D1.4 Data Management Plan

ENCRYPT: A scalable and practical privacy-preserving framework

Date: 21/12/2022

Lead Partner: EXUS

Doc. Version: 1.0

Document Control Information

Settings	Value
Document Title:	Data Management Plan
Deliverable Identifier:	D1.4
Project Title:	ENCRYPT: A scalable and practical privacy-preserving framework
Document Author(s):	Giannis Lazarou (EXUS) Sotiris Diamantopoulos (EXUS)
Project Manager:	Giannis LAZAROU (EXUS)
Doc. Version:	1.0
Dissemination Level[1]:	PU
Nature:	DMT
Delivery Date:	21/12/2022
Due Date:	31/12/2022

Document Approver(s) and Reviewer(s):

NOTE: All Approvers are required. Records of each approver must be maintained. All Reviewers in the list are considered required unless explicitly listed as Optional.

Name	Role	Action	Date
Irene Kamara [TIU]	Reviewer/ Ethics Manager	Review	15/12/2022
Salvatore D' Antonio [TRUSTUP]	Reviewer/ Technical Manager	Review	16/12/2022
Giannis Lazarou [EXUS]	Project Coordination Team/ Quality Manager	Approve	20/21/2022

[1] **PU**=Public, **CO**=Confidential, only for members of the consortium (including the Commission Services), **CI**=Classified, as referred to in Commission Decision 2001/844/EC

Document history:

Changes to this document are summarized in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Short Description of Changes
8	20/12/2021	Giannis Lazarou	DMP ready
7	19/12/2021	Giannis Lazarou Sotiris Diamantopoulos	Final Integration and Quality Check
6	15/12/2021	Salvatore D' Antonio Irene Kamara	Reviewer comments added
5	6/12/2021	Giannis Lazarou Sotiris Diamantopoulos	All sections compiled, ready for review
4	05/12/2021	All Partners	Tables and figures by collecting data from all partners
3	15/11/2021	Giannis Lazarou Sotiris Diamantopoulos	Section 2 and 3 main content
2	10/11/2021	Giannis Lazarou	Section for FAIR data
1	1/11/2021	Giannis Lazarou	Table Of Contents (ToC)

Configuration Management: Document Location

The latest version of this controlled document is stored in the ENCRYPT SharePoint Repository (ENCRYPT_D1.4.docx).

Table of Contents

LIST OF FIGURES

LIST OF TABLES

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

EXECUTIVE SUMMARY

The document provides an initial data management plan concerning the data processed, generated and preserved during and after the duration of the ENCRYPT project, as well as relative concerns generated from their usage. The deliverable aims to define a framework outlining the ENCRYPT project policy for data management. In particular, this deliverable covers topics like information about the data, metadata content and format, policies for access, sharing and re-use and long-term storage and data management. During the ENCRYPT project, the data management plan will be affected by future results of the work performed in all technical WPs. Therefore, the initial framework presented in this deliverable will further evolve during the project lifetime as a living document.

1. INTRODUCTION

The document provides an initial data management plan concerning the data processed, generated and preserved during and after the ENCRYPT project, as well as relative concerns generated from their usage. The deliverable aims to define a framework outlining the ENCRYPT project policy for data management. In particular, this deliverable covers topics like information about the data, metadata content and format, policies for access, sharing and re-use and long-term storage and data management, as well as personal data protection. This deliverable is considered as a "living" document and it is strongly linked with the work taking place in the Action's Work Packages.

1.1. Background

Deliverable D1.4 - *Data Management Plan* is part of Work Package (WP) 1 "Project Coordination and Cross-Cutting Activities" and reports on the activities concerning Task T1.6 covering the time period till M06. It is the first version of the Data Management Plan, while updated versions will be included in the Project's annual periodic reports.

1.2. Purpose and Scope

The deliverable aims to define a framework outlining the ENCRYPT project policy for data management and it is based on the guidance provided in "Guidelines on Data Management in Horizon 2020" published by the European Commission and aims to answer the following issues:

- *What types of data will the Action generate/collect?*
- *What standards will be used?*
- *How will this data be exploited and/or shared/made accessible for verification and re-use?*
- *How will this data be curated and preserved?*

As mentioned above, the document is dynamic and will be periodically updated in parallel with the development work taking place in other WPs. Overall, a common policy will be defined indicating the procedures for the data management during and after the Action, as well as at internal and external level.

1.3. Structure of the Document

The structure of the document is as follows:

- **Section 1** provides the deliverable's background, purpose and scope giving its overall structure
- **Section 2** describes the ENCRYPT Data management Plan in a glance, providing insights on the foreseen ENCRYPT data nature to be used/generated within the project;
- **Section 3** details the processes to be followed for the participation of the project in OperAIRE Open Research Data Pilot
- **Section 4** includes a description of the FAIR principles to be followed for the data used and generated throughout the duration of the project.
- **Section 5** refers to the resources needed for the ENCRYPT data collection and Management process.
- **Section 6** entails the data security insurance procedures to be followed in ENCRYPT
- **Section 7** comments on the Ethical aspects to be considered in ENCRYPT during the use of the generated data
- **Section 8** concludes the document
- **Section 9** includes an Annex as a reference of legal EU framework on Data Protection
- **Section 10** includes a template to be used in the project as an Information Notice and Consent form

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

2. ENCRYPT DATA MANAGEMENT PLAN OVERVIEW

According to the H2020 Guidelines on FAIR Data Management that also apply to the current Horizon Europe Framework Program, a Data Management Plan is vital for ensuring that data is adequately managed. To this end, we begin this section by identifying the types of artefacts generated and collected as part of the project. A variety of artefacts will be collected and generated during the ENCRYPT's project's lifespan, all of which will be listed In Section 3.2. As the project progresses, this list may need to be updated (artefacts added or removed) to reflect any new information.

2.1. Data Management Plan in Horizon Europe

According to the European Commission (EC) all project proposals submitted to "Research and Innovation actions", "Innovation actions" and "Coordination support actions" have to include a section on research data management which is evaluated under the criterion 'Impact'. Projects participating in the pilot action on open access to research data have to develop a DMP to specify what data will be open[2].

The DMP is defined as:

> *"Data Management Plans (DMPs) are a key element of good data management. A DMP describes the data management life cycle for the data to be collected, processed and/or generated by a Horizon 2020 project. The use of a Data Management Plan is required for projects participating in the Open Research Data Pilot. Other projects are invited to submit a Data Management Plan if relevant for their planned research."*

The purpose of a DMP is to provide a discussion of the main elements of the data management policy that will be used by the applicants with regard to all the datasets that will be generated by the project.

Overall, having taken into account all relevant principles regarding lawful processing of personal data, scientific research data should be easily discoverable, accessible, assessable and intelligible, useable beyond the original purpose for which it was collected and interoperable to specific quality standards.

The ENCRYPT Data Management also follows the Guidelines on FAIR Data Management in Horizon 2020, released by the European Commission Directorate – General for Research & Innovation. This Horizon 2020 FAIR DMP template has been designed to be applicable to any Horizon 2020 project that produces, collects or processes research data. According to these guidelines the management and organization of data should be based on four basic principles, which determine how research outputs should be processed so that they can be more easily accessed, understood, exchanged and reused. This means that data must be findable, accessible, interoperable and re-useable, for example by researchers interested in using the data in further research in the field.

These principles precede implementation choices and do not necessarily suggest any specific technology, standard, or implementation-solution. EC provides a Template with the FAIR principle. This template is not intended as a strict technical implementation of the FAIR principles, it is rather inspired by FAIR as a general concept. The template represents the set of questions that someone should answer with a level of detail appropriate to the project.

The European Commission (EC) requires that all project proposals related to "Research and Innovation Actions" (RIA), "Innovation Actions" (IA) and "Coordination and Support Actions (CSA)" incorporate research data management in their activity, which is being evaluated.

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

Furthermore, a Data Management Plan (DMP) is mandatory for projects which are part of the Open Research Data Pilot.

The goal of a DMP is to present the data management policy which will be followed by applicants with respect to the datasets produced by each project. The “Guidelines on FAIR Data Management in Horizon 2020” provide the following definition of a DMP: "Data Management Plans (DMPs) are a key element of good data management. A DMP describes the data management life cycle for the data to be collected, processed and/or generated by a Horizon 2020 project. The use of a Data Management Plan is required for projects participating in the Open Research Data Pilot. Other projects are invited to submit a Data Management Plan if relevant for their planned research."

Regarding the different types of data collected in the ENCRYPT project, the following are included in the project’s Data Management Plan:

Table 1. Type of Data

Type of Data	Description
Research data	Research data is the evidence that underpins all research conclusions (except those which are purely theoretical) and includes data that has been collected, observed, generated, created or obtained from commercial, government or other sources for subsequent analysis and synthesis to produce original research results. These results are then used to produce research papers and submitted for publication.
Open Research Data	Openly accessible research data that can typically be accessed, mined, exploited, reproduced and disseminated, free of charge for the user.
Secondary Data	Secondary data are data that already exist, regardless of the research to be conducted.
Metadata	Metadata is data used to describe other data. It summarizes basic information about data, which can make finding and working with instances of data easier.

In addition to the EU definition, ENCRYPT Data Management adopts the European Commission Directorate-General for Research and Innovation's Guidelines on FAIR Data Management in Horizon 2020. This Horizon 2020 FAIR DMP template was created to accommodate any Horizon 2020 project that generates, collects, or processes research data. The organization and management of data should be built on four key principles, according to these standards, which dictate how research outputs should be presented so that they can be more easily accessed, understood, shared, and re-used (to support, for instance, future studies of researchers working on the same field).

An EU project’s scientific research data should be based on the aforementioned guidelines and follow the FAIR Principles: the data should be easily Findable, Accessible, Interoperable and Reusable. The European Commission provides a template which is based on those principles and includes specific questions to be answered on a different level of detail, according to each project. This template identifies the following issues: a) Data Summary, b) FAIR data, c) Allocation of resources, d) Data security, e) Ethical aspects, f) Other issues, g) Further support in developing your DMP.

Each of those issues has its own set of questions which need to be addressed. According to the proposed template, it is not necessary to provide detailed answers to all of the DMP's questions by the project's 6th month; instead, the DMP can be a dynamic document in which information can be made available on a finer granularity level through updates as the project's

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

implementation progresses and when significant changes occur. For ENCRYPT, we are considering the use of online documents for continuous change monitoring and the generation of new interim DMP releases every six months, or whenever a significant change in the plan has occurred.

2.2. ENCRYPT Data Info

In this section we collect and present information regarding the project artefact types, their format, their access right and their size.

2.2.1. *Types and Formats of artefacts generated/collected*

To include the general picture of the various artefacts which are generated in ENCRYPT currently, as well as in the future – we have created a table. The table, presented below, depicts the artefact type, and the research data storage format.

Table 2. Type of Artefacts

Artefact Type	Description	Indicative Format
Research Item	Logs data (CTI Use case), Medical data (Health Use Case), EFS data (FinTech Use Case), Models, Policies, Questionnaires, Deliverables, Papers,	.xls, .xlsx, .csv, .txt, doc., .docx, .pdf, .rdf, .p7m, .dcm
Software	Code, APIs, microservices, libraries, dashboard	
Synthetic dataset		.xls, .xlsx, .csv, .txt, doc., .docx, .pdf, .rdf, .p7m, .dcm

2.2.2. *ENCRYPT Artefacts and Access Rights*

During the first months of the project, we conducted a survey. The input collected from the project partners is provided in the following table.

Table 3. Table of ENCRYPT Artefacts

Partner	Type	Artefact	Publishable/ Non-publishable
EPIBANK	Research item	Clients Data	Non-publishable
EXUS	Software	EFS AI models code	Non-publishable
EXUS	Research item	Conference/Journal paper	Publishable
EXUS	Research item	Questionnaires	Publishable
EXUS	Software	Back-end microservices	Publishable
EXUS	Software	Recommendation Engine	Publishable
EXUS	Research item	EFS Log Files	Non-publishable
CERTH	Research item	CTI Data	Non-publishable
CERTH	Research item	Conference/Journal Paper	Publishable
CERTH	Research item	CTI Extraction Tool Models/ methods, etc.	Publishable
CERTH	Research item	Questionnaires	Publishable

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

AUTH	Research item	Metadata - Knowledge Graphs	Publishable
TRUSTUP	Research item	Conference/Journal paper	Publishable
TRUSTUP	Software	TEE-HE confidential computing	Publishable
TRUSTUP	Research item	Questionnaires	Publishable
UNINA	Research item	Medical Data	Non-publishable
8BELLS	Research item	Internal Server Log Files	Non-publishable
DBC	Research item	Internal Server Log Files	Non-publishable
DBC	Software	Differential Privacy tool	Non-publishable
CEA	Software	HE implementation	Non-publishable
CEA	Research item	Conference/Journal paper	Publishable
UNIMAN	Software	Tornado VM	Publishable
UNIMAN	Research item	Conference/Journal Paper	Publishable
GUF	Research item	MIRACUM medical Data	Non-publishable
UMC-MAINZ	Research item	MIRACUM medical Data	Non-publishable
ENG	Research item	Methodological framework for assessment of PP computation services	Publishable
TIU	Research item	Questionnaires	Publishable
TIU	Research item	Conference/Journal paper	Publishable

2.2.3. *Expected size of the Data*

The ENCRYPT project is expected to generate research datasets, publications, new service proposals, dissemination material etc., but the expected size of the datasets cannot be currently estimated. In any case, this size will be reported in the document by the end of the project.

3. PARTICIPATION TO OPEN RESEARCH DATA PILOT (ORDP) – OPENAIRE

The open access and reuse of the research data initiated by H2020 and currently in Horizon new framework projects is facilitated by the Open Research Data Pilot (ORDP) – OpenAIRE[3] of the EC. Two are the main components which constitute the pilot: a) the development of a Data Management Plan (DMP) and b) the provision of open access to the research data.

A project which participates in the Open Research Data Pilot must follow specific conditions:

- To develop and keep an up-to-date DMP.
- To store the data in a research data repository.
- To make sure that any interested third party can openly access, mine, exploit, reproduce and disseminate the data.

[3] https://www.openaire.eu/

- To include any relevant information and pinpoint - or provide - the tools required to use the raw data in order to validate the research.

The ORDP is applied:

- To the data/metadata which are required to verify findings in scientific publications.
- To other curated and/or raw data/metadata which have been specified in the DMP.

3.1. Publishing Infrastructure for Open Access

The ENCRYPT publications infrastructure consists of a process and some identified publication platforms that provide long-term open access to all publishable, generated or collected results of the project. Furthermore, the implementation of the project will be done in accordance with the applicable regulations at the national and EU level and, especially, with the General Data Protection Regulation (GDPR) protection of personal data.

The process and the platforms to be used are described in the following subsections.

3.1.1. *Publishing Process*

In ENCRYPT we will use a simple process which decides, in a deterministic way, whether an ENCRYPT result must be published. All artefact types created during ENCRYPT are considered as project "results", including white papers, scientific publications, and anonymous data. Through this process, each result is classified as public or non-public. A public result must be published as Open Access, while a non-public result must not be published.

To classify each of the ENCRYPT's result, the questions below must be answered:

Table 4. Questionnaire for classification of Artefacts

Artefact type	Description
Does a result provide significant value to others, or is it necessary to understand a scientific conclusion?	If this question is answered with yes, then the result is classified as being public. If this question is answered with no, the result is classified as non-public. Such a result could be code that is very specific to the ENCRYPT platform (e.g., a database initialization), which is usually of no scientific interest to anyone, nor does it add any significant contribution.
Does a result include personal information that is not the author's name?	If this question is answered with yes, the result is classified as non-public. Personal information beyond the name must be removed if it should be published. This also bears witness to the repetitive nature of the publishing process, where results that are deemed in the beginning as non-publishable can become publishable once privacy-related information is removed from them.
Does a result allow the identification of individuals even without the name?	If this question is answered with yes, the result is classified as non-public. Sometimes data inference can be used to superimpose different user data and reveal indirectly a single user's identity. As such, in order to make a result publishable, the included information must be reduced to a level where single individuals cannot be identified. This can be performed by using established anonymization

	techniques to conceal a single user's identity, e.g., abstraction, dummy users, or non-intersecting features.
Does a result include any business or trade secrets of one or more partners of ENCRYPT?	If this question is answered with yes, the result is classified as non-public, except if the opposite is explicitly stated by the involved partners. Business or trade secrets need to be removed in accordance with all partners' requirements before the result can be published.
Does a result name technology that is part of an ongoing, project-related patent application?	If this question is answered with yes, then the result is classified as non-public. Of course, results can be published after the patent has been filed.
Can a result be abused for a purpose that is undesired by society in general or contradicts societal norms and ENCRYPT's ethics?	If this question is answered with yes, the result is classified as non-public.
Does a result break national security interests for any project partner?	If this question is answered with yes, the result is classified as non-public.

3.1.2. *Publishing Platforms*

Various platforms are used in ENCRYPT to support the open publication of our results. The next list presents the platforms chosen by the project and details their general concepts regarding publishing, storage and backup actions.

3.1.2.1. Project Website

The partners in the project consortium decided early to setup a project-related website. This website describes the mission and the general approach of ENCRYPT and its development status. Later in the project, the developed ENCRYPT platform will be announced, while the dedicated area for downloads (called "Findings") provides access to published deliverables and publications (in pre-camera ready form, or through links to the publisher's websites in case these are not open access). All documents will be published using the portable document format (PDF) and downloads are enriched by using simple metadata information, such as the title and the type of the document. All webpage-related data is backed up on a regular basis. All information on the project website can be accessed without creating an account. The website includes a data protection notice.

3.1.2.2. Zenodo Website

Zenodo is a research data archive / online repository that helps researchers share research results in a wide variety of formats for all fields of science. It was created through EC's OpenAIRE+ project and is now hosted at CERN using one of Europe's most reliable hardware infrastructures, with data being backed nightly and replicated to different locations. Zenodo supports the publication of scientific papers or white papers and the publication of any structured research data (e.g., using XML). All uploaded results are structured by using metadata, such as the contributors' names, keywords, date, location, kind of document, license, and others. Considering the language of textual metadata items, English is preferred. All metadata is licensed under CC0 license (Creative Commons 'No Rights Reserved'). The property rights or ownership of a result does not change by uploading it to Zenodo.

3.1.2.3. arXiv

arXiv is an open research-sharing platform that currently hosts more than two million scholarly articles in eight subject areas and offers researchers a broad range of services, like article submission, compilation, production, retrieval, search and discovery, web distribution for human readers, and API access for machines, together with content curation and preservation.

It is maintained and operated by Cornell Tech and the fields of physics, mathematics, computer science, quantitative biology, quantitative finance, statistics, electrical engineering and systems science, and economics.

3.1.2.4. Open Access Repositories and Directory of Open Access Repositories

Project members will also be offered the option of publishing in journals contained/registered in the Registry of Open Access Repositories (ROAR) and/or the Directory of Open Access Repositories (OpenDOAR).

3.1.2.5. Github/Gitlab

Github and GitLab are online repositories that support distributed source code development, management, and revision control. Many open-source projects use GitLab and Github to share their results for free. They use metadata like contributors' nicknames, keywords, time, and data file types to structure the projects and their results.

Based on the code development and integration decisions, source-code components implemented during this project and decided to be public will be uploaded with open access on one of these online repositories.

4. FAIR DATA

ENCRYPT supports the re-use of research data and follows FAIR principles, a set of guidelines for making data Findable, Accessible, Interoperable, and Re-usable. The quality of research data must be such, that the data can be made accessible, findable and re-usable. The following definitions are provided for each individual FAIR principle:

- **Findable:** the data has a unique, persistent ID, located in a searchable resource, and is supported by meaningful metadata.
- **Accessible:** the data is readily and openly retrievable by utilizing common methods and protocols; additionally, the metadata is accessible even when the data is not.
- **Interoperable:** the data is presented in widely accepted standardized formats, vocabularies, and languages.
- **Re-useable:** the data has clear licenses and accurate, meaningful metadata which conform to relevant community standards and identify its content and provenance.

4.1. Making Data Findable, including provisions for metadata

This document launches the data management plan to support the effective collection and integration of the ENCRYPT relevant data. Storage, processing and sharing (among project participants) will occur via data exchange platforms (such as Microsoft SharePoint). Data will be accessible even following the end of the project for 2 years. In contrast, interaction with the broader public will be achieved through the official project website.

For making the data findable, **a naming convention** will be used; this will include a concise description of contents, the host institution collecting the data and the month of publication.

Version numbering will only be an issue if a participant requests withdrawal of their data in which case a version number will be added to the filename.

No specific standards or metadata have been identified for the time being for the proposed datasets.

For all the ENCRYPT Use Cases, the sensitive data of individuals to be used by the technical consortium partners in order to feed their technical software tools will be pseudonymized by the data providers of the consortium and will comply with GDPR, meaning that data will not identify any individuals, and therefore real names of participants will NOT be distributed.

Data will be shared only in relation to publications (deliverables and papers). As such, the publication will serve as the main piece of metadata for the shared data. When this is not seen as being adequate for the comprehension of the raw data, a report will be shared along with the data explaining their meaning and methods of acquisition.

4.1.1. *Discoverability of the data*

It is critical to combine data from participants in the open calls, as well as the project partners' activities, to utilize the project-generated data. By considering the FAIR data principles[4], we specify that data/metadata must conform to the following requirements:

- The (meta)data must be assigned a globally unique and persistent identifier.
- Enough metadata must be included, so that the data can be fully interpreted.
- The data must be indexed in a searchable source.

The application of these principles and inclusion of their authentication and authorization details will result in the data becoming retrievable.

4.1.2. *Data Identification Mechanisms*

Each project-related document will be identified using the project name, along with a unique and persistent document type designator and a number provided to the coordinator for submission to the European Commission. The document version should be included in the document name and title.

Regarding the project activity and deliverable documents, the relevant task or deliverable numbers are going to be utilized for document identification, succeeded by a short activity/deliverable title.

Example

ENCRYPT_D1.4_Data-Management-Plan_v1.0.pdf

4.1.3. *Naming Conventions Used*

The data generated during the project (datasets, technical reports, deliverables etc.) will be named in a uniform fashion and a version control table will be included. The ENCRYPT project document naming recommendations are presented below:

- Easily readable identifier names must be chosen, i.e., brief and meaningful.
- Acronyms with limited acceptance must not be used.
- Abbreviations and/or contractions must not be used.
- Language-specific or non-alphanumeric characters should be avoided.
- A two-digit numeric suffix must be added to identify new document versions.

[4] Wilkinson et al., The FAIR Guiding Principles for scientific data management and stewardship, 2016.

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

- Date follow the YYYYMMDD format. They are stated 'back to front' and use four-digit years.

For deliverables

ENCRYPT_[Deliverable Code]_[Deliverable Title with dashes instead of spaces]_vA.BB i.e.: ENCRYPT _D1.4_Data-Management-Plan_v1.0 (for submission to the Commission)

For datasets

For datasets: WP [Work Package number] P [Partner number] - [description of the activity] i.e.: WP4 P1.X xxxx

4.1.4. *Clear Versioning of the documents*

Documents created by the consortium will be versioned; for this purpose, the deliverable template includes four descriptors (Version, Date, Status, Comments) to identify the versions and status of the documents, as depicted in the figure below.

Table 5. Revision History Table

Version	Date	Created by	Short Description of Changes
x.y	DD/MM/YYY		

Moreover, following the recommendations included in section "Naming conventions", partners will identify the different versions by using a two-digit number following the descriptor Draft. A document reviewed by another partner should be returned to the principal author by including the tag _reviewed_ and the acronym of the organisation. Only the principal author will change the draft number and add the word FINAL to documents ready to be sent to the EC or those to be used as final versions.

4.1.5. *Standards for metadata creation (if any)*

We consider the use of essential metadata, which are going to improve information recall and retrieval by project partners and external evaluators. To achieve this, all project documents are required to include author, editor, Work Package, dissemination level and version information in their front page.

To support metadata completeness, ENCRYPT provides a metadata template to be used by all stakeholders. This template is going to be a continuously-updated document, which can be expanded to fit any new project requirements.

Table 6. Metadata Template for ENCRYPT Datasets

#	Field	Description
1	Title	A name given to the resource.
2	Creator	An entity primarily responsible for making the resource
3	Subject	The topic of the resource
4	Description	e.g., abstract, table of contents, graphics, ...
5	Publisher	Only for published items.
6	Contributor	Entities contributed to the making of the resource.
7	Date	The termination of the data collection period.

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

8	Type	[dataset, article, questionnaire, ...]
9	Format	The file format of the resource.
10	Identifier	e.g., ISSN if item has been published
11	Source	Which tools were used to collect the data
12	Language	A language of the resource.
13	Relation	A related resource.
14	Rights	Information about the rights held in and over the resource.

In addition to the dataset's metadata document, dataset providers are compelled to attach additional documents such as:

- A description of the study
- Method of research
- Applied questionnaires
- Data documentation / usage manual
- Any other information that might be of interest to a data user

The following figures present relevant metadata information as part of the deliverable template.

Settings	Value
Document Title:	Data Management Plan
Deliverable Identifier:	D1.4
Project Title:	ENCRYPT: A scalable and practical privacy-preserving framework
Document Author(s):	Giannis Lazarou (EXUS) Sotiris Diamantopoulos (EXUS)
Project Manager:	Giannis LAZAROU (EXUS)
Doc. Version:	1.0
Dissemination Level[1]:	PU
Nature:	DMT
Delivery Date:	21/12/2022
Due Date:	31/12/2022

Name	Role	Action	Date
Irene Kamara [TIU]	Reviewer/ Ethics Manager	Review	15/12/2022
Salvatore D' Antonio [TRUSTUP]	Reviewer/ Technical Manager	Review	16/12/2022
Giannis Lazarou [EXUS]	Project Coordination Team/ Quality Manager	Approve	20/21/2022

Revision	Date	Created by	Short Description of Changes
8	20/12/2021	Giannis Lazarou	DMP ready
7	19/12/2021	Giannis Lazarou Sotiris Diamantopoulos	Final Integration and Quality Check
6	15/12/2021	Salvatore D' Antonio Irene Kamara	Reviewer comments added
5	6/12/2021	Giannis Lazarou Sotiris Diamantopoulos	All sections compiled, ready for review
4	05/12/2021	All Partners	Tables and figures by collecting data from all partners
3	15/11/2021	Giannis Lazarou Sotiris Diamantopoulos	Section 2 and 3 main content
2	10/11/2021	Giannis Lazarou	Section for FAIR data
1	1/11/2021	Giannis Lazarou	Table Of Contents (ToC)

Figure 1 . Project Documentation related Metadata as part of the Deliverables Template

4.2. Making Data Openly Accessible

Whenever it is feasible, the data will be released with respect to the Ethics, as well as the participant agreement. In the cases that data can be made available, we are going to use the ENCRYPT file repository which is hosted by the project coordinator.

Before any data release, the party requesting that data must reach the Project Coordinator and articulate their intended use of the dataset. The Project Coordinator will then send a "Terms and Conditions" form to that party for signing. Once the form is signed and returned, the dataset will be released, along with the documentation included.

ENCRYPT will follow a mix of Gold and Green Open Access policy for its scientific publications, which will be further specified and agreed upon during the initial months of the project, conforming to the European Commission Guidelines on Open Access Scientific Publications and Research Data in Horizon 2020[5] (see figure below).

[5] European Commission Directorate-General for Research & Innovation (2017) Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

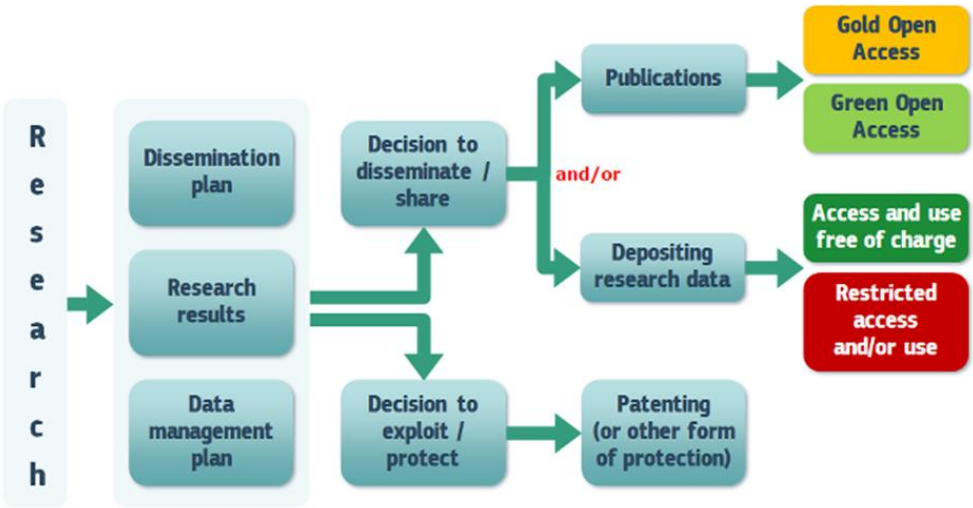

Figure 2. *Access to Research data in the Horizon Programme*

High-impact journal publications will be encouraged to use Gold Access, while the rest of the papers will grant Green Access by self-archiving. The repositories considered will consist of the consortium members' repositories, Zenodo, as well as any repositories listed in OpenDOAR. In addition, there will be a suitable repository on the project's website as well as on social networking sites for scientists and researchers (e.g., ResearchGate).

4.2.1. *Methods or software needed to access the data*

There will be no need for specific software to retrieve and access the ENRYPT data, as the anonymized datasets are going to be stored in common formats (using word, pdf and excel documents) to ease data exploitation and long-term access.

4.2.2. *Deposit of data, associated metadata, documentation and code*

Data will be deposited and secured on the Microsoft SharePoint file repository.

4.3. Making Data Interoperable

Interoperability requires consistency for any used terms throughout all documents and datasets, as well as the use of machine-readable formats by data/metadata.

4.3.1. *Interoperability of data assessment*

It is the duty of each project partner to store the data in an appropriate format, as well as to make any relevant modifications based on the needs of parties interested in using the project data. The current and future level of data interoperability will be assessed in further revisions of the document, to make sure that the ENCRYPT data can fit the needs of specific scenarios (data infrastructures, interests or purpose of data).

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

4.3.2. *Vocabulary use*

The project uses vocabulary which is widely adopted and common within the Security research and privacy preservation methods fields. In this regard, the project vocabulary should not pose any obstacles by itself to data re-use and interoperability.

4.4. Making Data re-usable

For data to be re-usable, it is -generally- considered that meta(data) have a plurality of accurate and relevant attributes and that they are released with a clear and accessible data usage license. Moreover, it is considered that (meta)data are associated with their provenance and that they meet domain-relevant community standards.

Note that the overall management of knowledge and the provisioning for the establishment of the related Intellectual Property Rights is dictated in detail under ENRYPT Grant Agreement and the consortium agreement stipulating -among others- for the ownership of the background and the foreground knowledge, as well as for the commercial exploitation of the project's results.

4.4.1. *Increase data re-use through clarifying licenses*

Some of the data will only be available on the website or Microsoft SharePoint, and their use will be restricted to the research use of the licensee and colleagues on a need-to-know basis. This non-commercial license shall mention that data may not be copied or distributed and must be referenced if used in publications.

4.4.2. *Data quality assurance process*

The project coordinator will be in charge of ensuring data quality by guaranteeing that the dataset adheres to the FAIR principles outlined in this plan and that the data is updated.

Personal data will be processed in accordance with EU, and relevant national regulations, as well as the "data quality" principles outlined below:

- Data processing is adequate, relevant and non-excessive.
- Accurate and kept up to date.
- Processed fairly and lawfully.
- Processed in line with data subjects' rights.
- Processed in a secure manner.
- Kept for no longer that necessary and for the sole purpose of the project.

The data quality assurance process will be guided by the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016 on the protection of natural persons with respect to the processing of personal data and the free movement of such data.

4.4.3. *Length of Time for which the data will remain re-usable*

The Consortium will help to keep data reusable after the project is completed, as long as it is feasible. A three-year baseline period has been set; however, this time can be extended with the written agreement of the partners.

4.5. Artefact Template

The following table will be used to capture the description of the data produced in the context of ENCRYPT.

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

Characteristic	Question/Description
Making data Findable	
Name of data set	Univocal identifier of the considered data [ENCRYPT _Wx_Tz_01]
Data types	[Real time data stream, unstructured like tweets, synthetic data stream, log data, etc.]
Data generation and/or collection	Description of the type of input used to generate the data and the complete methodology and tools used for data collection
Purpose	What is the data collected/generated specifically used for?
Data origin	[Where applicable, information from applications to be developed by the partner.]
Making data Accessible	
Accessibility	Open/Confidential
Repository	Description/location of the available data.
Shareability restrictions / related Information	[Where applicable, information from applications to be developed by the partner.]
Making data Interoperable	
Format	Data format, measuring unit, typical order of magnitude [JSON-like, CSV]
Expected size of the data	[To be defined, per day or in total size]
Standards and metadata	[The metadata attributes list. The used methodologies.]
Standard software Interfaces	List of the standards used to promote results replicability.
Extensions to standard interfaces	Extensions to the above standards as developed during the project.
Making data Re-usable	
RE-use of existing data	[No reuse of existing data, for the generation of synthetic datasets, it will be essential to create a recipe, reusing the existing data in logs etc.]
Data backup	Consistent location of the data, including previous releases
Quality Consistency	Constraints determining the quality/currency of the collected data.
Emulation tools	Description/location of possible emulation tools useful for replicating the data

Every use case and tech partner has been provided with the template, and subsequently, all the input will be collected.

5. Resources for Data Collection and Management in the Scope of ENCRYPT

All project's administration data (deliverables, reports, scientific papers, presentations, teleconference minutes, etc.) will be stored at the Sharepoint collaboration file repository. That data will be kept for 3 years after the end of the project and, if requested, for 2 additional years.

It is the coordinator's responsibility to maintain the repository on behalf of the ENCRYPT consortium, as well as to handle all project-related data management issues.

The scientific publications, in which the empirical data will be presented and analyzed, will be published in Open Access journals. The relevant costs will be covered by the Horizon Europe grant. The storage and compliance of the research data collected during the project will be part of the Task and Work Package leader responsibilities. This also includes the responsibility of uploading the data in the ENCRYPT SharePoint, when project information needs to be shared.

5.1. Data Management Responsibilities

The responsibility for updating the present document lies at the ENCRYPT coordinator, supported by the respective Work Package leaders. This responsibility also includes the development of a relevant strategy to:

- Pinpoint the most appropriate data sharing and data preservation methods.
- Facilitate the efficient use of the data and impose clear rules regarding its accessibility.
- Ensure the high quality of the stored data.
- Guarantee secure data storage.

5.2. Cost of potential value of long-term preservation

No extra funding will be required for data storage and maintenance after the project's completion.

6. Data Security

The ENCRYPT project does not involve activities or results raining security issues nor "EU-classified information" as background or results.

In addition, for data protection reasons, the ENCRYPT data exchange platform (Microsoft SharePoint) applies the following technical and organizational measures against data acquisition and processing by non-authorized entities, against data processing actions which violate the law and against any change, loss, damage or destruction of the specified data. Those measures include:

- **Information security:** Towards this end, the Secure Socket Layer (SSL) protocol is used in conjunction with the appropriate SSL certificates. The account password is going to exist in the platform solely in an encrypted form, to achieve the desired security level.
- **Options for reading data:** The platform provides the option rend the data available in a read-only or downloadable format, prohibiting unauthorized entities from accessing the information.
- **Backup policy:** Auto-backups are performed by Microsoft periodically. Furthermore, each time a document is modified, the previous document version is saved.
- **Accidental deletion/modification:** Previous dataset versions can be restored if the datasets are deleted, either partially or completely, because of a catastrophic event.
- **Data deletion/modification by users:** Administrators are the only ones allowed to modify or delete any information included in the datasets.
- **Terms and conditions:** All users of the platform have to accept the SharePoint terms of use and conditions.

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

7. ETHICAL ASPECTS

The ENCRYPT Partners adhere to ethical rules and comply with European legislation on data protection (Regulation (EU) 2016/679 General Data Protection Regulation[6]), the national legislation applicable in countries where the research will be carried out (see Annex I table), as well as recommendations and codes of conduct relevant to research activities. The CA has included specific agreements with regard to personal data processing.

The ENCRYPT Consortium has not identified any additional specific ethical issues related to the activities of the Project that are not already addressed in the Grant Agreement. Ethical procedures "Data Protection and Ethics of Research Guidelines" have been specified within the project (and disseminated between consortium members) and these procedures will have to be followed in project activities. The surveillance activities using ENCRYPT technologies will be designed and implemented while taking into consideration the dignity of the participants as well as other fundamental rights and freedoms (freedom, non- discrimination, etc.) and core values will be respected (proportionality, minimization, confidentiality) and will conform with the General Data Protection Regulation (EU) 2016/679 ("GDPR").

As national and EU laws and recommendations on privacy and data protection issues play an important role, the design of activities within the ENCRYPT project will involve all partners' engagement in designing, deploying and testing of ENCRYPT, which may raise concerns on data sharing and protection issues. ENCRYPT additionally has a dedicated Ethics and GDPR task (T.1.3) and expertise from within the consortium (TiU). It will also appoint an ethics and data protection expert in the Advisory Board.

The Consortium will consider that for the purposes of the ENCRYPT project the retention period is the one used in the relevant field, by analogy to the administrative and financial issues, this should be 2 years. The Consortium will take into account that in case of a future exploitation of the ENCRYPT, different retention periods may apply, depending on the national legislations.

The project adheres to the commitment to holding any data in secure conditions, and will make every effort to safeguard against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Additionally,

- The Consortium will evaluate a secure storage and transfer system/channel
- Research and other data will be stored in a secure and accessible form.
- The Consortium will specify procedures for keeping data accessible in terms of migration (conversion of data files from older formats to newer ones) and refreshing (transfer of data from one storage tool to another), if needed.
- The Consortium will define procedures for backup and recovery of data.
- Access rights and access conditions will be defined taking into consideration the task allocation and the category/type of data.
- When defining roles and permissions special attention will be paid to the possibility to track any interaction that entails access, modification and deletion of personal data.

Each partner is responsible for informing their own staff involved in the ENCRYPT project, and where relevant Data Protection and Privacy Officers, about the need to comply with the legal principles and provisions with regard to data processing. The Consortium considers all necessary and appropriate measures to mitigate risks, which include:

- The handing over of any data;
- The collection of data and its secure storage and transfer;
- The confidentiality declaration to be signed by staff;

[6] https://ec.europa.eu/info/law/law-topic/data-protection_en

- The process for conducting trials, participant's recruitment and gaining informed consent.

The Consortium will conduct the research and the design/ deployment of ENCRYPT in full respect of the rights of participants (via workshops, events, and interviews) with emphasis on informed consent.

- Templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) - see Template in English in Annex 2

The Participation / Information sheet provided will include (indicatively): contact information, subject and objectives of the research, data collection methods, voluntary nature of participation, confidentiality, and information about the potential reuse of data. The informed consent of the volunteers will include the information sheet and an informed consent form. Research participants (volunteers) will be informed that they may withdraw from the project at any time and they can request that their data be destroyed at any time up until the data have been anonymised (after the participant data has been anonymised it is impossible for the researchers to identify the data associated with the participant requesting withdrawal). Withdrawal from the research happens without participant's having to explain the reasons, and without any repercussions.

8. CONCLUSIONS

The purpose of the Data Management Plan is to support the data management life cycle for all data that will be collected, processed or generated by the ENCRYPT Action. The Data Management Plan is not a fixed document, but evolves during the lifespan of the Action. This document is expected to mature during the Action; more developed versions of the plan will be reported in the project's annual periodic reports. The Data Management Plan will be updated at least by the mid-term and final review to fine-tune it to the data generated and the uses identified by the consortium since not all data or potential uses are clear at this stage of the Action.

9. ANNEX I – REFERENCE LEGAL FRAMEWORK ON DATA PROTECTION

A. The reference legal framework on data protection includes, in chronological order:

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC
- Charter of Fundamental Rights of the European Union (2012/C 326/02), became legally binding on the EU institutions and on national governments on 1 December 2009, with the entry into force of the Treaty of Lisbon.

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) (Text with EEA relevance) *OJ L 119, 4.5.2016, p. 1–88.*

- Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/ JHA, *OJ L 119, 4.5.2016, p. 89–131*
- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union PE/53/2018/REV/, *OJ L 303, 28.11.2018, p. 59–68*
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1, *OJ L 295, 21.11.2018, p. 39–98*

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

B. National Implementations of EU GDPR & National Data Protection Authorities

Partner & country	GDPR National Adaptation Laws	Data Protection authority
Greece: EXUS, AUTH, EPIBANK, CERTH	Law 4624/2019, which entered into force on 29 August 2019. https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html	Hellenic Data Protection Authority https://www.dpa.gr/el/arxi/profile
Cyprus: 8BELLS	Law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data (Law 125(I) of 2018) (the "Data Protection Act") https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf	Office of the Commissioner for Personal Data Protection https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument
Germany: GUF, UMCMAINZ	Federal Data Protection Act, Bundesdatenschutzgesetz, Neufassung 2018 ("BDSG") https://www.gesetze-im-internet.de/englisch_bdsg/index.html	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit https://www.bfdi.bund.de/DE/Home/home_node.html
Belgium: DBC	Law of 5 September 2018 establishing the information security committee and modifying various laws regarding the implementation of 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 http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2018090501	Autorité de protection des données https://www.dataprotectionauthority.be/citizen
The Netherlands: TiU	Uitvoeringswet Algemene Verordening Gegevensbescherming (General Data Protection Regulation Implementation Act) https://wetten.overheid.nl/BWBR0040940/2019-02-19	Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl/en
Italy: ENG, TRUSTUP, UNINA	Legislative Decree No. 101/2018 setting out rules adapting Italian law to the GDPR, which amended Legislative Decree No. 196/2003 setting out the Italian privacy code. https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dat	Garante per la protezione dei dati personali https://www.garanteprivacy.it/web/garant

	aPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true	e-privacy-en/home_en
France: CEA	French Data Protection Act (as amended by the Law No. 2018-493 of 20 June 2018 on the protection of personal data and by the Decree No. 2018-687 of 1 August 2018) (the "FDPA") https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624	Commission Nationale de l'Informatique et des Libertés https://www.cnil.fr/

10. ANNEX II: TEMPLATE INFORMATION NOTICE AND CONSENT FORM

Information notice and Consent Form for Personal Data Processing

Title of the project: ENCRYPT: A scalable and practical privacy-preserving framework

Project aims

The aim of the project is to develop a scalable, practical, adaptable privacy-preserving framework, allowing researchers and developers to process data stored in federated cross-border data spaces in a GDPR-compliant way. The ENCRYPT framework is validated in 3-phases, comprising of i) in-lab validation tests, ii) use cases provided by consortium partners in three sectors, namely the health sector, the cybersecurity sector, and the finance sector, that include cross-border processing of data,and iii) external use cases including privacy preserving computations on federated medical datasets. The following entities participate in the ENCRYPT project ('consortium') 1. Engineering (Italy) 2. CERTH (Greece), 3. 8BELLS (Cyprus), 4. Commissariat A L Energie Atomique Et Aux Energies Alternatives, (France), 5. TRUSTUP (Italy), 6. Aristotle University of Thessaloniki (Greece), 7. DBC (Belgium), 8. Universita Napoli (Italy), 9. EPIBANK (Greece), 10. Universitaet Frankfurt am Main (Germany), 11. Universitaetsmedizin Gutenberg-Universitaet Mainz (Germany).

More information on the project is available on the ENCRYPT project website: https://encrypt-project.eu/

Funding and Responsibility

The ENCRYPT project ('ENCRYPT') is funded by the European Union's Horizon Europe program (Grant Agreement number: 101070670). The project coordinator EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS (EXUS) is the controller of the personal data that is being processed for the purpose of the study.

Information notice and purpose of processing

The (select relevant: interview/workshop/other) will inform and facilitate the research conducted for Work Package (add number and relevant task), which aims at (add WP goal, as stated in Grant Agreement).

You agree to participate, because your (select relevant: expertise/experience) is important to help ENCRYPT (select relevant: refine our initial findings and finalise the recommendations/ validate the ENCRYPT platform/ xx feature/use case/requirements). The interview/workshop/other will be held online/ at (add location), it lasts [add: number of hours] hours and you are invited to discuss your knowledge/experience/expertise.

Participation is voluntary and you may leave the interview/workshop at any point.

The interview/workshop will be recorded via paper notes/ digital recording, and you can request a copy of the notes if you wish.

There are no anticipated risks to participating in ENCRYPT. If, however, the questions the project partner will ask trigger reflection in a way that causes any issues or nuisance, you can ask the researchers for additional support.

For further information or clarifications about the data or the project, you are free to contact [add email of the task leader]

Personal data categories and legal basis

The research team will process your name, role/position at the organization, contact details, signature in this consent form, area of expertise, relevant personal and professional information that you provide during the interview, and in written communication before and after the interview/workshop/other. The basis for processing is your consent (Art. 6(1)(a) Regulation 679/2016).

Retention, and measures to protect your personal data

The data will be stored for a period of [add number of] years, and it will be erased at the end of the storage period. Your personal data will not be subject to automated decision-making procedures. The data will be stored in a secure location in [note to partners: mention in which country/EU] with restricted and granular access conditions in order to prevent unauthorised or unlawful processing, accidental loss, destruction or damage. Only the ENCRYPT partners/ [: or mention the specific partners] will have access to the data.

Disclosure to third parties and further processing

Your personal data will not be processed further, unless you provide explicitly your consent for further processing in the end of this form.

Your personal data provide will not be shared with any other institution other than the ENCRYPT project partners. (note to partners: adapt according to the actual practice)
The data will only be shared with third parties under these conditions with the following safeguards: All information that can identify you as a person will be removed from the data set we work with and be given a code. Only a select group of researchers will have access to this code which will be stored separately and securely.

Your rights as data subject

Right to information (Article 13), Right of access (Art.15 GDPR); Right to rectification (Art. 16 GDPR), Right to erasure ('right to be forgotten', Art. 17 GDPR); Right to restriction of processing (Art. 18 GDPR), Right to data portability (Art. 20 GDPR); Right to object (Art. 21 GDPR).

Consent form:

1. I, the participant, confirm that I have read and understood the participant information for the "ENCRYPT". I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.
2. I understand that my participation to the interview/workshop and to the ENCRYPT project is voluntary and that I am free to withdraw at any time, without giving any reason and without any consequences.

Note: when you withdrawing from ENCRYPT, the project partners will take all reasonable efforts to remove your personal data from the datasets. When results have already been processed in analyses, such removal may no longer be possible.

3. I understand that any information provided by me during written exchange in preparation, during, or following this focus group may be used in future publications, articles or presentations of the researcher and disseminated for scientific purposes, in compliance with the ethical standards of the scientific community.
4. (encircle the answer that applies)
   a. I agree to take part in the above ENCRYPT project activities.

b. If I decide to leave the ENCRYPT project interview/seminar/other, I agree that the ENCRYPT coordinator/[name of partner] can still use the data collected up to this point.
c. If I decide to leave the study, I request complete removal of the data collected up to that point.

5. If "a" has been selected, I (encircle the answer that applies)
a. I accept that my name and my position inside (or outside) the organization under study are mentioned;
b. I prefer to have my name referred to as 'anonymous' and my position in the organisation described as .....(description of position);
c. prefer to be referred to as 'anonymous', and only have only the name of the organization mentioned.

6. I am aware that, under the General Data Protection Regulation (EU) 2016/679, I am also granted the following rights: Right of access (Art.15); Right to rectification (Art. 16), Right to erasure ('right to be forgotten', Art. 17); Right to restriction of processing (Art. 18), Right to data portability (Art. 20); Right to object (Art. 21).

7. If I chose options b. or c in point 5., I understand that my name will not appear in any publications, articles or presentations, and no information that identifies me will be made publicly available, unless I expressly instruct the researcher to do otherwise.

8. (Optional, leave blank if you oppose) I consent that (encircle the option that applies)
a. the project Coordinator EXUS and the partners of ENCRYPT involved in Task [xx]
b. the ENCRYPT consortium

may use the data collected from my participation in this study for future research aligning to

the aims and values of the present research.

For further information about the data processing, you may contact [set up a dedicated email account].

The requests may only be made personally by you and you must identify yourself. We must answer your requests within one month, but if your request is too complex or we receive many other requests, we will inform you that this period may be extended by a further two months. We will respond to your requests in writing or when appropriate, electronically or orally.

In case you are dissatisfied with how the ENCRYPT project partner has managed a request or how your personal data are processed, you are entitled to submit a complaint to the competent supervisory authority. You may find a list of supervisory authorities and their contact details here:

https://edpb.europa.eu/about-edpb/about-edpb/members_en

_____

Signature of participant Date & Location

_____

Signature of researcher Date & Location