Grant Agreement No.: 101095542
Call: HORIZON- HLTH-2022-IND-13
Topic: HORIZON-HLTH-2022-IND-13-01
Type of action: HORIZON-RIA

CYLCOMED

Cyber-security toolbox
for connected medical devices

D1.2 Data Management Plan

Revision: v.1.0

Work package	WP 1
Task	T1.5
Due date	31/05/2023
Submission date	31/05/2023
Deliverable lead	MediaClinics Italia
Version	1.0
Authors	Simone Favrin (MCI, Luca Foracchia (MCI), Marco Mosconi (MCI) Dusko Milojevic (KUL)
Reviewers	Dietmar Frey (CUB), Orhun Utku Aydin (CUB)

Abstract	Data Management Plan for CYLCOMED project. This document presents the data management approach followed, guidelines to collect the data and the data collection itself. It is a first version at a very early stage of the project and will subsequently be updated during the course of the project.
Keywords	DMP

Funded by Horizon Europe Framework Programme of the European Union

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.0	23/05/2023	First issue	MCI
V0.1	29/05/2023	Formatting, executive summary and sec. 2.3 updated	MCI, KUL
V1.0	31/05/2023	Reviewers' comments and suggestions incorporated	CUB, KUL, MCI

Disclaimer

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	DMP	
Dissemination Level		
PU	*Public, fully open (e.g., web)*	**X**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Funded by Horizon Europe Framework Programme of the European Union

Executive summary

CONTENT OF THE DOCUMENT

This document (Data Management Plan - DMP) groups all the relevant information about the data that will be used or collected during the CYLCOMED project.

Due to the complex nature of the CYLCOMED project (involvement of partners with different backgrounds and fields of application, e.g., hospitals and tech companies), common understanding and guidance about data, ethical implication, dissemination, and FAIR principles is provided.

Due to the great variety of data involved in the project, the DMP is structured to collect information about data in sets (group of data that have common characteristics and common management requirements e.g., same origin and purpose), in order to collect information in a more readable and accessible way.

This document will be shared among the project partners and all the contribution to data management regarding their roles and expertise in the project will be tracked and inserted in this document to develop best practices.

A tailored table is created and made available through this document and new data sets are expected to be added following the project development.

The DMP tables' structure itself is borrowed from the EC template [1] and the FAIR principles, with a particular attention to ethical implications.

Real world pilots are the focal point of CYLCOMED project and data are mostly generated and used in this framework.

Some data are sensitive patients' data that are needed for clinical purposes while some data will be needed and managed for cybersecurity aspects.

GENERAL NOTES – DMP REVIEWS

The DMP is a "living document" [2] and not a self-standing document, it will be frequently integrated and updated during the project through various revisions; DMP would be considered final only by the end of the project.

The DMP should be updated every time a set of data is subject to modifications or new data types need to be manipulated. If new data sets are highlighted, a new table shall be created.

Funded by Horizon Europe Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

ATOS	Atos Spain
CFREU	The Charter of Fundamental Rights of the European Union
CUB	Charité – Universitätsmedizin Berlin
CYLCOMED	CYbersecurity tooLbox for COnnected MEdical Devices
D#.#	Deliverable (referred to CYLCOMED proposal)
DMP	Data Management Plan
DPO	Data Protection Officer
ECHR	Convention on Human Rights
ECtHR	European Court of Human Rights
FHUNJ	Fundación para la Investigación Biomédica Hospital Infantil Universitario Niño Jesús
GDPR	General Data Protection Regulation
H2020	Horizon Europe 2020 (projects)
ICU	Intensive Care Units
INOV	Inov - Instituto De Engenharia De Sistemas E Computadores, Inovação
KUL	Katholieke Universiteit Leuven
M#	Month of the project
MAR	Martel GmbH (Associated Entity)
MCI	MediaClinics Italia
OPBG	Ospedale Pediatrico Bambin Gesù
RGB	RGB Medical Devices
SaMD	Software as a Medical Device
WP	Work Package
XLAB	XLAB Razvoj Programske Opreme in Svetovanje

Funded by Horizon Europe Framework Programme of the European Union

1 Generated and collected data

This section describes the CYLCOMED project, the pilots and the CYLCOMED toolbox as currently (M6) defined; it will be enriched with new details during the project development.

1.1 Project overview

CYLCOMED is a research and innovation project that aims to strengthen the cybersecurity of Connected Medical Devices (CMDs), in vitro diagnostic devices (IVDs), and software as medical device (SaMD) to ensure the safety and privacy of patients' data.

The project focuses on addressing the complexity and sophistication of cyber threats that could affect the critical infrastructure of the health sector through developing technologically sovereign and trustworthy cybersecurity methodologies.

The project aims to cover identified risks and gaps, also providing training and awareness measures tailored to the needs of healthcare staff to address the weakest link in the security chain.

The CYLCOMED solution aims to provide recommendations for healthcare entities to drive adoption of new technological advances by hospitals and ensure the right levels of security and privacy protection.

The heterogeneity of healthcare organizational models and healthcare providers' CMD platforms make it necessary to produce a set of organizational and technical recommendations that take into account the diverse data sources and healthcare scenarios where CMDs are used.

The project started on December 1, 2022, and will run for 36 months.

The project will include two different pilots that will generate different sets of data, some needed for the clinical effort, some required by the security measures (e.g. - monitoring logs) that will be used to evaluate the effectiveness of the cybersecurity tool in protecting patient data and ensuring the security of the proposed solutions.

1.2 Pilots generated data description

This section provides a description of the data life cycle starting from an overview of the data journey and the trials in which data are generated.

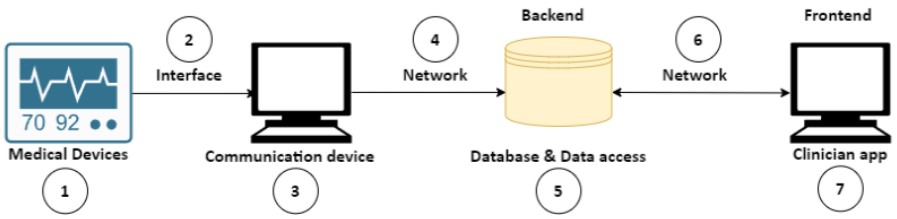

Figure 1: Data journey: general scheme of data generation and transmission (from D3.1 Baseline analysis, requirements and specifications)

Data acquired by the CMDs are transmitted through a communication device and then stored in the backend of the used solution (Figure 1), where they can be analysed. Each step of the data journey can follow different specifications depending on the specific scenario.

Funded by Horizon Europe Framework Programme of the European Union

Generated data can be classified in different categories, due to the nature of CYCLOMED project, particular attention should be paid to patient related data which are normally sensitive data and require additional care compared to technical data.

For CYLCOMED projects, patient related data include, but are not limited to, personal registry, and health-related parameters such as respiratory rate, blood pressure, heart rate, body temperature, Neuromuscular transmission (NMT) data, and blood glucose level.

The non-Patient related data that are generated by the CMDs and that will be recorded (e.g., systems logs) are usually needed to implement security measures (related to privacy and security threats, confidentiality, integrity, and availability of data). The origin of this data can vary: some technical data relate to the integration of the various medical devices and software used in the pilots, some data are related to hardware and software used during the pilot solutions.

1.2.1 Pilot no. 1 - Cyber Security in Hospital Equipment for COVID-19 ICU patients

The first pilot focuses on monitoring and controlling the neuromuscular transmission of COVID-19 ICU patients using NMTCuff technology and the Vision Air multi-parametric monitor with the CYLCOMED security components.

The data is used to establish the correct dosage infusion for each patient, which can vary based on several factors. This pilot will be conducted on a simulated patient, without any real patient involvement. The patient simulation using a computerized model allows for testing and development of the platform before being implemented in real-life situations. The security features developed within CYLCOMED will ensure confidentiality, integrity, availability, and interplay with device safety.

Data used:

- Patient data including medical history, diagnosis, and NMT status
- Neuromuscular transmission (NMT) monitoring data
- Dosage and infusion data

Steps where data is used:

- Monitoring of NMT to establish the correct dosage infusion
- Control of dosage infusion to maintain patient within NMT target limits
- NMT control by Target Control Infusion using NMTCuff technology
- Patient simulation using a computerized model for a digital twin approach

Hardware in Loop/Software in Loop interaction with the Vision Air Monitor and all CYLCOMED security components

1.2.2 Pilot no. 2 - Cybersecurity for Telemedicine Platforms

Pilot no. 2 focuses on the usage of telemedicine platforms to constantly monitor patients and answer specific medical needs. In this scenario we will use CMDs to remotely collect health-related parameters from paediatric cardiac patients that are not on hospital premises.

In this pilot we will use MediaClinics telemedicine platform (MHP) that will collect health-related parameters from patients, including:

Funded by Horizon Europe Framework Programme of the European Union

- ECG
- Blood pressure
- Heart rate
- Respiratory rate
- Body temperature
- Blood glucose

The security of the platform (already certified as a medical device) will be enhanced through the integration of CYLCOMED tools.

In this scenario the data has to guarantee the following properties:

- Accurate and reliable to ensure correct patient monitoring and diagnosis
- Secure and private to protect patient confidentiality and prevent unauthorized access
- Accessible remotely to allow for telemonitoring

1.3 CYLCOMED toolbox and dissemination

Due to the nature of the CYLCOMED project, not only the data itself but also other research outputs (such as the tools that are expected from the project and the dissemination itself) should be collected and managed.

1.3.1 CYLCOMED toolbox - package and methodologies

The main output of the CYLCOMED project is the toolbox itself (deliverables D5.1, D5.2 and D5.3) and the risk evaluation methodologies (D4.1, D4.2, D4.3).

Aspects related to the DMP will be reported in this section in the next reviews.

1.3.2 Dissemination and exploitation

Dissemination is a crucial task for H2020 projects and in CYLCOMED a complete work package is devoted to this purpose.

All the deliverables of this WP are strictly related to the DMP essence and the FAIR principles. The main document that shall be considered is D7.1 “Dissemination, Communication, Standardization and Exploitation Strategy and Plan” where information about research outputs (papers, conferences) are reported.

Funded by Horizon Europe Framework Programme of the European Union

2 Data management forms

This section presents an overview of the structure of the data information forms that are collected in Section 5.

Forms have three different parts that follow the EC guideline [1],[2]: Data summary, where general information about the data usage are provided, a FAIR section in order to collect and maintain all the information about how the data are made available and a final section that summarizes the ethical aspects, including the data protection and security.

2.1 Data summary

The standard DMP structure foresees only a common section for the data summary, but due to the different aspects that are involved in CYLCOMED, this section has been replicated for each data set that has been identified.

This section is meant to summarize general aspects of the data, and in the CYLCOMED framework it is used to describe more in detail the specific dataset, focusing on the origin of the data and the different purpose of collecting these.

We expect to answer the following questions in here:

- What data are we collecting? Name the dataset
- With respect to GDPR, how is this dataset classified? Public, confidential, sensitive, or personal data?
- Why are we collecting it? Which is the purpose of the data collection/generation and which is the relation to the objectives of the project?
- Which is the expected quantity of data that we aim to collect?
- Which is the source of the data? Is the data being re-used from another source?

2.2 FAIR data Principles in CYLCOMED

FAIR data refers to data that is Findable, Accessible, Interoperable, and Reusable. The following section outlines these principles to enable a common description of the data generated in CYLCOMED.

2.2.1 Findable

In order to make data available for further studies, the first requirements is to allow the possibility to search for it and this can be achieved granting some key aspects:

- **Data comes with identifiers**: To make the data findable a unique identifier should be assigned to each acquired entry of the dataset, such identifier must be unique and immutable.
- **Data is searchable**: Each dataset entry should provide some metadata that can be used to restrict the set of entries in the dataset. The metadata may be generated following platform-specific convention, but we should ensure that such information is in a standard machine-readable format (e.g., JSON) to facilitate automated discovery and access to the data.

Funded by Horizon Europe Framework Programme of the European Union

2.2.2 Accessible

For each dataset we shall provide indications on how and under which circumstances we allow access. Accessible data must comply with the following:

- Data is accessible and protected: Accessibility of the data should be determined by the type of data considered, more specifically, access to sensitive data will be limited to authorized healthcare personnel only. A strong authentication process, possibly involving multi-factor authentication, and Role-based access control (RBAC) mechanisms will be implemented to ensure only authorized users have access to the data, and that access is limited to the specific data required for their work. We will comply with all applicable data protection regulations and guidelines, including the EU General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), to protect the privacy and confidentiality of sensitive data.
- The authorization process is documented: If the data is accessible behind authorization, the process to grant access to the dataset must be properly documented, and the documentation must be available to those who may need access.

2.2.3 Interoperable

To ensure interoperability of the data, standard file formats should be used when possible. We will also use standard terminologies to ensure that the data can be easily understood and interpreted by researchers working in the same application domain. To facilitate interoperability, we will also use open APIs (Application Programming Interfaces) to allow authorized users to access the data and integrate it with other applications and systems.

2.2.4 Reusable

For health-related data, given their sensitive nature, it is very unlikely that the data could be used outside the scope of the CYLCOMED project. Anyway, it could be possible to make available some anonymized health data, as well as the technical data.

In addition, data will be provided in a machine-readable format to enable easy integration with other tools and platforms.

Nevertheless, whenever a data can be reused, it shall be ensured that:

- Data is well documented: we will ensure that it is well-documented and properly annotated to enable others to understand and reuse the data in their own research. We will provide detailed documentation about the data, including information about the data collection procedures, data cleaning and preprocessing steps, and any quality control measures that were taken.
- The data format is well defined: we will ensure that the data is available in a machine-readable format to enable easy integration with other tools and platforms. We will also provide data access and sharing guidelines to ensure that the data is used ethically and responsibly, and in compliance with all applicable regulations and guidelines.

Funded by Horizon Europe Framework Programme of the European Union

2.3 Data security and Ethics

2.3.1 Data security

Data security is one of the core topics for CYLCOMED, and therefore its implications are better described and analysed in the outcome of the project.

To ensure the security of the data, appropriate technical and organizational measures will be implemented to protect against unauthorized access, disclosure, or loss of the data.

We will ensure that the data is always transmitted encrypted. Access to the data will be limited to authorized personnel only, and access control mechanisms will be implemented to ensure that only individuals with the appropriate permissions can access the data. We will also implement robust backup and disaster recovery procedures to ensure that the data is protected against accidental loss or destruction. Backups will be stored in secure, off-site locations, and procedures will be in place to ensure that backups are regularly tested and restored to ensure their integrity.

Finally, we will comply with all applicable data protection regulations and guidelines, including the EU General Data Protection Regulation (GDPR) [3], to protect the privacy and confidentiality of patient data. This will include ensuring that all personnel handling the data are trained in data protection and privacy best practices, and that appropriate safeguards are in place to protect against unauthorized access or disclosure of patient data.

2.3.2 Ethics, legal and regulatory aspects

Ethics is regarded as the cornerstone of all projects funded by the European Commission. This can be illustrated through an EC statement which highlights that “ethics is an integral part of research from beginning to end, and ethical compliance is seen as pivotal to achieve real research excellence” [7].

Therefore, all research activities carried out under the CYLCOMED will be conducted in compliance with fundamental ethical principles and legal requirements, that are briefly clarified within this section.

As the rest of the document following project needs and development, this section will be updated during the course of the project.

At the moment it is envisaged that health data of hospital patients will be included in the project.

Rights that are fundamental to CYLCOMED data management

All personal data collected for the CYLCOMED project will be in accordance with the relevant European Union (EU) legal requirements on data protection, in particular the provisions of the General Data Protection Regulation (GDPR) [3] and will take into account the right to privacy and the right to data protection.

The right to privacy is a fundamental human right which can be found in the European Convention on Human Rights (ECHR) [4] as well as in the Charter of Fundamental Rights of the European Union (CFREU) [5] and has been given a broad interpretation by the European Court of Human Rights (ECtHR).

Funded by Horizon Europe Framework Programme of the European Union

While not specifically mentioned in the ECHR[1], the right to data protection is a separate right codified in Art. 8 CFREU. In order not to infringe upon Art. 8 of the CFREU, the personal data must be “processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”. It also states that “everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified” [6].

These requirements are also included in the GDPR. The GDPR defines obligations for controllers and processors of personal data and gives the data subjects certain rights.

Particularly the main concepts that should be followed are described in Art. 5 of GDPR [3] which lays out the principles which must be taken into account when processing personal data; specifically Data must be processed lawfully, fairly and in a transparent manner in relation to the data subject, which includes the obligation to have an appropriate legal ground for processing and to inform the data subject about the processing.

Data collection approach

Data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, though there exist some exceptions on compatible purposes. Moreover, it's imperative that the data remains not only adequate and relevant, but also strictly confined to what is required for the intended processing purposes. Additionally, maintaining data accuracy should be a priority, and if necessary, regular updates should be implemented to ensure its current relevance.

Data should only be kept in a form which permits identification of data subjects for as long as it is necessary for the purposes for which the personal data are processed. Afterwards it must be anonymised or deleted, with possible exceptions in case of processing solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Data usage

Finally, the data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

[1] *But in the court’s interpretation since the end of the 1970s/beginning of the 1980s implicitly included in the right to privacy.*

Funded by Horizon Europe Framework Programme of the European Union

3 Data sets DMP forms

This section will collect all the data informative forms. Here is reported a list of the identified dataset:

Subsec.	Dataset definition	Notes
5.1	Pilot's no.2 Health parameters[2]	Health parameters used to monitor patients in Pilot 2

[2] *This is a first iteration about health parameters collection in Pilot no.2 and it will be updated following pilots' definition.*

Funded by Horizon Europe Framework Programme of the European Union

3.1 Pilot 2 - Health parameters

Data Summary		
Data set	Pilot 2 - Health parameters (ECG, heart rate, …)	
Is data being re-used? (If yes, specify the source)	NO	
Data classification:	Personal data (see 1.2)	
What is the purpose of the data generation:	The data is collected to explore new ways of monitoring the patient outside the hospital premises. More details about the pilot trial can be found in the protocol that each hospital will validate against an Ethical committee.	
What is the expected size of the data that you intend to generate	Each hospital will enroll some patients, and for each of them a total of 3 months' worth of data will be collected.	
What is the origin/provenance of the data	Patients involved in the pilots	
To whom might your data be useful (data utility)	Project partners	
	OPBG	The hospital will collect and use data in the pilot context, clinical staff must be able to visualize this information in order to properly conduct their scientific activity. Each hospital will have access only to the data collected from its own patients.
	FHUNJ	The hospital will collect and use data in the pilot context, clinical staff must be able to visualize this information in order to properly conduct their scientific activity. Each hospital will have access only to the data collected from its own patients.
	CUB	The hospital will collect and use data in the pilot context, clinical staff must be able to visualize this information in order to properly conduct their scientific activity. Each hospital will have access only to the data collected from its own patients.
	Other parties	
	t.b.d.	External stakeholders will be identified during the next stages of the project

Funded by Horizon Europe Framework Programme of the European Union

FAIR principles		
Findable	Identifier is unique and immutable	YES
	Searchable metadata	These field are available for search through API: Type of measure Timestamp Patient identifier (internal to the telemedicine platform)
	Metadata format	application/Json
Accessible	Data access	Due to data sensitivity, access will be limited to authorized healthcare personnel, in accordance with applicable laws and regulations. The data will be stored in a secure server that is accessible only through an authentication process, possibly involving multi-factor authentication. A role-based access control (RBAC) mechanism will be implemented, to limit users' access permission to the specific data required for their work. We will also ensure that access to the data is audited and monitored to prevent and detect unauthorized access or use.
	Documentation	Appropriate documentation will be provided to help authorized users understand the data and how to use it.
	Data Protection	We will provide patients with clear and transparent information about how their data is used, processed, and obtain their informed consent to participate in the study. Patient's data will be treated in compliance with current regulations, including the EU General Data Protection Regulation (GDPR).
Interoperable	Data Standardization	We will store measurements in machine-readable format (JSON) and we will use standard clinical terminologies. Unit of measurement will be stored together with the value.
	Data Exposure	Data will be exposed using REST APIs (Application Programming Interfaces) to allow authorized users to access the data and integrate it with other applications and systems. Healthcare providers, for instance, could be able to use the data in their electronic health records (EHRs) and other clinical systems. Each access to the data will be traced and available for further inspections.
Reusable	Data documentation	Health parameter data type will be documented using the OpenAPI standard, which will be reachable only to authorized users upon request.
	Data format	The underlying data format is application/Json, for some health parameter we support export in standard formats, in particular: ECG can be exported in SCP format

Funded by Horizon Europe Framework Programme of the European Union

Data security and Ethics	
Data security	At the beginning of the project, data security is granted through standard protection measures such as restricted access via authentication, and data encryption at rest through proper database configuration. During the project we expect to improve beyond state of the art thanks to the CYLCOMED contributions.
Ethics	For personal and health data, a review of ethical requirements is performed both by WP2 and by the Ethics Committee of the hospitals involved. The approved trial protocols will be inserted as attachments to this document.

Funded by Horizon Europe Framework Programme of the European Union

Conclusions

As this version of the DMP, it is still at an early stage. It gives an overview of the current approaches of the partners and will be used as a start to further define the data management processes of the project.

Since the DMP is intended to be a living document, it will be updated internally during the course of the project

Scheduled revisions

The very next revision should incorporate the updated information about pilots (D6.1), requirements (D3.1) and ethical frameworks (D2.1) that are expected before the first year of the project (M12, M9, and M9 respectively).

Funded by Horizon Europe Framework Programme of the European Union

References

[1] Regulation (EU) 2016/679 (General Data Protection Regulation)

[2] EU Grants: Data Management Template (HE): V1.0 – 05.05.2021

[3] 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), OJ L 119, 4.5.2016.

[4] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950

[5] Charter of Fundamental Rights of the European Union, OJ C 202/2, 7.6.2016, p. 389-405.

[6] Article 8, 2 of the Charter of Fundamental Rights of the European Union.

[7] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm

Funded by Horizon Europe Framework Programme of the European Union

Appendix A

This table will serve as a template for the analysis of FAIR data within the CYLCOMED project. For each data type generated during the project involved partners shall fill in a copy of this table.

New Dataset form - template

Data Summary		
Data set	Pilot 2 - Health parameters (ECG, heart rate, …)	
Is the data being re-used from another project / source?	*NO / YES if this data is coming from another project / source please describe the source and why we are using it.*	
Data classification:	*Personal / Technical data (see 1.2)*	
What is the purpose of data generation?	*Why do we collect this type of data?*	
What is the expected size of the data that you intend to generate?	*Give an approximate quantification, it could be related to the number of patients (e.g., we expect to collect X measures for each patient every day, and the study will end in a month)*	
What is the origin/provenance of the data?	*From whom or what are we collecting/generating the data*	
To whom might your data be useful (data utility)	Project partners	
	Others (*External entity)*	
		Why does it need access to this data?

Funded by Horizon Europe Framework Programme of the European Union

FAIR principles		
F*indable*	Identifiers are unique and immutable.	*YES / NO if not, please explain why.*
	Searchable metadata	*Metadata provided for the given datatype.*
	Metadata Format	*Format of metadata (e.g., application/Json)*
A*ccessible*	Data access	*Describe accessibility of the data, specifying if restriction.*
	Documentation	*Describe the documentation provided together with the data, and how it is supposed to help the user in data consumption.*
	Data Protection	*Describe compliance with regulations such as GDPR and how end-users (if any) will be informed before data collection.*
I*nteroperable*	Data Standardization	*Is any standard being used? Is the terminology in line with domain standards?*
	Data Exposure	*How the data will be made accessible to other systems (if possible).*
R*eusable*	Data documentation	*Describe how the data will be documented, and how to access such documentation.*
	Data format	*Describe the data format if any standard is used, refer to it. This field should be compiled using the MediaType notation (rfc6838).*

Data security and Ethics	
Data security	Any relevant information about how we protect this data.
Ethics	Any relevant information about the possible ethical issues related to this data.

Funded by Horizon Europe Framework Programme of the European Union