Grant agreement no. 101016112

Project ESSENCE

Empathic platform to personally monitor, Stimulate, enrich, and aSsist Elders aNd Children in their Environment

INNOVATION ACTION

Medical technologies, Digital tools and Artificial Intelligence (AI) analytics to improve surveillance and care at high Technology Readiness Levels (TRL)
SC1-PHE-CORONAVIRUS-2020-2B

Deliverable reference number and title:	**Data Management Plan**
Due date of deliverable:	30th April 2021
Actual submission date:	05/05/2021
Start date of project:	1st November 2020
End date of the project:	31st October 2022
Organisation name of lead contractor for this deliverable	UMIL
Other organizations involved	All

Version 1.0

Horizon 2020 Framework Programme (2014-2020)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

History chart

ISSUE	DATE	CHANGED PAGE(S)	CAUSE OF CHANGE	IMPLEMENTED BY
1.0	15.09.2020		Initial draft	UMIL
2.0	17.09.2020		Purpose of data details were added and ethics section was revised	POLIMI
2.2	08.04.2021		In depth revision	UMIL
3.0	13.04.2021		Alignment with DPIA	UMIL
3.1	22.04.2021		Contributions from SCOM, POLIMI and RMHS	UMIL
3.2	26.04.2021		Alignment with DPIA	POLIMI
3.3	29.04.2021		Comments from SG, SCOM	SG, SCOM

This project has received funding from the *European Union's Horizon 2020 research and innovation programme under grant agreement No 101016112*

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

This document provides the plan for managing the data generated and collected during the project. It covers: a) the handling of research data during and after the project, b) what data will be collected, processed or generated, c) what methodology and standards will be applied, d) whether data will be shared/made open and how and e) how data will be curated and preserved.

As such, this is a living document that starts before the signature of the Grant Agreement and it will be updated throughout the project until the delivery of an initial Data Management Plan (M6) and the Final Data Management Plan (M24). The latter will contain also the list of the used data-sets and how the relevant data of the project is handled and stored.

Data sets will be preserved after the end of the project in an OpenAccess repository for further use by the research community. We have identified Zenodo as most suitable OpenAccess repository (https://zenodo.org/). Data will be kept for five years after the completion of the research. This is a repository supported by CERN, that has already been used to keep the Monitoring OpenData of the MOVECARE project.

This deliverable integrates and extends the Data Protection Impact Assessment (DPIA) that is uploaded, as a separate document, together with this deliverable. The DPIA was sent to the consortium on the 22nd of April and was validated by the Data Protection Officer of the Politecnico di Milano.

2 DEFINITIONS

Dataset: Digital information created in the course of a research project but which is not a published research output. Research data excludes purely administrative records. The highest priority research data is that which underpins a research output. Research data do not include publications, articles, lectures or presentations.

Data Management Plan: A formal working document, which outlines how datasets will be handled both during the active research phase and after the project is completed. DMPs in some form are now a requirement of a research grant proposals and therefore must be addressed at the earliest phase of the research lifecycle.

Metadata: Information about datasets stored in a repository/database template. For example, an image may require metadata that describe how large the picture is, the colour depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document.

Repository: A digital repository is a mechanism for managing and storing digital content. Repositories can be subject or institutional in their focus

Secondary data: Sources that contain commentary on or a discussion about a primary source.

4 LIST OF ACRONYMS

CBAC – Community Based Activity Center

CIA - Confidentiality, integrity and accessibility (of the data)

D1.1 – Deliverable 1.1 (Data Management Plan – preliminary)

D1.3 – Final Data Management Plan

DMP – Data Management Plan

DPIA – Data Protection Impact Assessment

DSA – Disturbi Specifici Apprendimento

EC – European Commission

FAIR - Findable, accessible, interoperable and re-usable (data)

JSON - JavaScript Object Notation

WP – WorkPackage

EAB – Ethical Advisory Board

PSC – Project Steeering Committee

ICT - Information & Communication Technology

NDD - NeuroDevelopmental Disabilities (NDD)

SD – Secondary Data

SLD - Specific Learning Disability (SLD)

5 Introduction to the document

Research data is as important as the publications they support. They allow other researchers to verify hypotheses and to build new research upon results without having to start again from scratch. This has been recognized as fundamental by the research community[1] and several OpenData initiatives have been proposed. Hence, the importance for ESSENCE to define a data management policy according to the European Commission Guidelines.

In fact, according to the EC, all project proposals submitted to "Research and Innovation actions" and "Innovation 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 data management plan (DMP) to specify what data will be open.

This document introduces the first version of the project Data Management Plan (DMP). The ESSENCE DMP primarily lists the different datasets that will be produced by the project, the main exploitation perspectives for each of those datasets, and the major management principles the project will implement to handle those datasets.

5.1 Data and Data Management in Horizon 2020

The DMPs have been introduced in the Horizon 2020 Work Programme since 2014:

"... Horizon 2020 ... use of Data Management Plans (DMPs) detailing what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved. 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."

In particular the following definition apply:

What is research data?	Research data refers to information, in particular facts or numbers, collected to be examined and considered as a basis for reasoning, discussion or calculation.
What is open research data?	Openly accessible research data can typically be accessed, mined, exploited, reproduced and disseminated, free of charge for the user.

Table 1: Research Data and Open Data as defined by the EC

The purpose of a DMP is to provide an analysis 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.

It will specify the functional aspects: how the principles "FAIR" (findable, accessible, interoperable and re-usable) will be implemented inside the project.

It will also specify the structural aspects in particular with respect to security: how "CIA" (confidentiality, integrity and accessibility) will be implemented.

5.2 Data Management Plan Lifecycle

The data management plan will cover all the data life cycle.

[1] *Kitchin, Rob (2014). The Data Revolution. London: Sage. p. 49. ISBN 978-1-4462-8748-4*

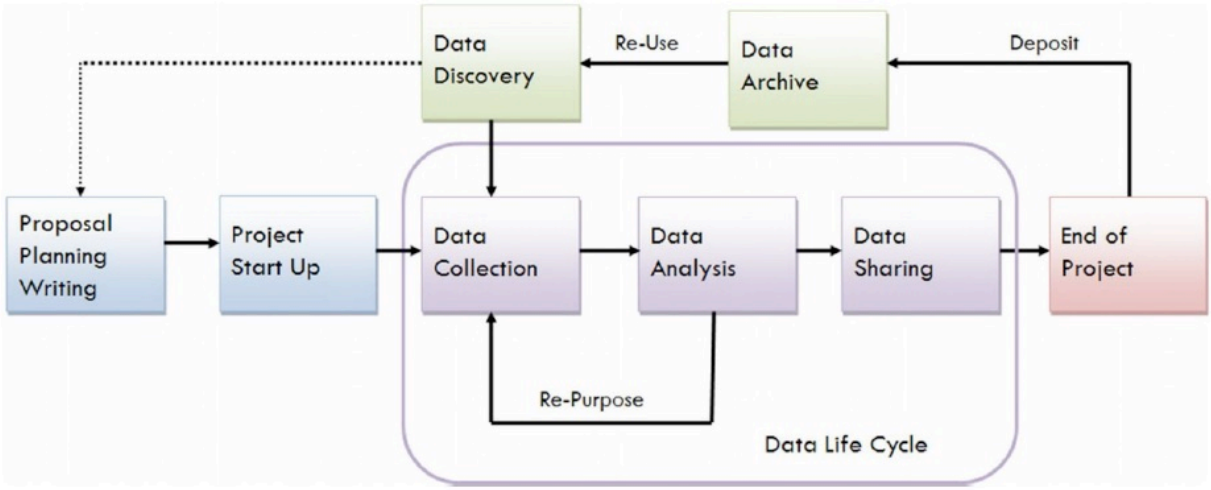

Figure 1. Source: Steps in the data life cycle. Source: University of Virginia, Research Data Services

Specifically, the DMP describes the data management life cycle for all datasets to be collected, processed and/or generated by a research project. It covers:

- The handling of research data during and after the project
- What data will be collected, processed or generated
- What methodology and standards will be applied
- Whether data will be shared/made open and how
- How data will be curated and preserved

5.3 Purpose of the document

Deliverable 1.1 Data management plan is the reference document for gathering, sorting, protecting and sharing all the datasets produced during the operation of the ESSENCE platform and its functioning inside the pilot.

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

The DMP is not a fixed document, on the contrary it will have to evolve during the lifespan of the project. This first version of the DMP includes an overview of the datasets to be produced by the project, and the specific conditions that are attached to them. The final version of the DMP will get into more details and describe the practical data management procedures implemented by the ESSENCE Project.

The most important part in the document is the description of the datasets and the explanation of how the ESSENCE project will manage them and fulfil their adjustment to the requirements provided by the European Commission regarding H2020 projects.

This deliverable builds mainly on the results coming from:

T2.2 (M1-M6) Definition of the users, scenarios and functionalities,

T2.4 (M3-M12) Technical specifications of the components at the engineered prototype level

T2.5 (M3-M12) Design ESSENCE architecture and data model

T3.8 (M3-M12) Implementation of cloud based data center

T5.1 (M13-24) Field testing of the older adults scenario

T5.2 (M13-24) Field testing of the children scenario

Monitoring data forms the basis of the ESSENCE project. They play a crucial role and should be effectively managed to ensure the verification and reuse of research results, and the sustainable storage of the datasets.

This Data Management plan aims at providing a timely insight into facilities and expertise necessary for data management both during and after the ESSENCE project, to be used by all ESSENCE partners and their environment.

The most important reasons for setting up this Data Management plan are:

- Embedding the ESSENCE project in the EU policy on data management, which is increasingly geared towards providing open access to data that is gathered with funds from the EU. The rationale is that the Horizon 2020 grant consists of public money and therefore the data should be accessible to other researchers.
- Enabling verification of the research results of the ESSENCE project.
- Stimulating the reuse of ESSENCE data by other researchers.
- Enabling the sustainable and secure storage of ESSENCE data in the consortium web based repositories.

The DMP considers all the data sets that will be collected, processed and/or generated within the project. The methodology the consortium follows to create the DMP is as follows:

1. Create a data management policy. To this end, we describe:
    a. The elements that the EU proposes to address for each dataset.
    b. The strategy that the consortium will use to address each dataset.
2. The elements that will be used to create a data management plan will be a set of templates, which we will send to the partners of the consortium in order to fill them with information for each relative data set.
3. Analyze the completed data management plan templates filled by the project's partners.
4. Provide a method to store and share the resulting identified datasets and the access policies to them.

Regarding the methodology, these guidelines will be taken into account at all moments.

5.4 Application Area

The Data Management Plan provides clear guidelines on how each partner responsible of a dataset needs to take care of the preservation and sharing of the information. These guidelines will be shared and agreed by all ESSENCE partners. They will provide a clear picture on each partner's responsibilities regarding the management of the data in the project.

5.5 Document Evolution Procedure

This deliverable is largely based on the Guidelines on Data Management in Horizon 2020. The content of this deliverable will be considered final at the time of its submission to the European Commission.

This document may be affected by the execution of the project work plan if new datasets (beyond the ones initially identified) arise further than the first version of the Data management plan. This aligns with the philosophy of a Data management plan where it acts as a living document reflecting the actions taken to manage all the datasets of information that may appear in the project.

Any project partner may request amendments, but each amendment will be analysed by the Ethical Review Board if ethical issues would arise. No modifications will be possible after Ethical approval by the responsible ethical committee.

In particular the DMP will incorporate the conclusions and guidelines summarized in the DPIA delivered in March 2021.

A DMP is a living document outlining how research data will be handled during a research project and evolves until the project completion. It gains more precision and substance during the project lifecycle. A final Data Management Plan will be submitted as Deliverable D1.3 at the end of the project. This will be a public document that will illustrate the procedures, discussions, ethical issues tackled throughput the project to make the Public Data compliant with EC regulations on one side, and easy to use by the researchers on the other.

5.6 ESSENCE methodology

The ESSENCE project[2] is an Innovation Action project funded by the European Union Horizon 2020 research and Innovation programme under the grant agreement number 101016112.

It involves six countries and is coordinated by POLIMI.

ESSENCE aims at using the data and information gathered during the Covid-19 pandemic period to open new opportunities for services targeting vulnerable populations:

- non- or pre-frail seniors, ages ≥ 65 years
- and children of the first years of primary school (5-7 years old).

To contribute to the public health response in the context of the ongoing epidemic, and preparedness for future emergencies, ESSENCE aims at boosting the creation of a new model of home-based care that relies on:

- Stimulation
- Remote monitoring
- Tele-assistance
- Social inclusion, favouring the connection between users, families, and professionals.

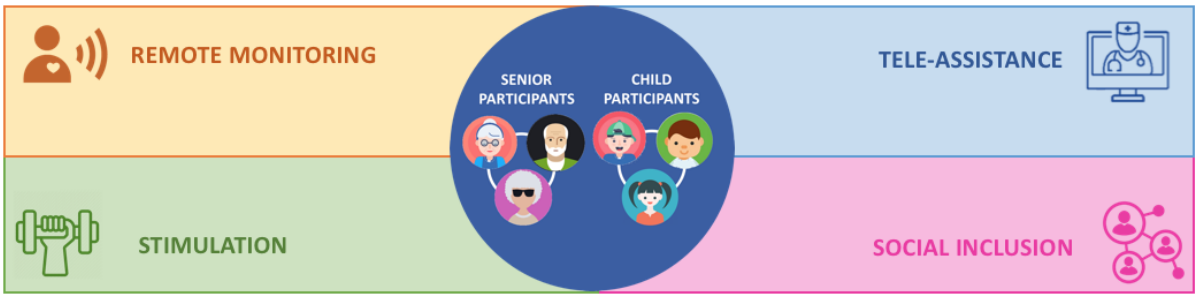

Figure 2 ESSENCE users and application domains.

The main aim of this project is the design of an innovative, multi-faceted platform to connect, stimulate, assist and monitor two categories of vulnerable target users: non-frail or pre-frail older adults independently living at home, and children - with particular attention to those with learning difficulties. ESSENCE builds upon the results of MoveCare H2020 and adopts an iterative optimization process between two pillars - technology transfer of a subset of successful modules and feedback received from testing on target users – with the final target of achieving CE mark and promptly entering the market.

The ESSENCE platform consists of three main components:

- **the Community-Based Activity Center** (CBAC), a holistic platform, based on virtual rooms, providing a series of diverse activities with declared recreational, socialization, educational, and assistive purposes;

[2] https://www.essence2020.eu/

- the **Monitoring Module**, that gathers heterogeneous information from the activities mediated by the CBAC, a smart ink pen, and diverse applications to extract cognitive, physical, and emotion-related indicators. Artificial Intelligence (AI) is exploited to provide personalized feedback, and alerts whether a change in behaviours or performances is detected;

- **the ESSENCE Manager,** that acts as the system control unit to manage user profiling, system configuration, possible system malfunctioning, and delivery of notifications, alerts, or feedback.

Through ESSENCE, a multi-level user empowerment will be promoted both by: (i) delivering empathic feedback aimed at maximizing engagement in the use of the platform and relieving stress; (ii) producing alerts on potential risks to family members, and health and education professionals aimed at fostering early detection of possible weaknesses and anticipation of care.

A longitudinal field testing of 12 months will be organized on both target populations with the deployment of the ESSENCE system at home.

6 Data Summary

In ESSENCE data will be collected in three phases of the research process: Phase 1) Co-design of the engineered prototype (WP2), Phase 2) Integration and testing (WP4) and Phase 3) Field testing in the two relevant scenarios (WP5).

Phase 1: CO-DESING

In the first months of the project, we administered questionnaires about COVID impact on daily life habits, humor, depression and general behavior of seniors and children in 4 of the countries involved in the consortium: Spain, France, Italy and Israel. The questionnaires were performed in the form of surveys under the supervision of FS in Spain, UIN in Italy, ESE in France and UH in Israel. In the same phase, focus groups with stakeholders have been organized to refine the requirements of the ESSENCE system.

The survey data acquisition procedure for the project purposes is in the form of qualitative data in the case of questionnaires and focus groups and quantitative data (cardinal, ordinal and nominal responses) to questions relating to user's socio-economic status, living arrangements and behavior.

All research methods adopted are well known and broadly utilized and have measures established to ensure ethical practice. All work will be undertaken in compatibility with national and EU law or with Israel (see Section 5.1.3 non-EU country) law, and none of the proposed research is foreseen to face any legal obstacles or objections.

Phase 2: EARLY TESTING

At the end of the first year, at least 6 seniors and 6 children will be requested to participate in testing the ESSENCE system at the POLIMI laboratory, and in protected environments (protected apartments of Servimayor in Extremadura, and in one school in Italy)

Phase 3: FIELD TESTING

In the second year of the project, seniors and children will be asked to participate in testing the ESSENCE system in their home for a 1-year period.

For both Phase 2 and 3, which include testing of the ESSENCE system on users (WP4/WP5), the national legislation of Italy and Spain will be the legal and ethical framework (cf. all deliverables associated to WP8).

In conducting research and deliberations, the national legislation of countries in which activity is implemented will be guiding the ethics. The whole list of informed consents, information sheets and ethical committee procedures which are needed for data collection in all 3 phases is reported in Del 8.1.

In phase 2 and 3 all the data will be stored inside a cloud-based repository according to CIA (Confidentiality, integrity and accessibility) specifications. The details on the cloud architecture are reported in Del 3.1.

6.1 Type of data

The Processing under consideration is the management of the users' personal information and data in the framework of the ESSENCE project.

Complex set of data, including user's lifestyle and health related parameters, and environmental data, will be collected, stored and managed during the project lifecycle. All the data are processed according to GDPR[3] regulation.

[3] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it

The consortium will sign a Data Sharing Agreement to ensure that there is in place proper arrangements relating to personal data transferred or shared between members of the ESSENCE consortium. In agreement with art. 26 of GDPR, it has been agreed that each of the parties is a joint data controller in relation to the data being transferred or shared under for the purpose described in the Grant Agreement. For scientific analysis and dissemination purposes, users' data will be shared with all the partners of the consortium in a complete anonymized form.

Third parties will be also involved in the management of sensitive data and different procedures will be adopted depending on their different roles, according to art. 28 of GDPR. In particular, three different categories of third parties are foreseen:

- *Institutions involved in the recruitment of the users, which are:*
  - Servimayor, a nursing home based on a non-profit association and third party of FS, involved in the early testing phase on Seniors;
  - CNC, a Professional Association of Neuropsychologists in Spain and third party of FS, supporting in the recruitment of seniors in the field testing phase;
  - Territorial School Office of Varese, a Third Party of UIN, supporting in the recruitment of children both for the early testing and the field testing phases.

  In this case, since only specific persons within the institutions will have access to the data, a written authorization letter to data processing will be signed by those persons.
- *Companies for Technical Support Services*: these companies will provide technological support to the users during the field testing phase. Since they may have access to the data, they will be appointed as external responsible of data processing through a specific contract or legal act which will set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.
- *Cloud platform* (AWS – Amazon Web Services as detailed in the following sections), where all data will be uploaded limiting geographically to EU the data storage. By applying for AWS Services SCOM agreed with the AWS Service Terms[4] which effectively represent a contract between SCOM and Amazon Web Services, and an external responsible of data processing has been already appointed. The AWS Service Terms include the AWS GDPR Data Processing Addendum[5] and are thus GDRP compliant.

Data which will be collected in the ESSENCE project are classified into two main categories:

- **General Personal Information (Private data)**

These data include mainly personal and identity information and contacts (phone number and email) and those data that are released directly by the users who give their explicit consent to the management conditions. These data are collected mainly in the written informed consent after detailed information ex art. 6 lect. a) of GDPR and in the form of questionnaires on user preferences.

This is in line with and respectful of the principle of privacy by design (art. 25 GDPR, privacy by default). The informed consent is provided in written form in accordance with deontological rules.

General personal information data are collected and stored at the recruitment site (FS for seniors and UIN for children). Contact data (email) are stored in the database under the responsibility of SCOM,

[4] AWS Service Terms. https://aws.amazon.com/service-terms/

[5] AWS GDPR Data Processing Addendum. https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/

the partner responsible for user authentication, but will be encrypted and the access to data in the database will be protected with authentication and authorisation mechanisms

- **Behavioural Data and Health Data (Sensitive Data)**
    - *Behavioural Data* are acquired from the application integrated in the CBAC module (e.g. exergames, serious games, social games…), from the smartphone through the voice analysis application and from the smart ink pen. Then, data are gathered by the AI monitoring module which extracts relevant indicators in order to track the participant's status in the following domains: cognitive, physical and emotion valence and arousal. These data are classified as personal data under the privacy regulation.

      These data are obtained through consent after detailed information ex art. 6 lect. a) of GDPR. This is in line with and respectful of the principle of privacy by design (art. 25 GDPR, privacy by default).
    - *Health Data* includes all the health data acquired through the light health data monitoring (an application used by the users to input diaries of relevant parameters such as the weight, the pressure ...) and all the data acquired and stored during and after the teleconsultation done through the CBAC (e.g. professionals' report of the tele-consultation, specific tests done during the consultation). These data mainly relate to physical and cognitive status of the user and are classified as special categories of personal data by article 9 of the GDPR.

These data are obtained through consent after detailed information ex art. 6 lect. a) of GDPR. This is in line with and respectful of the principle of privacy by design (art. 25 GDPR, privacy by default). All partners can have accessed to behavioural and health data ad data processors, but data will be shared anonymised.

The raw data collected by the ESSENCE platform are called measurements and are stored into the ESSENCE cloud platform as a data source. Then, several applications on the ESSENCE servers included in the cloud architecture are processing the measurements to transform them in indicators. Indicators are peculiar features extracted from the measurements and correlated to the user status. Such indicators are managed by the AI monitoring module, the intelligence of the system, which tries to detect preference and anomalies able to provide inputs to the ESSENCE Manager. Such inputs are called feedbacks and are suggested activities, alerts and reminders for the user. The ESSENCE Manager distributes feedbacks to the user. The feedbacks are provided through notifications to the ESSENCE tablet or the smartphone, and/or via emails to professionals depending on the context and feedback meaning.

In Figure 3 all the main components of the ESSENCE project interacting with the users are shown. The target users at home are provided with a pen connected to a tablet, a home station for exergames, and some applications to be installed on their smartphones. The professional users instead are provided with web applications that can be run from their working stations. The external users can also connect to the ESSENCE platform with their own device (i.e., a tablet) to join social activities.

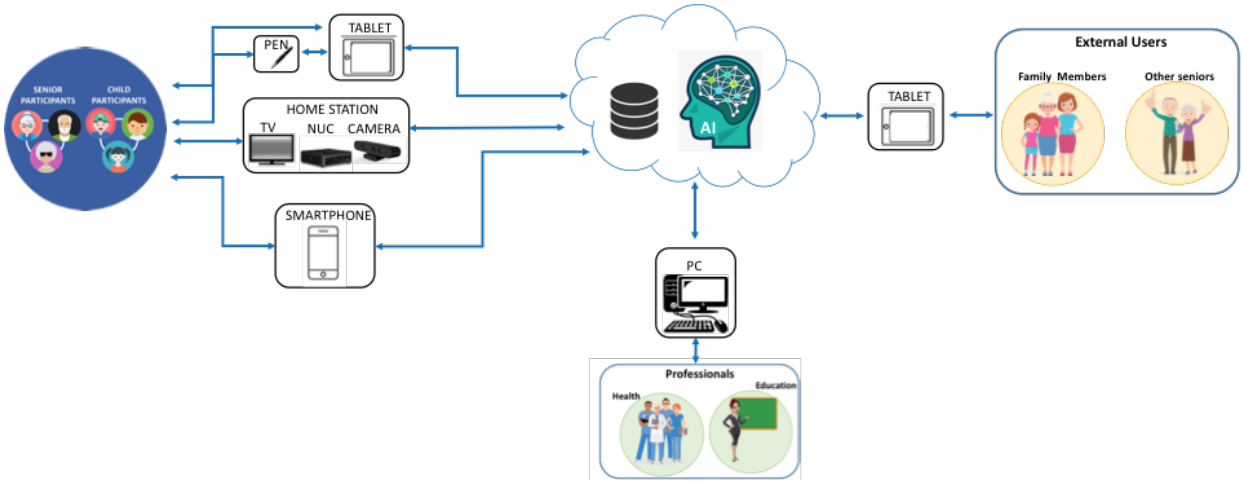

Figure 3. Essence overview showing components provided to the users and users.

Personal data will be stored for five years and then destroyed. After five years, data will be kept in a complete anonymized form only for scientific purposes.

Anonymous data, in an aggregated form, will be also shared in open access one month after data generation as declared in the Article 29.3 of the Grant Agreement.

n Appendix A, a list of ESSENCE functionalities is reported: for each functionality, raw measurements and exemplary indicators are reported. Please do not consider this table as a complete list of data collected through ESSENCE. However, this is a living document which will be continuously updated when new indicators will be available.

6.2 Purpose of the data

Data in ESSENCE are central at the beginning for defining user needs (phase 1), for testing the engineered prototype in real environment (phase 2) and then for monitoring and assisting the users at home and personalize their activities (phase 3).

The questionnaires used in Phase 1 include generic questions on the impact of COVID in the quality of life, on their habits and needs, on their use of technologies and so forth. All answers are pseudonymized. The data collected in Phase 1 are used to define the user needs, and thus refine the ESSENCE platform accordingly.

Concerning Phase 2 and 3, the data collected are used by the *ESSENCE manager* that communicates with all the users involved in the target user ecosystems (professionals, caregivers, the target user himself/herself and so forth).

In particular as reported in the DoA (pp 3-4 part B) the data are collected by the different modules as follows:

The monitoring module gathers heterogeneous information from the activities mediated by the CBAC, the smart ink pen, and diverse applications. It will extract relevant indicators for both populations in order to track the participant's status and adapt the profile in the following domains:

- **Cognitive Status**: information collected through the *CBAC Entertainment* (e.g.: cognitive games performance), *CBAC Tele-assistance* (e.g.: professionals' opinion from tele-consultation), Handwriting and Voice Analysis with the goal of monitoring seniors at risk of age-related cognitive decline and children at risk of Specific Learning Disability (SLD) and Neuro-Developmental Disabilities (NDD)

- **Physical Status**: information collected through the *CBAC Entertainment* (e.g.: physical exergame), *CBAC Teleassistance* (e.g.: parameters inserted in the Health Data Diary), Handwriting Analysis with the goal of monitoring DSA, seniors in terms of age-related changes in balance and tremor, or light health monitoring, and to track children at risk of SLD and NDD

- **Emotion Valence and Arousal**: information collected through Voice Analysis (either voice parameters collected during the activities mediated by the CBAC, or from the mobile voice app for seniors), to monitor important indicators related to emotion valence, arousal, stress...

The *Monitoring Module* will exploit AI with a twofold aim: i) to enrich the users, providing personalized suggestions and feedback on their strengths, thus maximizing engagement and relieving stress; ii) to timely detect deviations from usual physiological behaviours and send alerts to others (family members, health and education professionals) to foster prevention and anticipation of care.

The ESSENCE Manager coordinates the platform: it is the system control unit that manages the user profile registrations, the system configuration, and possible system malfunctioning in a proactive way. In addition, it receives pre-processed data coming from the AI-based monitoring module and distributes notifications, alerts, or feedback accordingly to the user of interest."

All these behavioural data collected in Phase 2 and 3 cannot be considered strictly biometric data because from the time series it is not possible to identify univocally the person.

6.3 Data life cycle

The ESSENCE project conducts a prospective interventional study on the impact of novel technologies at keep or improve a good health and well-being status.

In particular, through the final field-testing study, the ESSENCE project is aiming at validating the ESSENCE platform in relation to three main factors:

- Feasibility, i.e., carrying out a pilot study on a small court (i.e. a not statistically significant sample size for assessing clinical outcomes, compose by 120 test users - 60 children and 60 elders)
- Usability
- Acceptance.

General Personal Information are collected by the two pilot sites of the ESSENCE project:

- FS in Spain, involved in the recruitment of seniors, helped by three third parties, as previously mentioned, which are:
  - Servimayor, involved in the early testing phase
  - CNS, involved in the on field testing phase
- UIN in Italy, involved in the recruitment of children, with the help of the Territorial School Office of Varese, as third party, for both testing phases.

These data are collected mainly in the informed consent on voluntary based participation and by means of questionnaires to have an evaluation of the user before and after testing the platforms. Data necessary for ESSENCE evaluation are inserted in a structured database according to the most common information technology standards (.xls, .CSV, .TXT data format). Data necessary to the ESSENCE ICT platform are inserted in a structured MONGODB dataset in the ESSENCE platform.

Contacts are maintained completely separated with respect to the other data Other sensitive data will be uploaded in the ESSENCE platform in a pseudonymized form and different measures are taken to

assure data protection according to the principle of privacy by design (art. 25 GDPR, privacy by default).All the Behavioural and Health data collected are stored into the ESSENCE cloud architecture as *measurements* that are then processed first to become *indicators* relevant to the single functionalities. Then, the *indicators* are managed by the monitoring AI to generate *feedbacks* in the form of suggested activities, alerts and reminders to the relevant user. All these *feedbacks* are orchestrated by the ESSENCE Manager.

Data are managed and stored through a structured Mongo database. Specific measures will be implemented, e.g., pseudonymization, cryptography (physical encryption), and proprietary data format, and access control through authentication and authorisation. The field testing is structured with a continuous monitoring of users' data to check their integrity and coherence. In addition, it is foreseen even in the protocol that users will be contacted on a regular basis to keep on track the pilot. At intermediate points, a check of data protection with users and on the system will be added in the protocol. From this perspective we can say that the ESSENCE consortium will perform a continuous update and monitoring of the DPIA condition and assessment.

Eventual deviation could be immediately detected, analysed and solved.

In Table 1 all the steps of the life cycle of data processing are reported and detailed from the creation of a user account towards the deletion of the whole data.

PROCESS	DETAILED DESCRIPTION OF THE PROCESS
Create an account	The user provides identification data (email) and opens his/her new account. In the case of children, the parent or legal representative oversees the account creation.
Enter the initialisation data	The user chooses his/her preferences so that the configuration and initialisation data are entered on the device (tablet, smartphone, smart TV for the target user or PC for professionals). In the case of children, the parent or legal representative oversees data initialization.
Transfer data	Data are transferred to the cloud architecture
The ESSENCE platform collects data	The ESSENCE applications are used by the user and the collected raw data are stored to the cloud architecture.
Computation of indicators	The raw data are processed on the servers by means of automatic algorithms able to compute the daily indicators. The indicators are stored on the MongoDB data base in the ESSENCE cloud architecture.
AI reasoning	The monitoring AI processes all the indicators saved on the MongoDB data base on the cloud in order to derive feedbacks for the users in case of anomalies and/or behaviour changes. The feedback are suggested activities, alerts and reminders to the relevant user. The feedbacks are stored on the MongoDB data base.
Feedbacks sent to the home devices	The feedbacks are sent to the relevant user by means of notifications for the mobile, or the tablet or via email.
Share data	The generated data (indicators) are shared in open access one month after data generation as declared in the Article 29.3 of the Grant Agreement.
Delete data	Personal data are deleted 5 years after the end of the project.

Table 1 Life cycle of data

6.4 Type and format of data collected

The data register will deliver information according to Annex 1 of the Horizon 2020 guidelines (2015) (in italics):

- **Data set reference and name**: Identifier for the data set to be produced.
- **Data set description**: Descriptions of the data that will be generated or collected, its origin (in case it is collected), nature and scale and to whom it could be useful, and whether it underpins a scientific publication. Information on the existence (or not) of similar data and the possibilities for integration and reuse.
- **Standards and metadata**: Reference to existing suitable standards of the discipline. If these do not exist, an outline on how and what metadata will be created.
- **Data sharing**: Description of how data will be shared, including access procedures, embargo periods (if any), outlines of technical mechanisms for dissemination and necessary software and other tools for enabling re-use, and definition of whether access will be widely open or restricted to specific groups. Identification of the repository where data will be stored, if already existing and identified, indicating in particular the type of repository (institutional, standard repository for the discipline, etc.). In case the dataset cannot be shared, the reasons for this should be mentioned (e.g. ethical, rules of personal data, intellectual property, commercial, privacy-related, security-related).
- **Archiving and preservation (including storage and backup)**: Description of the procedures that will be put in place for long-term preservation of the data. Indication of how long the data should be preserved, what is its approximated end volume, what the associated costs are and how these are planned to be covered

Data sets description is reported in Section 11. Details on the data format will be provided in the final Data Management Plan, Deliverable D1.3, due at M24.

In particular, data will be complemented with a data model that will contain explanation of the data. A metadata file will be assigned to datasets for effective and persistent citation when it is uploaded to the web repository. This metadata file can be used in any relevant publications to direct readers to the underlying dataset. The metadata file will be stored in the ESSENCE dataset section in the project website.

6.5 Re-use of existing data

We will use the data produced by the MOVECARE project to define a suitable data model for the data of ESSENCE.

6.6 Origin of the data

Data in ESSENCE will be heterogenous and provided by different devices.

Primary data will be provided by the CBAC during the interactive activities. Other data will be provided by the smart objects that belong to the smart network monitoring the subjects, that comprehends also the smart phone. Additional data will be the data that define the users in the dimensions defined (e.g. their preferences, needs, social data – age, weight…).

The specific data provided by the different components will be defined in the final version of the DMP (Deliverable D1.3).

From these primary data, indicators will be computed and stored in the data center. These will be for instance the features automatically extracted on the fly from the voice signal over the smart phone, indexes of tremor intensity, speed with which an activity is performed, and so forth.

A detailed description of the data provided will be part of the final version of the DMP (Deliverable D1.3).

6.7 Expected size of the data

According to the data flow identified in the DoA, we have the following initial estimate of the data amount:

- Smart pen: 1 hour a day of use, sampling at 50 Hz, records of 8 data (X, Y, Z acceleration; X, Y, Z angular velocity, pressure, timestamp) => 1.6 K Byte /s => 6 Mbyte / day.
- CBAC: 1 hour a day of use, sampling at 10 Hz, records of 3 data (x,y position, pointer activity (click, drag) => 120 Byte /s => 500 Kbyte /day.
- Additional information like: voice features from phone conversations / users profile / dairy information and so forth may contribute with 500 K Byte / day.

These data have to be multiplied by 1440, that is the number of users in the final pilot (120) times the duration of the pilot (12 months). That leads to a bit less of 10 GByte.

These data dimension led to the choice of the cloud space storage (cf. Deliverable 3.1). A 10 fold margin is added to take into account the data that are acquired in preliminary experiments and we will look for a cloud space of 100 GByte.

Nevertheless, enlargement of the cloud data space can be required any time.

6.8 Data utility

Data collected from monitoring devices will be used by the ESSENCE Monitor to tune intervention and to provide warnings and alarms to caregiver.

The data collected constitutes a data corpus of high value as they will be acquired in normal everyday life in ecological conditions, and they will be therefore extremely useful to computer science researchers who work on big-data for e-Health to propose new models and refine the existing ones as well to clinical researcher who investigate new modalities for early detecting abnormal behaviour.

7 FAIR data

All the public data of the project will be openly accessible in a public repository during the project.

Indeed, as declared in the Article 29.3 of the Grant Agreement, one month after collection anonymous data will be shared in open access, using platform such as Zenodo OpenAccess repository (https://zenodo.org/), supported by CERN, that has already been used to keep the Monitoring OpenData of the MOVECARE project.

Non-public data will be archived at the repository using a non visible, indexed directory in the cloud storage.

The final choice of the repository has been made at the kick off meeting at project start in order to assure that the collected data will be made available at the latest within 30 days after they have been generated, through open access or, if agreed by the Commission, by giving access rights to those third parties that need the research data to address the public health emergency.

7.1 Making data FAIR

ESSENCE consortium is committed to make the data produced FAIR: Findable, accessible, interoperable and re-usable.

The ESSENCE project aims to collect and document the data in a standardized way to ensure that, the datasets can be understood, interpreted and shared in isolation alongside accompanying metadata and documentation.

A data model will be associated to data that fully describes how they were acquired, their format and their semantical meaning such that they can be used by other researchers fruitfully also long after the data have been produced.

To this aim **metadata** will be extensively used to categorize the data and fully support semantic query in the cloud database for use inside the project and also outside the project as well as for re-use of the data.

We will start creating the metadata that accompany each data record from the domain knowledge of the ESSENCE partners. The number and type of metadata will increase throughout the first year of the project. They will describe the data both from the technological point of view (e.g. smart object, pressure sensing…) and from the functional point of view (tremor, pressure…). The final metadata used will be contained in D1.3 – Final Data Management Plan.

Naming conventions will be defined by partners and will be part of D1.3 the final Data Management Plan.

Data will be acquired sequentially in time, and each new recording will have its own time stamp that clearly distinguishes from the other data of the same user both in different days and inside the same day.

7.2 Making the data openly accessible

The datasets will be made available for re-use through uploads during the project through an OpenAccess data repository, like Zenodo.

Nevertheless, the consortium aims to transfer the ESSENCE resulting sharing data deposited in the project cloud repository to an the OpenAccess data repository, as soon as possible unless a decision has been taken to protect results.

Specifically, research data needed to validate the results in the scientific publications should ideally be deposited in the OpenAccess data repository at the same time as the publication occurs.

During embargo/restriction periods, information about the restricted data will be published in the data repository, and details of when the data will become available again will be included in the metadata.

Restricted data will be agreed amongst all partners. Where a restriction on open access to data is necessary, attempts will be made to make data available under controlled conditions to other individual researchers.

Data are stored in the project cloud repository. They must be made available to partners upon request, including in the context of checks, reviews, audits or investigations. Data will be made accessible and available for re-use and secondary analysis.

Data objects will be deposited in the cloud repository under:

- Partners access to data files and metadata and data files provided over standard protocols such as HTTP.
- Use and reuse of data permitted.
- Privacy of its users protected.

In principle, all the data with no restriction on access will be moved from the project cloud repository to an OpenAccess repository at least within 30 days after data generation without additional cost.

All the research data will be of the highest quality, have long-term validity and will be well documented in order other researchers to be able to get access and understand them after 5 years.

If datasets are updated, the partner that possesses the data has the responsibility to manage the different versions and to make sure that the latest version is available in the case of publicly available data. Quality control of the data is the responsibility of the relevant responsible partner generating the data.

The definition of a data model will allow to access the data easily. Data will be stored with most common standard and formats like JSON format to fully support inter-operability. As such, simple APIs that access the data in the OpenAccess repository will be required to access and download the data. For this reason, no particular documentation on Software for retrieving the data is required.

The partners will evaluate if to include software used to compute features in the OpenAccess repository. This will be part of the Final Data Management Plan (D1.3), delivered at M24.

We aim to provide the right of use of the data only for research purpose and with the request to acknowledge the project name, ESSENCE, that has provided the data. This will be clearly stated in a companion document that specifies the license under which the data are provided. Moreover, access to the data will be monitored through the log of the accesses and actions operated by the Zenodo website.

7.3 Interoperability of the data

Most used standards will be used to store data. We will use JSON format to store the data with a full description of the data record through a complete data model.

We will provide a semantic description of the data that support semantic search both in the applicative and methodological domains.

Keywords in the data model will be chosen according to the best practices of the field of interest such that data can be easily identified and used in different disciplines. We will resort to partners knowledge to use the best data description as possible.

7.4 Increase data re-use

Data will be licensed under wide OpenAccess license, under Creative Commons, of the type: cc by-nc-nd 4.0, that allows full use of the data for non-commercial purposes.

Data quality is fundamental for the development of the project itself as all interventions are based on these data. Data quality will be checked first by the consortium partner that produces the data, and the partners who consume or read these data will double check them.

The consortium strongly believes in the concepts of open science, and in the benefit that the European innovation ecosystem and economy can draw from allowing reusing data at a larger scale.

Therefore, a number of valuable datasets produced by the project can potentially be published with open access – though this objective will obviously need to be balanced with the other principles described below.

7.4.1 IPR management and Security

Project partners obviously have Intellectual Property Rights (IPR) on their technologies and data, on which their economic sustainability relies. As a legitimate result, the ESSENCE project consortium will have to protect these data and consult the concerned partner(s) before publishing data. This may result in a processing of the datasets to be made available to the public.

Another effect of IPR management is that – with the data collected through ESSENCE being of high value – all measures should be taken to prevent them to leak or being hacked. Hence, all data repositories used by the project will include a secure protection of sensitive data.

7.4.2 Personal Data Protection

For some of the activities to be carried out by the project, it may be necessary to collect basic personal data (e.g. full name, contact details, background), even though the project will avoid collecting such data unless deemed necessary.

National legislations applicable to the project are also be strictly followed, such as the Italian Personal Data Protection Code2 or the Spanish LOPD[6] or see below.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1] The GDPR replaced the data protection directive (officially Directive 95/46/EC)[2] of 1995. The regulation was adopted on 27 April 2016. It became enforceable from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

[6] https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

8 Allocation of resources

There are no immediate costs anticipated to make the datasets produced in ESSENCE. The datasets will be deposited in an OpenAccess website repository for at least 5 years after the conclusion of the project.

Each ESSENCE partner should respect the policies set out in this DMP. Datasets have to be created, managed and stored appropriately and in line with European Commission and local legislation. Dataset validation and registration of metadata and backing up data for sharing through repositories is the responsibility of the partner that generates the data in the WPs.

The datasets in the ESSENCE web server project will be preserved in a UMIL storage archive, in line with the European Commission Data Deposit Policy, with no costs. The data will be preserved for 5 years and there are currently no costs for archiving data in this repository.

The data that will be made available to the scientific community will be also moved to an OpenAccess repository like Zenodo at no costs.

Indeed, costs will be minimized as functionalities will be developed with inter-operability in mind: the data generated by all components will be re-used first into the project and therefore a clear data model has to be set-up and maintained throughout the development.

In particular, data management will be supervised by UMIL and by its PI, Prof. N. Alberto Borghese. His declared costs will cover also these tasks and will be associated to D1.1 and D1.3.

8.1 Data repositories

General personal information data include personal information and those data are collected mainly compiling and signing paper sheets and data necessary to the ESSENCE platform are inserted in a structured dataset or database according to the most common information technology standards (.xls, .CSV, .TXT, .JSON data format). Final data model will be reported in D1.3.

Instead, Behavioural and Health Data acquired from ESSENCE modules are organized in measurements (readings from a single sensor) and indicators (characteristics of a user which may be derived from measurements) and are represented as a JSON format for message exchange between ESSENCE modules, as well as for the storage in a NoSQL (mongodb) database collection.

Measurements and indicators are sent to the cloud repository through ad hoc implemented API and are stored and physically encrypted in a separated repository from the p data.

On the cloud, the AI monitoring module process these data to provide the correct feedback to the user (e.g. suggested activities, required teleconsultation). The ESSENCE interface is the tablet CBAC application.

The cloud environment has been deployed on the Amazon Web Services platform (limiting geographically to EU the data storage), with all modules running on separate machines (each machine being under the responsibility of a lead technical partner – POLIMI, UMIL, SCOM, SXT) interfacing through secure service oriented (RESTful web services) and message queuing (MQTT) architectures. This modular architecture will allow separate teams to build an integrated platform incrementally.

Specific measures will be implemented in data repositories, e.g. pseudo anonymization, cryptography (physical encryption), proprietary data format, and access control through authentication and authorisation.

Informed consents will be kept on papers at recruitment sites.

8.2 Data quality

All devices and apps run a thorough validation in terms of accuracy and reliability. An iterative testing approach of each single component and of the integrated prototype will be used.

This means that a prerequisite for the introduction in the pilot test of the technology is their approval by consortium on the basis of a test report.

The tests and their results are described in the corresponding deliverables:

- D2.3 - Definition of methodology and metrics for testing on users
- D4.1 - Protocols and metrics for system technical and functional testing at engineered level
- D 4.2 - Integration and testing of the complete ESSENCE prototype.

9 Data security

Full CIA (Confidentiality, integrity and accessibility) of the data will be considered according to documents reported in Section 13

Data will be stored in a cloud data center, that will guarantee redundancy in the storage and thus data integrity over time.

Following completion of the project, all the responsibility concerning data recovery and secure storage will go to the OpenAccess repository.

Accessibility will be granted to all partners of the project for the entire duration of the project. At the end of the project, partners will be asked to dump the data before moving the data on permanent storage and on the OpenAccess data repository.

Data will be archived and preserved in the ESSENCE webserver data sharing repository. This provides options for making data openly available and other data restricted access as required.

ESSENCE will take into account the GDPR data requirements regulations.

All data collected by the project will be considered compliant after giving data subjects full details on the experiments to be conducted, and after obtaining signed informed consent forms.

The subjects will read and sign an information sheet (cf. section 10) in which specific information on data treatment and security will be described. Specific attention will be given to the permission for open data. A full reference to article 25 of GDPR will be included.

All ESSENCE datasets will be pseudo-anonymized at the time of their publication in the OpenAccess repository, in order to assure privacy regarding the origins of the data.

From the implementation point of view, all sensitive personal data will be encrypted inside the data centers of ESSENCE and secure transfer through HTTPS protocol will be implemented to guarantee protection.

Essential security mechanisms will be implemented, building on strong AES encryption. Data in transfer will secured with the TLS protocol. Data at rest will be protected with relevant authentication and authorisation mechanisms. Authentication will be done using cryptographically signed tokens (JWT). After successful authentication, authorisation for access to services/data is enforced checking user assigned roles against access rights (privileges) assigned to different roles. The platform therefore provides protection at database and communication levels.

9.1 Managing CIA

The ESSENCE consortium is composed of 9 partners from the following countries, namely: Italy (4), Spain (1), France (1), Slovenia (1), Cyprus (1) and the Israel (1) covering all key research fields addressed in ESSENCE.

The coordinator is Politecnico di Milano, an Italian technical university. Being the coordinator, this is the entity entitled to have the final data management.

The persons in charge of the different roles and related responsibilities are the following ones:

- Scientific Coordinator: Prof. Ferrante Simona (Department of Electronics, Information and Bioengineering, DEIB, POLIMI), email: simona.ferrante@polimi.it
- Data Protection Officer: Dr. Vincenzo Del Core (Data Protection Officer. POLIMI), email: privacy@polimi.it
- Legal representative: Prof. Stefano Tubaro (Director of the DEIB Dept., POLIMI, as delegate of the Rector), email: Stefano.tubaro@polimi.it

- All partners of the ESSENCE consortium have appointed an internal responsible for privacy compliance, who points of contact are reported in Table 2.

Partner	Address	Point of contact for the management of personal data
Politecnico di Milano (POLIMI)	Piazza Leonardo da Vinci 32, Milano, 20133, Italy	Dr. Vincenzo Del Core (Data Protection Officer) Email: privacy@polimi.it
Università degli Studi di Milano (UMIL)	Via Festa Del Perdono 7, Milano, 20122, Italy	Data Protecion Officer Email: dpo@unimi.it
Università degli Studi dell'Insubria (UIN)	Via Ravasi 2, Varese 21100, Italy	Data Protecion Officer Email: privacy@uninsubria.it
Fundación para la Formación e Investigación de los Profesionales de la Salud de Extremadura Fundesalud (FS)	Calle Pio Baroja 10, Merida 06800, Spain	Jonathan Gómez-Raja Email: jonathan.gomez@fundesalud.es
University of Haifa (UH)	Abba Khushy Blvd Mount Carmel, Haifa 31905, Israel	Dr. Nadav Azoulay Email: nazoulay@univ.haifa.ac.il
SXT srl - Sistemi per telemedicina (SXT)	Via Torquato Tasso 29, Pogliano Milanese 20010, Italy	Luca Piccini Email: lpiccini@sxt-telemed.it
Smart Com d.o.o. Informacijski in Komunikacijski Sistemi (SCOM)	Ulica Brnciceva 45 Crnuce, Ljubljana 1231, Slovenia	Marko Žnidaršič Email: marko.znidarsic@smart-com.si
Signalgenerix Limited (SG)	Grigori Afxentiou 23c Mesa Geitonia, Limassol 4003, Cyprus	Marios Milis Email: marios.milis@signalgenerix.com
Initiation des Seniors aux NTIC Association (ESE)	Cite Phalsbourg 19, Paris 75011, France	Monique Epstein Email: monique.epstein@gmail.com

Table 2 List of responsible for privacy compliance for all partner of the ESSENCE consortium.

The main partners dealing with users data during the pilots are:

- SCOM: cloud and IT infrastructure provider (responsible for data storage)
- POLIMI, UMIL, SXT, SG: other technical partners responsible for the other modules to make the essence platform fully working
- UIN: pilot site (responsible for data collection for children)
- FS: pilot site (responsible for data collection for seniors)
- All other partners: responsible for data processor for research purposes.

The consortium will sign a Data Sharing Agreement to ensure that there is in place proper arrangements relating to personal data transferred or shared between members of the ESSENCE consortium. In agreement with art. 26 of GDPR, it has been agreed that each of the parties is a joint data controller in relation to the data being transferred or shared under for the purpose described in the Grant Agreement. For scientific analysis and dissemination purposes, users data will be shared with all the partners of the consortium in a complete anonymized form.

Third parties will be also involved in the management of sensitive data and different procedures will be adopted depending on their different roles, according to art. 28 of GDPR. In particular, three different categories of third parties are foreseen:

- *Institutions involved in the recruitment of the users*, which are:
  - Servimayor, a nursing home based on a non-profit association and third party of FS, involved in the early testing phase on Seniors;
  - CNC, a Professional Association of Neuropsychologists in Spain and third party of FS, supporting in the recruitment of seniors in the field testing phase;
  - Territorial School Office of Varese, a Third Party of UIN, supporting in the recruitment of children both for the early testing and the field testing phases.

  In this case, since only specific persons within the institutions will have access to the data, a written authorization letter to data processing will be signed by those persons.
- *Companies for Technical Support Services*: these companies will provide technological support to the users during the field testing phase. Since they may have access to the data, they will be appointed as external responsible of data processing through a specific contract or legal act which will set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.
- *Cloud platform* (AWS – Amazon Web Services as detailed in the following sections), where all data will be uploaded limiting geographically to EU the data storage. By applying for AWS Services SCOM agreed with the AWS Service Terms[7] which effectively represent a contract between SCOM and Amazon Web Services, and an external responsible of data processing has been already appointed. The AWS Service Terms include the AWS GDPR Data Processing Addendum[8] and are thus GDRP compliant.

The ESSENCE project consortium (all the partners and not only the coordinator) signed with the European Union a Grant Agreement that defines all the obligations with respect to the data processing. In particular, Article 39 - Processing of Personal Data – establishes the rights and duties of the Commission and of the beneficiaries for what concerns the processing of personal data and the consequences for non-compliance.

The Data Sharing Agreement, which will be signed among ESSENCE partners, will define specific rules and procedures intra-consortium. In it, the ESSENCE consortium will establish how third parties are foreseen to be given access to the Data.

If any processing activity would be assigned to another entity, institution or person outside the ESSENCE consortium, a processing contract will be signed with it or him, setting out all of the aspects stipulated in Art. 28 of the GDPR: duration, scope, purpose, documented processing instructions, prior authorisation where a processor is engaged, provision of any documentation providing evidence of compliance with the GDPR, prompt notification of any data breach, etc.

The parties will in any case ensure that these third parties which are permitted by all Parties, undertake in writing the same obligations as agreed in the Data Sharing Agreement.

As far as data transfer of data outside Europe, we remark that the project consortium includes a partner from Israel.

[7] AWS Service Terms. https://aws.amazon.com/service-terms/

[8] AWS GDPR Data Processing Addendum. https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/

However, Israel is among the few non-EU countries which have received an 'adequacy determination' from the European Commission indicating that they have a data protection framework offering a level of protection equivalent to that provided under EU law.[9]

Furthermore, to minimise the risk of data transfer of data to non-EU countries, only pseudonymized data will be transferred to Israel. Personal data will be collected and stored by the pilot sites responsible at the recruitment of the users.

Data transfers with non-EU countries will be in accordance with Chapter V of the GDPR.

Moreover, the following is clearly expressed in the clauses of the Data Sharing Agreement:

3.2. Data sharing with Partners of the Consortium in Switzerland is covered by the 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C (2000) 2304).

3.3. Exceptional events can bring to redefine the role of one or more consortium partners with respect to the belonging to the EU area: in this case this contract will adopt the standard clauses defined by the COMMISSION DECISION of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, and the COMMISSION DECISION of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271). Except these cases, the project does not foresee to transfer data outside the European Union.

9.2 National legislation

We report here additional documentation provided by single EC states involved in the project.

Italian national legislation

The Legislative Decree no. 196 of 30 June 2003 (the "Data Protection Code"), as amended by the Legislative Decree no. 101 of 10 August 2018, adapts Italian data protection laws to the new provisions of the GDPR. The Legislative Decree no. 101 entered into force on 19 September 2018.

https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg

Spanish national legislation

Data protection in Spain is ruled by organic law 3/2018 (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

French national legislation

French laws apply the GDPR principles. In French legislation, this was transcribed by the law 2018-493 of 20 June 2018 on the protection of personal data.

https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037085952/

[9] The list of countries covered by a Commission adequacy determination is available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

The CNIL (Commission *nationale de l'informatique et des libertés* is the French Data Protection Authority. https://www.cnil.fr/

Cypriot national legislation

On 31 July 2018 the national 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)/2018), was published in the official gazette of the Cyprus Republic (see Unofficial Translation in English: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf

Israeli national legislation

The legal framework for data protection in Israel is reported at the following link:

https://www.gov.il/en/departments/the_privacy_protection_authority

Slovenian national legislation

Slovenia has yet to implement in its legal system the Regulation (EU) 2016/679 of the European Parliament and the Council, of April 27, 2016, regarding the protection of natural persons with regard to the processing of their personal data and freedom of circulation of these data (GDPR), which became effective as of May 25 2018. For this purpose, a revised Protection of Personal Data Act (ZVOP-2) is currently under preparation in Slovenia. In the meantime, the data protection has been regulated since May 25 2018 by the direct implementation of the GDPR, which has precedence over the (old) Protection of Personal Data Act (ZVOP-1; Official Gazette of Republic of Slovenia No. 86/04, 51/07, 67/07, 94/07, 177/20). The latter is still valid, until superseded by the revised Act (ZVOP-2), but only applied to a limited extent.

The Information Commissioner (IPRS) is the Slovenian national data protection authority:

https://www.ip-rs.si/

10 Ethical Aspects

ESSENCE partners are to comply with the ethical principles as set out in Article 34 of the Grant Agreement, which states that all activities must be carried out in compliance with:

a. Ethical principles (including the highest standards of research integrity — as set out, for instance, in the European Code of Conduct for Research Integrity (European Science Foundation, 2011) — and including, in particular, avoiding fabrication, falsification, plagiarism or other research misconduct) and
b. Applicable international, EU and national law.

10.1 Purposes specification, making them explicit and legitimate

Before recruitment, each participant will receive an information sheet including the information on the research ongoing, the information on the treatment of personal data in accordance with the EU Regulation 679/2016 (GDPR) and the informative note for the treatment of personal data.

In the information sheet will be clearly specified the use of data and it will be asked permission also for sharing de identified data in open access repository for further research after the project, by other research teams. In case of denial of this clause, the data associated to that user will not be transferred to the OpenAccess repository.

When research participants are children, the informed consent will be signed not only by them but also by their legally authorised representative and it will be ensured that they have sufficient information to enable them to provide this on behalf and in the best interests of the participants.

The informed consent explicitly declares and informs subjects that they will participate in a research project on a voluntary basis and of the risks related to their data processing.

Personal data will be collected only for the specified, explicit and legitimate purposes of the ESSENCE pilot test and not further processed in a manner that is incompatible with those purposes, in accordance with the Art. 5.1 b) of [GDPR].

In case of dissemination of results data will be presented in an anonymous format as in the standard scientific publication policy. This is also said to and approved by the users in the informed consent.

10.1.1 Data consent properties

Prior to the participation all subjects are informed about the data processing procedure and outcomes and their right about data management (access, rectification, opposition, erasure, portability and automated decision making) through the informed consent they sign to enter into the study.

The information is provided to subjects by verbal and written means, in the mother tongue of each participant in their own living country.

A checklist is provided to assure the user has the full comprehension and understanding of participation and data treatment during and after the trial.

After this time, during data collection we can distinguish two cases:

- data processing in the pilot;

- data processing outside the pilot.

During the pilot, the users will receive feedback and alerts from the AI monitoring module which will suggest activities and inform about any eventual change in behaviour (e.g., an anomaly detected in voice analysis features or handwriting features with respect to their normal patterns). Other data which will be visible to the user are summaries on game scores performed with the CBAC.

After the pilot, data are stored in a safe and encrypted way on the project servers, and anytime anywhere the subject is entitled to ask for retrieve these data and processed information.

The consent is obtained by signing the form prepared by the consortium after he/she has read it and had sufficient time to ask questions to the responsible of the pilot: after this he/she can freely and aware decide to sign or not and be recruited or not for the trial.

For exercising the rights regarding access and data portability, the subject should contact the responsible of the pilot in his/her country which is the entitled person, and/or the DPO of the involved institution and ask for access or data portability.

The contact mean is the writing of an e-mail to the above-mentioned responsible people (whose contact details are in the informed consent sheet in the hands of the user) asking for the required action.

In accordance with Art. 20 of GDPR, by virtue of the right to request data portability, the users have a right to receive a copy of their personal data in a structured, commonly used, machine-readable format. The users may also request that the responsible of the pilot in his/her country transfer your data to another data controller indicated by him or her.

For exercising the rights regarding rectification and erasure, the subject should contact the responsible of the pilot in his/her country which is the entitled person, and/or the DPO of the involved institution and ask for rectification and/or erasure.

The contact mean is the writing of an e-mail to the above mentioned responsible peoples (whose contact details are in the informed consent sheet in the hands of the user) asking for the required action.

The required operation should be done without undue delay.

In accordance with Art. 17 of GDPR, by virtue of the right to request data rectification and erasure, the users have a right to receive a notification of the rectification and erasure of their personal data without undue delay. The users may also request that the responsible of the pilot in his/her country transfer your data to another data controller indicated by him or her.

All data will be treated only in accordance with the ESSENCE objectives stated in the informed consent.

However, if the subject considers out of scope some data processing, for exercising the rights to restriction and objection, the subject should contact the responsible of the pilot in his/her country which is the entitled person, and/or the DPO of the involved institution and ask for them.

The contact mean is the writing of an e-mail to the above-mentioned responsible peoples (whose contact details are in the informed consent sheet in the hands of the user) asking for the required action.

In accordance with Art. 21 of GDPR, by virtue of the right to request data restriction or objection, the users have the right to receive a notification of the conclusion of the procedure in a structured, commonly used, machine-readable format.

The following CA clauses are relevant.

39.2 Processing of personal data by the beneficiaries

The beneficiaries must process personal data under the Agreement in compliance with applicable EU and national law on data protection (including authorisations or notification requirements).

The beneficiaries may grant their personnel access only to data that is strictly necessary for implementing, managing and monitoring the Agreement.

The beneficiaries must inform the personnel whose personal data are collected and processed by the Commission. For this purpose, they must provide them with the privacy statement(s) (see above), before transmitting their data to the Commission.

39.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under Article 39.2, the Commission may apply any of the measures described in Chapter 6 of the CA.

10.2 Confidentiality

ESSENCE partners must retain any data, documents or other material as confidential during the implementation for the project. Further details on confidentiality can be found in Article 36 of the Grant Agreement along with the obligation to protect results in Article 27.

10.3 Legal basis on data collection

The legal basis is represented by the GDPR regulation and all the national laws regarding data protection and research with human beings.

ESSENCE data are obtained after the subject has signed the consent after detailed information ex art. 6 lect. a) of GDPR.

This is in line with and respectful of the principle of privacy by design (art. 25 GDPR, privacy by default). Only personal data strictly necessary for data processing, e.g. contacts, will be collected and kept separately from data collected by the ESSENCE platform and analysed by the AI module. The informed consent is provided in written form in accordance with deontological rules.

Furthermore, and first of all, the driving principle that ESSENCE consortium is adopting is not to affect dignity and safety of people. All measures and procedures have been designed and put in place with these two pillars.

11 Risks on data management

In the following table we are reporting all the planned measures used to augment data security.

ID	Measures	Application
1	Encryption	Essential security mechanisms will be implemented, building on strong AES encryption. Data in transfer will secured with the TLS protocol. Data at rest will be protected with encryption and relevant authentication and authorisation mechanisms. Authentication will be done using cryptographically signed tokens (JWT). After successful authentication, authorisation for access to services/data is enforced checking user assigned roles against access rights (privileges) assigned to different roles. The platform therefore provides protection at database and communication levels. The authentication data will include sensitive data (email, name surname) and will be stored on a secured Database separated from the Data Center and they will be encrypted. All other data will be stored as pseudonymized. Encryption keys are generated using a random source with high entropy (OpenSSL on an AMD Ryzen host). The encryption key is not stored on the same machine as the encrypted database, but on a remote virtual machine in a key vault. Change in the case of key compromise includes manual database decryption and re-encryption with a newly generated key.
2	Partitioning data	Data are partitioned on different servers by splitting over identification data from sensitive data. Even sensitive data are partitioned to assure the best privacy level. In particular, the authentication data include all personal sensitive data (email name surname mobile number) and an encrypted data storage will be used for them. These data are stored in separate servers with respect to all the other data. The information stored in each module's data server (e.g., the CBAC) will not allow the association between personal data and behavioral/health data. This is achieved with two alternative approaches. The first operates through data partitioning: the personal sensitive data will never be locally stored in the module's data server, instead, they will be retrieved on a need basis by exploiting specific API endpoints provided by the authentication module. When partitioning with API-based retrieval cannot be efficiently applied and a copy of the personal sensitive data will need to be stored in the module's data server, such a copy will be always encrypted.
3	Logical access control	Only internal personnel have access to ESSENCE repository. A dedicated data repository will be set up for data from the users in the pilot. Only a subset of personnel (the responsible persons of the pilot sites and specially identified operators, and the DPO) will be allowed to access the user data (both personal and sensitive). Access will be granted with a userID/password mechanism.
4	Traceability (logging)	Access to data will be granted with a userID/password mechanism. A log file to trace accesses and operations will be implemented.

5	Archiving	The generated data (indicators) are shared in open access one month after data generation as declared in the Article 29.3 of the Grant Agreement. The shared data will be anonymized and will be shared in Zenodo.
6	Paper document security	Paper documents will be duplicated (photocopies) and digitalized and stored in a secure and locked placed with access limited only to the personnel involved in the recruitment. The digital copy of the documents will also be stored in the repository of the ESSENCE project.
7	Operating security	Operations security will be aligned with the ISO 27002 standard code of practice, i.e. the best practice recommendations for implementing and maintaining an information security management system. The recommendations cover procedures and responsibilities, malware protection, backup, logging and monitoring, control of operational software, technical vulnerability management and information systems audit coordination. Our approach to addressing these aspects is described in this document.
8	Clamping down on malicious software	ESSENCE is a closed infrastructure running on AWS servers (limiting geographically to EU the data storage) and using the Amazon Layer 4 Virtual Private Cloud Firewall for protecting communication among components and perimeter towards public internet. In addition, an Application Layer Firewall (Layer 7) is set up to assure the minimization of the access risk.
9	Managing workstations	The partner responsible for the infrastructure and integration (SCOM) is ISO 27001 certified and compliant. Moreover, all partners feature IT departments, which centrally implement relevant technical measures and security policies, including automatic workstation locking, regular updates, configuration, physical security, etc.
10	Website security	The website communication is secured according to relevant recommendations, e.g. the ANSSI. Access to website and servers from public internet is protected by the TLS protocol. Authentication and authorisation is done using cryptographically signed tokens (JWT), more details on JWT and encryption key management are provided above in the table item 1. Note that JWT token has validity limited to 5 minutes to limit misuse in case of token compromise.
11	Backup	The data backup is developed and provided according to the needs and policies defined in the experimental protocol of the study. The project servers hosting relevant data are running in the AWS cloud environment and AWS backup service will be used.
12	Maintenance	By using the AWS cloud services hardware maintenance is transferred (outsourced) to Amazon. Remote monitoring and maintenance of components/applications is featured, where each partner has remote administrative access and responsibility for the maintenance of their respective component/app running in the cloud infrastructure. Maintenance of cloud infrastructure is provided by the ESSENCE partner SCOM. They are a qualified and ISO 9001 and ISO 27001 quality certified IT entity.
13	Network security	Network security management is based on the Amazon Virtual Private Cloud (VPC), most notably the Security Groups for VPC and Network Access Control Lists (ACL). A Security group acts as a virtual firewall for a virtual machine (VM) instance to control inbound and outbound traffic. When an instance is launched in a VPC, up to five security groups can be assigned to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in a VPC can be assigned

		to a different set of security groups. A network access control list (ACL) is an optional layer of security for a VPC that acts as a firewall for controlling traffic in and out of one or more subnets. One might set up network ACLs with rules similar to one's security groups in order to add an additional layer of security to one's VPC. Each partner has its own Security Group, internally these groups can access each other's networks. External access to these security groups is protected through firewalls (more details are provided in the table item 9 above).
14	Monitoring network activity	ESSENCE services are running in the AWS Cloud infrastructure, network level protection is provided by the inherent AWS security services, such as network security groups and ACL's, as described in table item 13 above. We additionally need to monitor the application layer (Layer 7) access, which is monitored and controlled by the Application layer firewall.
15	Personnel management	Personnel will participate in pilot procedures definition and both technical and clinical operators will be properly trained before the pilot start. Dry run tests are done and confirm the commitment and preparation of the personnel for the trial in technical, clinical, legal and ethical issues.
16	Pseudonymization	The personal data management procedure implements pseudonymization, i.e., processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Hash technique is implemented.
17	Personnel training	The first adopted measure is the training of the project staff and their need to be aware of the risks involved in processing personal data and how to mitigate those risks though proper measures and countermeasures.

Table 3. Data security measurments

Additional risks can be grouped under illegitimate access to data,

11.1 Illegitimate access to data

If an illegitimate access to data, we envisage here a moral feeling of invasion of privacy. This might happen for misuse of information from the qualified personnel, loss of personal device (e.g. tablet) or breach into Essence platform.

This risk is miminised as data protection in the platform has been enforced by design. The following control and design measures have been adopted for this aim:

- Encryption of sensitive data
- Partitioning data
- Traceability (logging)
- Clamping down on malicious software
- Backup
- Maintenance
- Personnel management and training
- Paper on document security

- Logical access control
- Pseudo-anonymization
- Managing workstations
- Website security
- Monitoring network activity
- Network security
- Operating security

For this reason we estimate the risk severity as negligible because the only result of a data breach could result in feeling of invasion of privacy without a real or objective harm. For the same reason the probability that this hazard occurs can be considered negligible.

11.2 Unwanted modification of the data

The loss of data integrity can let the users encounter inconvenience from unauthorised alteration of health data (signals and statistics), which could even make it difficult for them to receive appropriate feedbacks in the form of notifications and/or alerts and could result in unnecessary tele-consultations. This may potentially raise mental stress.

The loss of data availability could again hinder the timely and accurate feedbacks to subjects.

The main threats that can lead to this hazard are: Data Hacking from external sources, Data manipulation by internal personnel without proper qualification or training, Software bias or errors

This risk is miminized as data protection in the platform has been enforced by design. The following control and design measures have been adopted for this aim:

- Encryption of sensitive data
- Traceability (logging)
- Clamping down on malicious software
- Backup
- Maintenance
- Personnel management and training
- Paper on document security
- Logical access control
- Pseudonymization
- Managing workstations
- Website security
- Monitoring network activity
- Network security
- Operating security

Due to the implemented controls, if on one side the risk severity could be high in case a person is receiving wrong feedbacks and alerts, on the other side the overall risk severity is estimated as limited as this is very difficult to happen. Indeed, no final decisions on health status are taken solely by the AI monitor but users will have the possibility to do teleconsultation with clinicians and teachers to

understand the potential anomalies highlighted by the AI models. For the same reason the probability that this hazard occurs can be considered negligible.

11.3 Data disappearance

Data disappearance can result in wrong alerts and feedbacks from the system to the user, because of missing data. This may be attributed to hardware or Software malfunctioning or to hacking. Main risk sources are identified in:

- External human resources
- Internal Human resources
- Hardware and software malfunctioning

This risk is miminized as data protection in the platform has been enforced by design. The following control and design measures have been adopted specifically for this aim:

- Backup,
- Clamping down on malicious software
- Maintenance
- Logical access control
- Personnel management

Resorting to data center that by design guarantee data safety through redundancy and this makes this hazard unlikely to happen. Also proper personnel training is minimizing the risk for the internal personnel.

11.4 RISK OVERVIEW

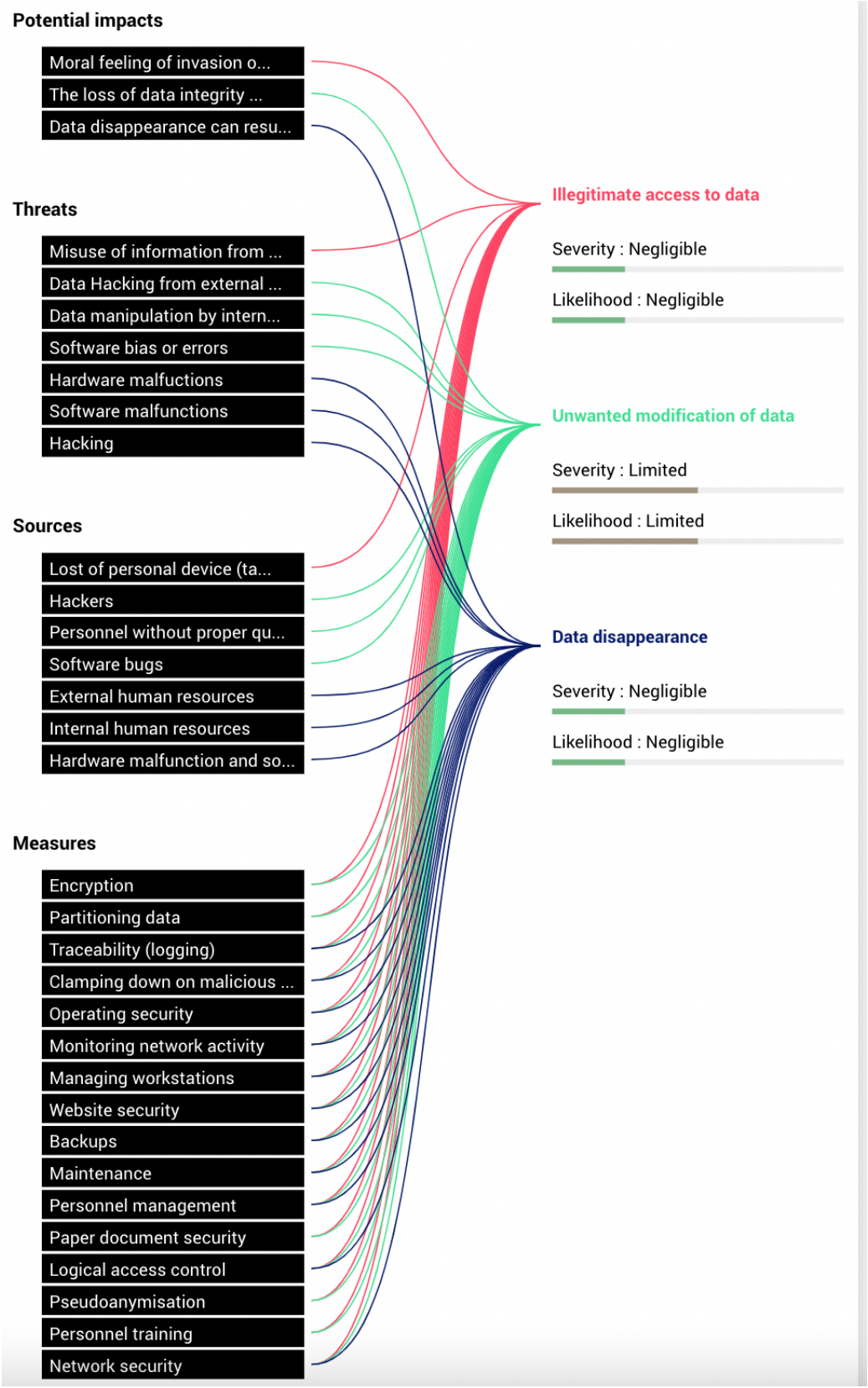

Figure 4. Risk overview.

Figure 4 reports the risk seriousness on illegitimate access to data (I), Unwanted modification of data (U) and Data disappearance (D) before (on the left) and after the action plan on the Unwanted modification of data (on the right) reported in the DPIA.

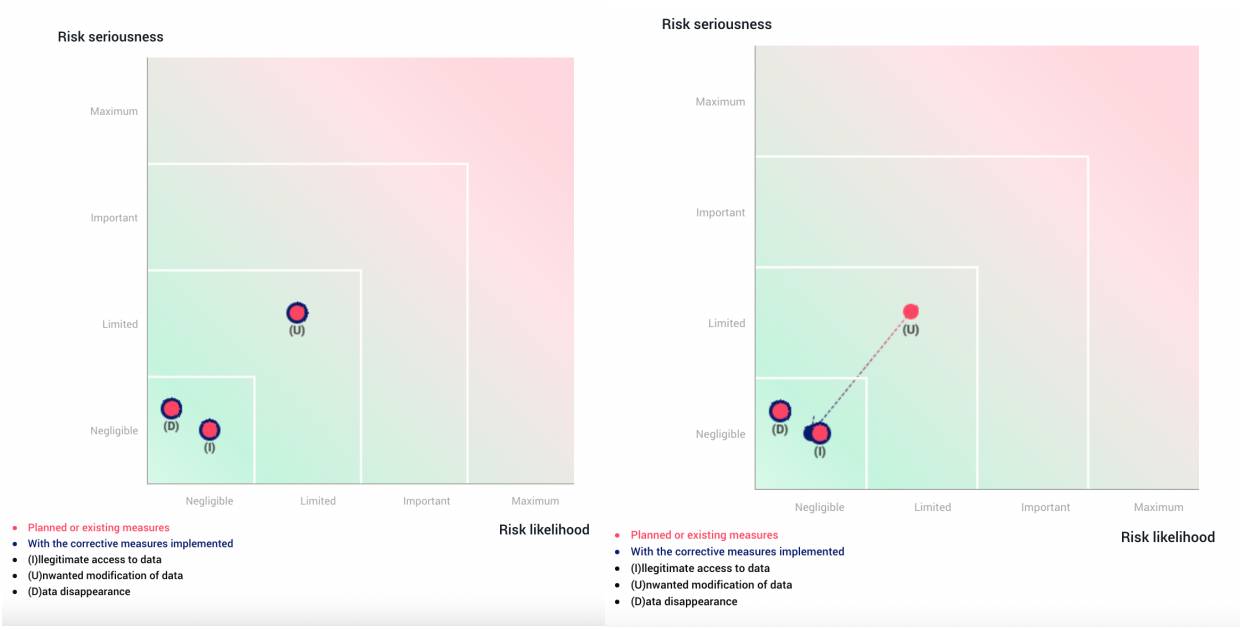

Figure 5. Risk seriousness before and after the action plan

The abovementioned measures make also the risk related to unwanted modification of personal data low.

12 Datasets description

More specifically, each dataset generated during the project will be recorded in a file with a standard format and allocated with a dataset identifier. The dataset file will be hosted at the ESSENCE data repository alongside its metadata file. This dataset information will be included in a web page file at the beginning of the documentation, and updated with each version. The final data model will be included in D1.3 Final Data Management Plan.

For each dataset, ESSENCE proposes the creation of:

1) A single identification name for the dataset
2) An identification metadata file describing the characteristics of the dataset
3) An extended metadata file describing the particularities of the content of the file

12.1 Single identification name of the dataset

ESSENCE naming convention for project datasets will comprise of the following:

1. A unique chronological number of the datasets in the project will be added.
2. The title of the dataset.
3. For each new version of a dataset it will be allocated with a version number which will be for example start at v1.0.
4. A prefix "ESS" indicating an ESSENCE dataset.
1. A unique identification number linking with the dataset work package and deliverable/task e.g., "W4_D4.X": 01_ Monitoring Data_v1.0._ESS_W4_D4.X.xlsx

12.2 Identification medatata file

A temptative identification metadata file that would describe the dataset characteristics, formats and volume are given in the following table:

Dataset Identifier	The ID allocated using the naming convention
Tile of Dataset	The title of the dataset which should be easily searchable and findable
Responsible	Partner Lead partners responsible for the creation of the dataset
Partner in charge of the data collection	
Partner in charge of the analysis	
Partner in charge of the data storage	
Relate Work Package	The associated work package this dataset originates
Data access	CONFIDENTIAL / ONLY FOR MEMBERS OF THE CONSORTIUM / OPEN
Dataset Description	A brief description of the dataset
Dataset Benefit	What are the benefits of the dataset
Dataset Dissemination	Where will the dataset be disseminated
Type Format	This could be DOC, XLSX, PDF, JPEG, TIFF, PPT etc.

Expected Size	The approximate size of the dataset
Source	How/why was the dataset generated
Repository	Expected repository to be submitted
Date of RepositorySubmission	The date of submission to the repository can be added once it has been submitted
Keywords	The keywords associated with the dataset
Version Number	To keep track of changes to the datasets
Public	YES/NO
Link to metadata file	
Link to data repository	
Version of dataset	
Date of latest update	
Update history	
Embargo periods	
Reason of non availability	
The file contains personal data	YES/NO
Written consent of the participants	YES/NO

Table 4. ESSENCE dataset identification metadata description

12.3 Extended metadata file

An extended metadata file concerning the dataset technical characteristics will be uploaded with the dataset. This metadata file would follow the following structure:

This metadata file was generated on <insert date> by <insert name>

GENERAL INFORMATION

---

1. Title of Dataset:

2. Dataset Identifier in Repository:

2. Responsible Partner:

3. Author Information:

Investigator Contact Information

Name:

Email:

Supervisor Contact Information

Name:

Email:

Co-Supervisor Contact Information

Name:

Email:

3. Date of data collection:

4. Geographic location of data collection (where was data collected?):

6. The title of project and Funding sources that supported the collection of the data:

SHARING/ACCESS INFORMATION

---

1. Licenses/access restrictions placed on the data:

2. Link to data Repository:

3. Links to other publicly accessible locations of the data:

4. Links to publications that cite or use the data:

5. Was data derived from another source?

If yes, list source(s):

DATASET & FILE OVERVIEW

---

1. This dataset contains X sub-dataset as listed below:
    a. Datasheet name:
    b. Datasheet name:
    c. Datasheet name:
    d. Datasheet name:
2. What is the status of the documented data? – “complete”, “in progress”, or “planned” Are there plans to update the data?

13 References

Reference website for updates about Data Protection in the EU:

https://ec.europa.eu/info/law/law-topic/data-protection

Reference website for updates about Cyber Security strategy in the EU:

https://ec.europa.eu/digital-single-market/en/cybersecurity

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) can be found at:

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679

Ethics and Data Protection relevant doument:

https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf

WHO guideline on digital health interventions:

https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1

Towards a framework for policy development in cybersecurity - Security and privacy considerations in autonomous agents:

https://www.enisa.europa.eu/publications/considerations-in-autonomous-agents

Recommendations on European Data Protection Certification:

https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification

Handbook on European data protection law - 2018 edition Council of Europe

https://www.coe.int/en/web/data-protection/documentation

Handbook on Security of Personal Data Processing, Enisa

https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Guidelines on Data Management in Horizon 2020

http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oapilot-guide_en.pdf

Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020, Version 2.0, 30 October 2015:

http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oapilot-guide_en.pdf

Annotated GA version 30 October 2015, p. 218

Fact Sheet: Open Access in Horizon 2020:

http://www.nks-swg.de/media/content/FactSheet_Open_Access.pdf

Webpage of European Commission regarding Open Access:

http://ec.europa.eu/research/science-society/open_access

European Commission (2016): Guidelines on Data Management in Horizon 2020, Version 2.1, 15 February 2016:

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

European Science Foundation (2011), European Code of Conduct for Research Integrity of ALLEA (All European Academies) and ESF, March 2011:

http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-ofconduct_en.pdf

FAIR data principles (FORCE11 discussion forum):

https://www.force11.org/group/fairgroup/fairprinciples

OpenAIRE repository:

https://www.openaire.eu/opendatapilot-dmp

UK Data Service:

https://www.ukdataservice.ac.uk/manage-data/document

14 Appendix A

Functionality	Responsible	Brief Description	Target Population	Measurements	Exampe of Indicators
Handwriting Standalone	POLIMI	Daily unconstraint handwriting to monitor features correlated to the handwriting performance and tremor	Child Senior	Acceleration Gyroscopes and tip force raw data	handwriting and tremor indicators such as tilt, approximate entropy
Voice Analysis Standalone	SG	Voice acoustic features extracted on the fly during phone call to monitor cognitive decline, araousal and valence	Senior	-	acoustic features computed on the fly such as pitch...
Serious Games 1	POLIMI	Mini games in three domains of learning: writing reading and calculation; these games should be played by all children and if the child is identified as a child at risk the game should be planned by the teacher as reinforcement	Child	Raw data of the pen interaction of the user with the tablet during the game (x,y coordinate, pressure)	game score, frequency of use, game level and if possible features correlated to handwriting smoothness ..

Serious Games 2	POLIMI	Serious game used to detect potential signs of learning delays; 1. copy square; 2. copy sequence; 3. tunnel square; 4. tunnel ELE	Child	Raw data of the pen interaction of the user with the tablet during the game (x,y coordinate, pressure)	
Clinical teleconsultation 1	UMIL/POLIMI	The teleconsultation module will be provided inside the CBAC. The module will provide activities to be performed during teleconsultation (such as cognitive tests and cognitive exercises). Two users with different roles: consultant and consultee. The interface will show the videos of the two roles, an active area will be shown and used to display tests or images or to let the consultee draw or write during the visit. In this latter case the drawing of the consultee is shown in real time to the consultant and the consultant can collect results and fill in reports.	Senior/Child with clinician	Digital Clinical Test raw data	Report

Postural Exergames for elders	UMIL	Postural exergames carried out with the RGB-D camera and skeleton analysis to extract the user movement.	Senior	-	game score, frequency of use, game level and features correlated to postural control
Virtual gym for elders	UMIL	It is a virtual room in which elders can see and speak each other while in a specific part of the screen they are following a tutor that is doing exercises	Senior	-	frequency of use
Physical education	UIN	The same setting as virtual gym for elders but devoted to children	Children	-	frequency of use
Tutorial for children	UIN	The same setting as virtual gym but finalized at teaching children how to hold the pen and other abilities	Children	-	frequency of use
Multiplayer Cognitive Games	UMIL	Cards, Pictionary, Puzzle, Ruzzle, Bingo of rhyms and syllabus	Senior Child	-	frequency of use
Health Data Diary	SXT	It is a tablet UI that allows the senior to insert health data to be monitored: weight, quality of the day (1-5), sleep quality, specialistic visit carried out, GP visits carried out, ..	Senior		Systolic and diastolic values Heart rate Weight (kg) Hours of sleep Body temperature Glucose index Coagulation index Daily steps (suggested by ESE) SpO2 QoL/mood question with emoticons

Digital Tests (TMT, Bells)	UMIL	Digital Tests to be performed by the senior alone with the automatic supervision of the SW	Senior	raw x,y inputs of the trace executed during the test	test score
Therapy reminder App	UMIL	It is an android application running on the recruited senior smartphone that assist him in reminding the therapy	Senior	-	frequency of use
Dashboard	SXT	Visualization of indicators relevant to professionals		-	frequency of use
Virtual rooms for between generation exchange	UMIL	HomeWorks shared	Child Senior	-	frequency of use