of Valencia and the Port of Livorno. In particular, data will include information about the arrival and departure of vessels, identity of vessels, identity of trucks and containers, gate in and gate out events for trucks, meteorological data and potentially, real-time positioning data.
Data collection (methods, standards used)	Data will be collected by FV and CNIT from the existing data sources available at the Port of Valencia (Valenciaport PCS, AIS, PI System OSIsoft, etc.) and the Port of Livorno (TPCS, GTS3, AIS Dispatcher, M2M Platform, VBS, etc.). Most of this data will be extracted and aggregated by DVL and then shared with Cross-DLT by using APIs for the distribution over different DLTs, according to their own capabilities.
Documentation available	The description of all data streams involved in this use case is provided in deliverable D2.1. Some information is also public on https://www.valenciaportpcs.net/portcalls and https://tpcs.tpcs.eu/
Storage and backup	Data will be initially stored in safe local and cloud database storage environments. Subsequently, a set of this data could be stored in Cross-DLT layer for enabling the exchange of data with different DLTs.
Access and security	Data will be initially made accessible to partners involved in the development of this use case under specific agreements of confidentiality and non-disclosure between the owner of the data (Port of Valencia and Port of Livorno) and the recipient when specified. When data is moved to Cross-DLT layer, data accessibility will be restricted to authorized users.
Ethical issues	Personal and sensitive data will be pseudoanonymised before sharing datasets following guidelines provided by GDPR and DPO (deliverable D7.4).
IPRs (data ownership, licensing, etc.)	Data ownership resides in the entities providing the data, in this case both the Port of Valencia and Port of Livorno. External entities with access to these data will only exploit the data for project purposes related to this Use Case and exclusively during the lifetime of the project.
Planned use (documentation, validation, analytics, etc.)	The aforementioned data sets will be used as an input for developing Artificial Intelligence based algorithms in order to optimize Truck Turnaround Times in maritime ports and terminals.
Data sharing (public, partners only, selected personal, etc.)	Data will be only made accessible to partners involved in the development of this use case under specific agreements of confidentiality and non-disclosure between the owner of the data (Port of Valencia and Port of Livorno) and the recipient, when considered private. When data is moved to Cross-DLT layer, data accessibility will be restricted to authorized users.
Preservation (delete-after-project, archive, etc.)	Data will be deleted after the execution of the project and it will not be stored in any open-access repository during the project lifetime.

TABLE 5: DATA CATALOGUE: SITUATIONAL UNDERSTANDING AND PREDICTIVE MODELS IN SMART LOGISTICS SCENARIOS

Co-funded by the Horizon 2020 Framework Programme of the European Union

4.4 UC/PoC: IMPROVE DRIVERS' SAFETY WITH MR AND HAPTIC SOLUTIONS

Type of data	Encoded, compressed and secured digital data transmission in a real-time application. Data involved, · automatic guided vehicles (AGVs) presence (anonymized id & location) · IoT presence (anonymized id & location) · delivering goods (anonymized id & location) · transport routes, topography (secured) · over-the-air (OTA) wirelessly (secured) · over the network to the backhaul (secured) · cockpit´s cams, sensors, immersive gloves, trackbands and actuators (images, description - anonymized id & secured)
Data collection (methods, standards used)	Data collection is mainly given by the IoT devices that are involved in the use case. The collection is made in real-time from e.g. cams and every time interval for e.g. available sensors and actuators (the broadcasting occurs upon actuation/triggering). The data is fetched from the futuristic immersive cockpit´s cameras and presence sensors that are installed in AGVs and its comprised immersive gloves, trackbands and actuators. This data is used only while the trial and final demonstration occurs and not stored thereafter, therefore will comply with the iNGENIOUS data management plan (DMP).
Documentation available	Documentation is not publicly available and instead will be shared only among the involved use case partners. The iNGENIOUS project describes the data format. The IoT platforms that are involved in the use case have proprietary data format but used for internal use only with no documentation publicly available.
Storage and backup	Other than non-personal data is temporarily stored locally and not backed up. It is merely used for the project trial and demonstration and though some data reaches up to the cloud this is in private mode and not open access (publicly available). Any historical data therefore is overridden periodically and erased after final demonstration.
Access and security	Will be performed through the iNGENIOUS DMP authentication & authorization methods
Ethical issues	None. No personal data will be collected specifically for the use case demo since own staff not external people will be used in principle.
IPRs (data ownership, licensing, etc.)	None.
Planned use (documentation, validation, analytics, etc.)	For the trial and final demonstration.
Data sharing (public, partners only, selected personal, etc.)	Partners only.
Preservation (delete-after-project, archive, etc.)	Delete-after-project.

TABLE 6: DATA CATALOGUE: IMPROVE DRIVERS' SAFETY WITH MR AND HAPTIC SOLUTIONS

Co-funded by the Horizon 2020
Framework Programme of the European Union

4.5 UC/PoC: Inter-modal Asset Tracking via IoT and Satellite

Type of data	Data to be obtained by the IoT sensor: • Real-time location of the cargo: Real-time tracking of cargo will be especially relevant at the land and terminal sides (not so relevant at the seaside). This data stream will be provided in real time by an IoT tracking sensor (Sensor 1). • Cargo conditions: Three different IoT sensors (Sensors 2, 3 and 4) will provide information on cargo conditions related to: o Temperature (Sensor 2); o Humidity (Sensor 2); o Movement (Sensor 3); o Vibration (Sensor 4). • Safety conditions: Data related to the container safety will be provided by two different sensors (Sensors 5 and 6): o Stop and bump detection (Sensor 5); o Container door opening (Sensor 6).
Data collection (methods, standards used)	A Smart IoT Gateway collects and process the data, sent by the IoT devices. The collection is made in real-time. The location of the cargo will be provided in real time. The humidity and the temperature of the cargo will be measured every 10 minutes. The movement and vibration of the cargo will be measured constantly. The stop/bump detection and the container door opening will be measured constantly. This data is used only while the trial and final demonstration occur and not stored thereafter, therefore will comply with the iNGENIOUS data management plan (DMP).
Documentation available	Documentation is not publicly available and instead will be shared only among the involved use case partners.
Storage and backup	Other than non-personal data is temporarily stored locally and not backed up. It is merely used for the project trial and demonstration and though some data reaches up to the cloud this is in private mode and not open access (publicly available). Any historical data therefore is overridden periodically and erased after final use case demonstration.
Access and security	It will be performed through the iNGENIOUS DMP authentication & authorization methods.
Ethical issues	None. No personal data will be collected specifically for the use case demo since own staff and not external people will be used in principle.
IPRs (data ownership, licensing, etc.)	None.
Planned use (documentation, validation, analytics, etc.)	For the trial and final demonstration.
Data sharing (public, partners only, selected personal, etc.)	Partners only.
Preservation (delete-after-project, archive, etc.)	Delete-after-project.

TABLE 7: DATA CATALOGUE: INTER-MODAL ASSET TRACKING VIA IOT AND SATELLITE

4.6 UC (PoC): Supply Chain Ecosystem Integration

Type of data	The following data sets are considered as relevant for this use case: - data needed for a proper events' definition, namely Gate-In, Gate-Out, Vessel Arrival and Vessel Departure events; - complementary data produced and stored by cross-DLT layer (e.g. timestamps, DLT's address, user login data); - data related to underlying network used to improve network resources utilization.
Data collection (methods, standards used)	Above mentioned data are expected to be retrieved, aggregated and distributed by means of APIs. Data will be collected mainly by DVL. Data consumers will be allowed then to use these data (e.g. Trust-OS, AI-based module form MANO) through relative APIs.
Documentation available	Additional information is available in D2.1 as well as in D2.2.
Storage and backup	Raw data will be collected and stored within different M2M platforms. DVL will extract these data, aggregating them according to a given data model. Data are then consumed by cross-DLT layer and MANO platform. Cross-DLT layer stores both aggregated data coming from DVL and complementary data needed to keep track of the interaction with different DLTs. Moreover, MANO platform will store network usage data in order to train its algorithm. Two different DBMS are expected to be used.
Access and security	Two access control layers are foreseen. The first one is about Trust-OS access from users side. In this case users roles are defined according to the scope of their access (e.g. Port Authorities). The second one is about DVL access. In this case, for each data consumer (e.g. Trust-OS, AI-module from MANO platform) data access roles are defined in terms of permissions (e.g. read, write, delete, update, etc.).
Ethical issues	Personal data will be pseudoanonimized according to GDPR requirements.
IPRs (data ownership, licensing, etc.)	Data ownership resides in the entities providing the data, in this case both the Port of Valencia and Port of Livorno. External entities with access to these data will only exploit the data for project purposes related to this Use Case and exclusively during the lifetime of the project.
Planned use (documentation, validation, analytics, etc.)	Identified data sets will be used to define events related to sea port and will be distributed (if supported) within different DLTs by means of cross-DLT layer (data will be also stored).
Data sharing (public, partners only, selected personal, etc.)	Data will be made accessible to partners involved in the development of this use case by means of agreements of confidentiality and non-disclosure with the owner of the data, Port of Valencia and Port of Livorno in this case.
Preservation (delete-after-project, archive, etc.)	Data will be deleted after the execution of the project and it will not be stored in any other public repository during the project lifetime.

TABLE 8: DATA CATALOGUE: SUPPLY CHAIN ECOSYSTEM INTEGRATION

5 CONCLUDING REMARKS

This deliverable, the iNGENIOUS Data Management Plan (DMP), has presented the project's action plan pertaining to the data management policy that will be used throughout the span of the project. The document covered the exploitation of public research data generated (and collected) within the project, the dissemination of the scientific results which are created by the project, as well as data ethics and security for sensitive data, and project guidelines for intellectual properties.

This document, an Open Research Data Pilot, will be updated on an as-needed basis until the end of the iNGENIOUS project, and will continue to contain all methods for the handling of project data. Any changes to the Data Management Plan will also be included in the mid-term and final dissemination, standardisation and exploitation reports, D7.2 and D7.3 respectively.

Co-funded by the Horizon 2020
Framework Programme of the European Union

6 REFERENCES

[1] E. Commission, “H2020 Programme Guidelines on FAIR Data Management in Horizon 2020,” 2016.

[2] M. D. M. A. I. e. a. Wilkinson, “The FAIR Guiding Principles for scientific data management and stewardship,” 2016.

[3] CERN, “Zenodoo, general-purpose open-access repository,” 2013. [Online]. Available: zenodoo.org.

Co-funded by the Horizon 2020
Framework Programme of the European Union