H2020 5GASP Project

Grant No. 101016448

D7.2 Data Management Plan

Abstract

The Data Management Plan (DMP) outlines the measures that the project 5GASP has put in place in order to comply with the requirements for participating projects in the Horizon 2020 pilot action on open access to research data. The plan is considering the protection of personal data and business confidential information.

The DMP identifies the requirements for accessing existing datasets that form the basis of the work of the project. Primarily, these datasets are scientific publications of prior art and documentation and specifications from standards bodies. This document covers overarching issues concerning data management. It concerns all qualitative and quantitative data generated by the project. The *Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020, Version 3.2, 21 March 2017*, and *Guidelines on Findable, openly Accessible, Interoperable and Reusable (FAIR) Data Management in Horizon 2020, Version 3.0, 26 July 2016* have been consulted for the creation of the DMP.

Document properties

Document number	D7.2
Document title	D7.2 Data Management Plan
Document responsible	C. Tranoris
Document editor	C. Tranoris, K. Trantzas University of Patras
Editorial team	C. Tranoris, D. Gomes
Target dissemination level	PU
Status of the document	Final
Version	1.0

Document history

Revision	Date	Issued by	Description
0.1	12/5/2021	C.Tranoris, K.Trantzas	Draft ToC
0.2	12/5/2021	D. Gomes	NetApp contributions
0.3	17/5/2021	E. Oproiu	NetApp contributions
1.0r	22/6/2021	T. Ernst, A. S. Muqaddas	Review
1.0	25/6/2021	C.Tranoris	Final document

Document authors

Author names	Organization
C.Tranoris, K.Trantzas	UoP
D. Gomes	ITaV
E. Oproiu	ORO
X. Vasilakos, A. S. Muqaddas	UNIVBRIS
L. Korsic, J. Sterle	ININ
T. Ernst	YoGoKo

Disclaimer

This document has been produced in the context of the 5GASP Project. The research leading to these results has received funding from the European Community's H2020 Programme under grant agreement number 101016448.

All information in this document is provided “as is” and no guarantee or warranty is given that the information is fit for any particular purpose. The reader thereof uses the information at its sole risk and liability.

For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors view.

Contents

List of Figures

No table of figures entries found.

List of Tables

List of Acronyms

3GPP	3rd Generation Partnership Project
5G	Fifth Generation (mobile/cellular networks)
5G PPP	5G Infrastructure Public Private Partnership
ACM	Association for Computing Machinery
API	Application Programming Interface
C-ITS	Cooperative Intelligent Transport Systems
CA	Consortium Agreement
CEN	European Committee for Standardization
CI/CD	Continuous Integration and Continuous Deployment
DMP	Data Management Plan
DOI	Digital Object Identifier
E2E	End-to-end
EC	European Commission
EG	ETSI Guide
eMBB	enhanced Mobile Broadband
EN	European Standard
driveuES	ETSI Standard
ETSI	European Telecommunications Standards Institute
EU	European Union
FAIR	Findable, openly Accessible, Interoperable and Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation
GR	ETSI Group Report
GS	ETSI Group Specification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IS	International Standard
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
mMTC	massive Machine Type Communications
OA	Open Access
OSS	Open Source Software
PPDR	Public Protection and Disarter Relief
SDO	Standards Developing Organisation
SR	ETSI Special Report
TM Forum	TeleManagement Forum
TR	ETSI-Technical Report
TS	ETSI-Technical Specification
URLLC	Ultra-Reliable Low-Latency Communication
VNF	Virtual Network Function

Executive Summary

The Data Management Plan (DMP) outlines the measures that the project 5GASP has put in place in order to comply with the requirements for participating projects in the Horizon 2020 pilot action on open access to research data. The plan is considering the protection of personal data and business confidential information.

The DMP identifies the requirements for accessing existing datasets that form the basis of the work of the project. Primarily these datasets are scientific publications of prior art and documentation and specifications from standards bodies.

Pertaining to the data that the project will produce, the DMP initially identifies the types of datasets that will be outcome of the project, namely: public deliverables, scientific publications, contributions to standards, open source software and datasets obtained externally, e.g. from experimentation with external stakeholders. Additionally, the access control and sharing methodologies are going to be discussed under the scope of security, with the ethical considerations being also a concern of the DMP. For each type of result (dataset) the DMP identifies the quality assurance processes that are relevant for each type of result. In particular, it elaborates the quality process for deliverables, as well as the process for achieving consensus ahead of scientific publications and contributions to standards.

With respect to open source software, the project is planning contributions to existing open source projects and will adhere to the license terms thereof. The project does plan to create its own open source projects or support existing ones.

With respect to datasets from experimentation with stakeholders the DMP outlines the nature of the data that will be collected and how these data will be sanitised. Furthermore, the DMP describes the data backup policy that is implemented for the main data of the project, both during the project execution as well as for the period after the end of the project. Data that will be made publicly available will receive a Digital Object Identifier (DOI) and will be made available through the 5GASP web server for at least 5 years after the end of the project or at https://data.europa.eu/en/about/add-your-open-data-catalogue. The project is planning to publish papers in open access journals as well as in the Open Research Europe publishing platform[1]. In addition, the long-term availability of DOI marked data complies with the related policies of the DOI handling system.

Finally, the DMP discusses Data Copyright and Intellectually Property Rights issues and assigns responsible persons for each type of data identified in the DMP.

The DMP is expected to be a guide throughout the lifetime of the project, with updates in D7.6.x Annual Dissemination Reports [M12/M24/M36] which will contain annual dissemination activity results.

[1] https://open-research-europe.ec.europa.eu/

1 Introduction

5GASP targets the creation of a VNF marketplace for SMEs & start-ups that includes Open Source Software (OSS) examples and building blocks, as well as the incubation of a community of NetApp developers assisted with tools and services that can enable an early validation and/or certification of products and services for 5G. To that extent, we focus on inter-domain use-cases, development of operational tools and procedures (supporting day-to-day testing and validation activities) and security/trust of 3rd party IPR running in our testbeds. 5GASP's main technical objective is therefore to build and operate an Open 5G NFV-based European network of experimental facilities that provides the means for the instantiation of fully softwarised architectures of vertical industries (e.g. automotive, cooperative mobility and PPDR) for testing, validation, and pre-certification, close to a real-life 5G environments.

For this, 5GASP will leverage the latest 5G technologies, including results from previous 5G PPP projects. This approach employs Network Function Virtualization, Network Slicing and a rigorous automated CI/CD process. To ensure realistic scenarios, 5GASP will create and make available an open framework to give verticals, NetApps and peer projects easy access to the 5GASP services, both legally and technically, e.g., via open APIs.

1.1 Objective of this document

Following the guidelines of the EU for open access to scientific knowledge produced within the European funded projects, the members of the 5GASP consortium are establishing mechanisms for allowing open access to their scientific publications, adopting the Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020[2], according to the strategy and plan outlined in this document.

The aim of this Data Management Plan (DMP) is to describe the whole lifecycle of the project results, under the scope of the implementation of the 5GASP project, in a way that all major aspects of the process are covered. Project results can be categorized as:

i) Project deliverables;
ii) Scientific publications;
iii) Contributions to standards;
iv) Open Source Software contributions;
v) Data from experimentation and testing.

Therefore, the main objective of this deliverable is to provide an overview of:

- How and what data was either collected or generated and what its existing formats are;
- The methodology and principles according to which the data was collected/generated;

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

- The conditions under which the data will be shared;
- How data will be preserved and secured.

The 5GASP project will be aligned with the "FAIR"[3] guidelines (Open Research Data pilot by the ERC in Horizon 2020):

- Making data Findable;
- Making data Openly Accessible;
- Making data Interoperable;
- Increase data Re-use.

This means that the manner in which the data owned by the consortium will be shared and become openly accessible to third parties will be determined by the owners themselves, in a way that facilitates their commercial benefits but at the same time complies with the FAIR guidelines of the Horizon 2020 pilot.

If any significant change to the existing datasets or to the relevant guidelines occur, the DPM will be updated accordingly to reflect the actual state of data in every stage of the 5GASP lifetime.

1.2 Organisation of the document

The document is organized in several sections:

- Section 2 presents the requirements for access to existing datasets;
- Section 3 presents the Data management Plan of 5GASP;
- Section 4 discusses how 5GASP data will be made available;
- Section 5 presents the approaches followed by 5GASP for data security;
- Section 6 any addressed ethical issues; and finally
- Section 7 summarizes the Data Management Plan according to FAIR.

[3] Guidelines on FAIR Data Management in Horizon 2020, https://ec.europa.eu/ research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

2 Requirements for access to existing datasets

5GASP builds on existing knowledge that is publicly available from scientific publishers and for most importantly standards organizations: 3GPP, ETSI and IETF.
The following table summarizes the different datasets that are input to the project.

Dataset name	Description of dataset	Owner/Source	Access issues
Scientific publications	Journals, books, conference proceedings, etc.	Publishers such as Springer, IEEE, ACM and others.	Available at a cost based on unit purchase or subscription basis.
Open Access scientific publications	Online open access scientific publications.	Respective copyright holders, such as publishers and authors.	Typically available at no cost on the Internet.
IETF drafts and RFCs	Working documents of the Internet Engineering Task Force.	IETF Trust and the persons identified as the document authors.	Available at no cost on the Internet.
3GPP	3GPP Specifications and Working Drafts of various working areas.	The 3GPP Organizational Partners jointly own copyright on the Technical Specifications and the Technical Reports approved by 3GPP.	Free of charge – published up to four times a year.
TM Forum standards	TM Forum standards and technical reports.	TM Forum	Available at a cost based on unit purchase; free for TM Forum members.
ISO / CEN Standards	ISO International Standards (IS), ISO Technical Report (TR), ISO Committee Draft (CD), etc.	ISO or CEN	Available at a cost based on unit purchase. Draft versions available to delegates registered with national standardization bodies.
ETSI Standards	European Standard (EN), ETSI Standard (ES), ETSI Guide (EG), ETSI Technical Specification (TS), ETSI Technical Report (TR), ETSI	ETSI and authors of working drafts.	Available at no cost on the Internet.

	Special Report (SR), ETSI Group Report (GR), ETSI Group Specification (GS).		Working drafts available for members only. Membership fee depending on type of organization
Open Source Project Repositories and associated Project Sites	Code repositories maintained e.g. on GitHub, Google code and other places.	Depends on Open Source license used.	Typically available at no cost on the Internet.

3 Data Management

The project plans to produce various results such as: public deliverables, scientific publications, contributions to standards, open source software contributions, datasets from experimentation and testing campaigns.

3.1 Public deliverables

The list of public deliverables is included in the Grant agreement of the 5GASP project. 5GASP defined a specific process to assure quality of the produced deliverables.
Deliverables will be published in the project website as they are produced and in accordance to their nature (public/private). Public deliverables will be made available free of charge and in PDF format. Private deliverables will be listed on the website, but their content protected for exclusive use by project partners. Together with the website, deliverables will be available for 5 years or more after the conclusion of the project.

3.2 Scientific publications

A list of planned scientific publications is considered by the 5GASP partners. A list of successful submission is provided online at a dedicated location on the project website and is reported through the EC project management portal. During the project, the Dissemination of Results by one or several Parties, including but not restricted to publications of whatever form (excluding patent applications(s) and other registrations of IPRs), shall be governed by the procedure of the Grant Agreement, i.e. following the Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020.

3.3 Contributions to standards

5GASP aims to contribute to the activities in major international standardization bodies such as 3GPP, ETSI, ISO, CEN and IETF.

Focus areas	Target Standards Developing Organisation (SDO) and groups
Network Slicing	3GPP SA2
Service based architecture	3GPP SA2
5G Service Management	3GPP SA5
5G New Radio	3GPP
Orchestration	ETSI NFV, ETSI ZSM
Edge Computing	ETSI MEC, 3GPP SA2
Testing	ETSI NFV
Cooperative ITS	ISO TC 204 “ITS”, CEN TC 278 “ITS”, CEN TC226 “Road Equipment”, ETSI TC "ITS".
Automotive	ISO TC 22 “Road Vehicle”

Internet technologies	IETF

In general "Contributions" to standards can relate to:

- Proposals for new activities: work items, working, research or study groups, actions, etc;
- Formal support to the creation of a new activity;
- Creation of working drafts, as a baseline document for standardization activity, technical contribution in standards, reviews of standards;
- Provisioning of comments to working drafts;
- Active participation in conference calls or face-to-face meetings, standard drafting teams, working groups, plenary meeting, national standard committees, i.e. verbal commenting.

3.4 Open source software

Concerning, use and contributions to open source initiatives, the consortium will follow strictly the license terms of the open source project in question. Project partners have been working with open source software for many years and are aware of incompatibilities occurring when different open source licenses are combined, with or without own proprietary code. The main open source initiatives considered by 5GASP, for example Openslice, ONAP and OSM, have released their code under exploitation-friendly licenses, such as Apache 2.0. Contributions to the code base of such projects will follow the target license terms.
5GASP NetApp providers aim to offer their solutions as open source under specific licenses and terms that their respective owners will decide according to any existing IPR.

The owner initiates the process determining the distribution terms. To facilitate this process, and in order to easily maintain an overview of open source contributions of 5GASP results, all partners acknowledge that any result submitted to the target software repository will be provided under the corresponding license terms of the open source project. An electronic copy of the license terms is usually available at the hosting repository of each open source project.

5GASP will manage an OSS repository on GitHub that will host eventual forks of OSS, but with a clear objective of contributing back to the main OSS project.

3.5 Datasets from experimentation and testing campaigns

NetApp developers will typically use data from the test and experimentation service provided by the 5GASP testbeds. NetApp developers will typically create data during the usage of the testbed and 5GASP services either directly via NetApps to be run on the testbed, or by attaching entities to the infrastructure that may be used to generate data, e.g. attached databases, user equipment (UE) or sensors, application logs.
The project will facilitate experimentation and testing campaigns of NetApps. These activities will produce and operate on a limited set of datasets, relating to:

- The usage of components and their APIs as developed within the 5GASP project;
- The ressource usage of the testbed infrastructure at the testbeds used for running the NetApps experimentation and testing campaigns;

- Telemetry data provided to NetApps and users by testbed components, i.e. readings from telemetry sensors attached to the testbed or operational performance indicators and configuration parameters of, e.g., base stations or access points or communication link characteristics;
- Data generated by the NetApps developed and deployed as part of the experimentation and testing campaigns.

Access to the 5GASP testbed will be granted on the basis of terms and conditions of the respective testbed owner. In principle, before being granted access to the testbed infrastructure, any NetApp user participant in the experimentation and testing campaigns is made aware of the fact that specific data is collected and what are the terms of use of the collected data.

The terms of use of the 5GASP services will include a waiver statement that gives the 5GASP project and the testbeds sites' operators the right to collect, store and evaluate the gathered data in specified ways. Data ownership always remains with the NetApp developer or experimenter. Data related to the infrastructure validation will be made available in full or partially, subject to constrains specified by the testbed site operator and involved partners.

The documentation of 5GASP services and APIs will be publicly available, where the external developers can get access to the required information. This information will be typically part of 5GASP public deliverables in the form of aggregates and statistical information.

Production logs of the 5GASP platform and testbed constitute also an interesting source of information for researchers and dataset with anonymized information will be created containing this information. Such dataset will be released through our project webpage and eventually submitted to public repositories such as data.europa.eu.

3.5.1 Handling of research data

Data generated and collected as part of experimentation and testing campaigns are subject to sanitisation under the following considerations that define the framework for the 5GASP policy hereto. It includes provisions in case data privacy and data confidentiality is affected. Specifically, data that contain privacy related information, commercially sensitive data, or data that provide a business competitive advantage, will be excluded from the Open Research Data policy of the project. The project will use open access repositories for storing data that fall under the project's open research data policy. In parallel the data assets will be available through the project's website for the period specified in Section 4.

Third-party customer data resulting from experimentation of NetApps will be treated as confidential by default and the responsibility to consider the openness of these data will be left to the NetApp owners/experimenters that will use the 5GASP services. The NetApp owners/experimenters will be asked to decide whether to: (a) retain data confidentiality for intellectual property rights or privacy reasons; (b) manage their open data through their policy; and (c) adopt the policy of 5GASP and use the same policy and open data store.

The management of open data is based on the following principles:

What standards will be applied?

The project will not define a new data model for the data-generating functions. It will re-use existing industry standard models and formats to ensure interoperability. This approach will ensure usability and comparability of research-result data across all pre-production and research facilities.

How will data be exploited and/or shared/made accessible for verification and reuse? If data cannot be made available, why?

Result data will be available in open repositories. NetApp owners/experimenters of the facility have the option to fully or partially opt-out of the obligation to publish its data.

How will data be curated and preserved?

The project will make data assets available through the project's website for the period specified in Section 4. In addition, source code repositories will host the source code artifacts.

Reflect the current state of consortium agreements on data management (be consistent with exploitation and Intellectual Property Rights (IPR) requirements).

The project participants have agreed not to opt-out the Open Research Data pilot, subject to data specified in the DMP that will be excluded.

3.6 Formats of Datasets

The following table depicts the data types and their respective formats.

Table 1 Formats of data types.

Data Type	Format
Text, Log files	PDF, docx, pptx, xls, txt, log,
Sensor Data	text, numerical (integer, float, double, long), audio, image
Images	Png, Jpg
Videos	MPEG2, MP4
Audio	MP3,MP4
Software, visualization and analytics	JSON, XML, HTML

3.7 Origin of Data

The following table is showing the origins of various data types.

Origin of Data	Data Type
Consortium partners	Text, images, video, audio, software
NetApp 1 ; vOBU (virtual OnBoard Unit) Data sources: OBU	Sensor data (numerical): latitude, longitude, speed, altitude, climb rate, fuel consumption per 100 Km, C02 emission per Km.

NetApp 2 ; Virtual RSU (virtual RoadSide Unit)	RSUs are sending various types of broadcast messages (SPaT/MAP, CPM, SAM, ...), each message is standardized (ISO, CEN, ETSI) and contains a certificate (IEEE P1609.2) used for authentication and non-repudiation. Data is formatted using ASN.1. None of the message carry personal information but vehicle ownership and location privacy is ensured by the used of pseudonyms that change over time.
NetApp 3 ; ITS station	The ITS station NetApp allows to transfer to the cloud all data types required by C-ITS services. This includes C-ITS messages and also synchronisation of data used by ITS stations to transmit C-ITS messages (LDM content, etc.). Data transmitted to the cloud is secured using IEEE P1609.2 certificates and TLS 1.3.
NetApp 4 ; Multi-domain Migration Data sources: OBU (OnBoard Unit)	Sensor data (numerical): latitude, longitude, speed, altitude, climb rate, fuel consumption per 100 Km, C02 emission per Km.
NetApp 5 ; Vehicle-to-Cloud (V2C) Real-Time Communication	Communication data: timestamp modem_id imei imsi simIdentifier network_type operator rsrp rsrq rssi globalcellid band servingcellid latency_min latency_max latency_mean latency_median latency_quantile_95 loss_rate latitude longitude
NetApp 6 ; *Remote Human Driving*	Video Data: timestamp delay frame_seq jitter
NetApp 7: Efficient MEC Handover	Monitoring data: UE Radio parameters (RSRP, RSRQ, Cell ID, GPS) MEC PoP compute parameters (CPU, RAM utilization) Log file: Event collection of various software components/microservices
NetApp 8 ; PrivacyAnalyzer	This NetApp shall analyse data from User Equipment (UE) employed in the PPDR use-case of the project. The UE shall be carried out by First Reponders, taking part in the PPDR use-case. PrivacyAnalyzer shall use as input data the

	qMON agent logs on the PPDR UE. The input data is in log/XML format and includes various attributes, such as the IMSI of the UE, Radio parameters, IP parameters, etc. as defined by the qMON configuration.
NetApp 9 ; 5G Isolated Operations for Public Safety (5G IOPS)	5G UE performance and monitoring data: RSRP, RSRQ, SINR, Tx Power, band, bandwidth, PCI, Cell ID, MCC MNC, Operator, latitude, longitude, ul/dl speed, RTT, jitter, packet loss, Web download time, Web MOS
NetApp 10 : Vehicle Route Optimizer NetApp	Monitoring data: UE Radio parameters (RSRP, RSRQ, Cell ID, GPS) Sensor data
NetApp 11 ; FIDEGAD	Sensor data (numerical): latitude, longitude, speed, altitude Video Stream UE Radio parameters (RSRP, RSRQ, Cell ID, GPS)
5GASP Community Portal	Text, Images, Video
5GASP TEE	Text (log files)

3.7.1 Documentation, Organisation and Storage

There are different aspects concerning the documentation, organisation and storage of the files. In terms of labelling and organizing data, this will be determined by the NetApp developers or WP leaders' approaches, and some criteria could be the type and time of acquisition of data. Furthermore, some cases will include data analysis and processing but not data handling.

Generated data will be annotated with the following metadata:

- Document Number – Sequencial number assigned by the project coordinator;
- Document Title – Human readable and descriptive of the content of the data collected;
- Document Archiver – Person responsible for the collection and storage of the file
- Target Dissemination Level – Public vs Private;
- Version Number – Semantic version number defined by the Document Archiver;

- Data will be stored in a static repository that also hosts the project website, and preserved in accordance to what is defined in section 4.

4 Data Availability

The 5GASP data storage will be preserved for up to 5 years after 5GASP's completion. Appropriate protocols will be implemented to control the storage period. Furthermore, partners of the consortium commonly store their data by means of physical (non-network attached) local mass storage devices, personal computers, private servers (e.g., project's repository), data centres and cloud-based storage (Microsoft Azure, Amazon Web Services or Google Cloud).

The actual storage of the results is managed by the ITAV technical infrastructure team. Storage and availability of the results will be provided for at least 5 years after the end of the project. This includes:

- Public deliverables (including the project website);
- Any Data from experimentation and testing campaigns;
- Open Source Software (links to public repository, and local copies for backup purposes).

For the following types of results the project will rely on the service of external service providers with respect to the long-term availability of project results:

- Scientific publications;
- Contributions to standards;
- Open Source Software (future versions of evolved components in public repository).

5 Data Security

According to the “Open Access to Scientific Publications and Research Data” guidelines, all participants to the H2020 projects are obliged to take the following measures:

- Data and metadata necessary for the validation of the research outputs and research publications should be immediately stored in the relevant repository of the project. The same applies for any other data or metadata which researchers regard as important to be stored and preserved.
- Any pertinent measure that facilitates the access, inspection, usage, copying and distribution of the data by third parties should be taken.
- Validation techniques and relevant information, such as algorithms and analysis codes, should be made available in every repository necessary, to help with the validation process of the research results.

All the consortium members will have to conform to the General Data Protection Regulation (GDPR) regarding “the protection of natural persons with regard to the processing of personal data and on the free movement of such data”[4]. The major risks regarding the data security are the loss of the data, data leak, data breach, and the access to it and its transmission by unauthorized parties as well as server crashing or cyber-attacks.

The 5GASP members aim to tackle these potential threats and ensure a safe data storage, sharing and management plan by taking one or more of the actions listed below:

- Establish secure access protocols (e.g., multi factor authentication) to the data repositories;
- Set up a data backup mechanism and cloud storage services;
- Follow internal security policies and procedures, applicable to each partner and dataset;
- Perform frequent server maintenance;
- Use robust end-to-end channel encryption and pseudonymization techniques.

[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) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

6 Ethical Issues

In the 5GASP project, no ethical issues are addressed. The partners do not intent to make any use of data which belong to special categories, neither to have children or vulnerable groups as data subjects. Additionally, the vast majority of the partners are not going to collect personal/sensitive data from people who have not given their explicit consent to be part of the project and if anyone does, it is going to be data coming from public sources and that will be used only for communication and dissemination purposes.

7 FAIR Data Management

The FAIR data policy requires that all data generated during a H2020 project has to be Findable, openly Accessible, Interoperable and Reusable (FAIR). The following table summarizes how 5GASP conforms to FAIR policies:

DMP	Action
Data summary	Section 3 specifies the general context for the production of data and the purpose, external datasets that will be used as input and the types of data that are produced.
Making data findable, including provisions for metadata	Section 4 specifies how data will be made discoverable and which mechanisms and standards will be used. More specifically: • (Meta)data should be determined by a worldwide unique and persistent identifier; • Data has to be described by rich metadata; • The identifier of the data it describes is plainly and distinctly contained in the metadata,; • (Meta)data is recorded in a searchable repository.
Data is openly accessible	Section 3 and 4 specifies the data that will be made openly available, as well as how these data will be curated and made available. Data should be accessible: • Through an open, free, and universally implementable identifier protocol, by a data repository. This protocol should permit an authentication and authorization procedure, when required. If access to certain data is restricted, proper justification should be provided; Access to metadata should be possible even when the data is no longer accessible.
Making data interoperable	The collection of data adheres to industry standards as defined by 3GPP, ETSI, ISO, CEN, IEEE and IETF. No proprietary formats are used. More precisely: • The exchange and re-use of the (meta)data among the partners should be assisted by data dictionaries and shared knowledge representation codes for semantic consistency among researchers; • These data dictionaries should abide by the FAIR principles,; • (Meta)data should contain references to further (meta)data.
Data is re-usable	Standards contributions adhere to the terms of the corresponding SDO. Open source contributions adhere to the license terms of the related open source project. Specifically: • Clarifying licensing is needed in order for data to be as much re-usable as possible; • Origin of (meta)data must be precisely mentioned;

	• (Meta)data should conform to domain-relevant community standards.
Allocation of Resources	General resources for curation are part of the project work plan. The budget for dissemination activities will be allocated among the 5GASP members who aim to issue scientific publications. The allocation of these resources should be sufficient to accommodate, at least partially, the requirements of the project for making data FAIR. The costs for data preparation and management will also be part of the project's expenses.
Data security	Section 5 covers security aspects
Ethical aspects	Section 6 covers ethical aspects