Project Title:	**Sensing and predictive treatment of frailty and associated co-morbidities using advanced personalized models and advanced interventions**
Contract No:	690140
Instrument:	Collaborative Project
Call identifier:	H2020-PHC-2014-2015
Topic:	PHC-21-2015: Advancing active and healthy ageing with ICT: Early risk detection and intervention
Start of project:	1 January 2016
Duration:	36 months

Deliverable No: D9.6 vers.a (D9.9)

Ethics, Safety and mHealth Barriers (regulation, legislation, etc.) Manual (vers. a)

Due date of deliverable:	M5 (1st June 2016)
Actual submission date:	6th June 2016
Version:	1.1
Lead Author(s):	John Ellul (UoP), Vasileios Megalooikonomou (UoP)
Other lead partners:	Cristiana Degano (SIGLA), Luca Bianconi (SIGLA), Kimon Volikas (MATERIA), Athanase Benetos (INSERM)

Horizon 2020
European Union funding
for Research & Innovation

Change History

Ver.	Date	Status	Author (Beneficiary)	Description
0.1	18/3/2016	draft	John Ellul (UoP)	First Draft
0.2	28/3/2016	draft	Vasileios Megalooikonomou (UoP)	Several additions/revisions
0.3	6/4/2016	draft	Kimon Volikas (MATERIA) and Athanase Benetos (INSERM)	Incorporation of sections related to EU and local policies
0.4	12/4/2016	draft	Konstantinos Moustakas (CERTH)	Review and revisions
0.5	21/4/2016	draft	Andreas Kanavos (UoP), Christos Makris (UoP)	Additions on technical aspects
0.6	26/4/2016	draft	Vasileios Megalooikonomou (UoP)	Additions on technical aspects
0.7	6/5/2016	draft	Kyriakos Sgarbas (UoP), Nikos Fazakis (UoP)	Additions on technical aspects
0.8	14/5/2016	draft	Ilias Kalamaras (CERTH)	Additions on technical aspects
0.9	20/5/2016	draft	Cristiana Degano (SIGLA) and Luca Bianconi (SIGLA)	Several additions on recent EU directives
1.0	25/5/2016	draft	Kimon Volikas (MATERIA) and Athanase Benetos (INSERM)	Final internal review comments
1.1	4/6/2016	Final	John Ellul (UoP) and Vasileios Megalooikonomou (UoP)	Final document incorporating reviewers comments

EXECUTIVE SUMMARY

The purpose of this document is to guide FrailSafe researchers in ensuring that the principles and legal requirements of biomedical research and Information and Communications Technology (ICT) research are adhered to.

The primary purpose is not to rehearse the details of research ethics as applied in the conventional setting of a medical research team working with patients in a healthcare environment – these details are well-known and available elsewhere. The main purpose of this Ethics Blueprint is to survey the principles and legal requirements pertaining to work in FrailSafe where biomedical data is incorporated into an ICT research and development project.

First, we define the specific contexts in which research ethics and data protection issues are relevant in FrailSafe. Next, we define personal data (informative data and sensitive data), since this is a key concept. Subsequently, we review major legislation and guidelines relevant to research involving personal data, especially at the interface between health care and ICT. Finally, we make a list of recommendations, relevant to those aspects of FrailSafe which will process personal data.

All the research and innovation activities carried out under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols [REGULATION (EU) No 1291/2013].

Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination, to the protection of geolocation data and to Web and social media mining issues, and to the right to be forgotten.

.

DOCUMENT INFORMATION

Contract Number:	H2020-PHC–690140	**Acronym:**	FRAILSAFE
Full title	Sensing and predictive treatment of frailty and associated co-morbidities using advanced personalized models and advanced interventions		
Project URL	http://frailsafe-project.eu/		
EU Project officer	Mr. Ramón Sanmartín Sola		

Deliverable number:	9.6 (a)	**Title:**	Ethics, Safety and mHealth Barriers (regulation, legislation, etc.) Manual (vers. a)
Work package number:	9	**Title:**	Management & Ethics

Date of delivery	**Contractual**	1/6/2016	**Actual**	6/6/2016
Status	Draft ☒		Final ☐	
Nature	Report ☒	Demonstrator ☐	Other ☐	
Dissemination Level	Public ☒	Consortium ☐		
Abstract (for dissemination)	This Ethics manual aims to outline the project's plan towards issues related to the safety and privacy as well as to ensure the fulfillment of high ethical standards during the project duration			
Keywords	FrailSafe, Ethics, website, frailty, repository, social media			

Contributing authors (beneficiaries)	John Ellul (UoP) and Vasilis Megalooikonomou (UoP)			
Responsible author(s)	John Ellul (UoP)		**Email**	ellul@upatras.gr
	Beneficiary	UoP	**Phone**	+30-2610-999854

TABLE OF CONTENTS

TABLE OF FIGURES

No table of figures entries found.

1 Brief Overview of the FrailSafe Project

Ageing population is increasing worldwide and it is estimated that by 2050 there will be approximately two billion people aged over 65 years. While the increasing life expectancy is a positive outcome due to long-lasting health and social improvements, there is still much to do in improving the quality of life. A consequence of age related decline is the clinical condition of frailty. By the term frailty we refer to a medical syndrome with multiple causes and contributors that is characterized by diminished strength, endurance, and reduced physiologic function that increases an individual's vulnerability for developing increased dependency and/or death. It is characterized by multiple pathologies such as weight loss, and/or fatigue, weakness, low activity, slow motor performance, balance and gait abnormalities. Frailty makes elderly more vulnerable to stressors and has major health care implications which include increased risk of incident falls, delirium, worsening of mobility, disability, hospitalization, institutionalization, and mortality, which eventually increase the burden to cares and costs to the society.

The lack of standardized definition of frailty causes heterogeneity in studies. Frailty as a syndrome is characterized by a cluster of symptoms and signs that can be grouped in a physical, cognitive, functional, and social domain. Frailty seems a dynamic, and not an irreversible process; it seems preventable, may be delayed, or even reversed. Transition between frailty states, i.e. non-frail, pre-frail, frail, has been documented. The rate of progression varies among elderly and some cases show sudden onset and rapid transition, whilst others slow and progressive changes. Interventions that alter the natural course of frailty may prevent or reduce adverse health outcomes, and thus, may be proved beneficial not only to individuals, but to families, carers, and society.

FrailSafe, is the acronym of this HORIZON 2020 project, which addresses all of the above domains and challenges, i.e. lack of an agreed single operational definition of frailty, lack of a reliable frailty model, understudy of cognitive, functional, and social domains in addition to the physical domain of frailty, the fact that behavioral changes may precede the transition to pre-frail or frail, the need to develop real life tools for the assessment of physiologic reserve and the need to test interventions that alter the natural course of frailty. FrailSafe also aims to better understand frailty in relation to co-morbidities; to identify quantitative and qualitative measures of frailty through advanced data mining approaches on multiparametric data and use them to predict short and long-term outcome and risk of frailty; to develop real life sensing (physical, cognitive, psychological, social) and intervention (guidelines, real-time feedback, AR serious games) platform offering physiological reserve and external challenges; to provide a digital patient model of frailty sensitive to several dynamic parameters, including physiological, behavioural and contextual; this model being the key for developing and testing pharmaceutical and non-pharmaceutical interventions; to create "prevent-frailty" evidence-based recommendations for the elderly; to strengthen the motor, cognitive, and other "anti-frailty" activities through the delivery of personalised treatment programmes, monitoring alerts, guidance and education; and to achieve all with a safe, unobtrusive and acceptable system for the ageing population while reducing the cost of health care systems.

FrailSafe is an international partnership of nine partners from six countries. Clinical partners include: the University of Patras (Greece, project coordinator), INSERM (France), and MATERIA (Cyprus). ICT partners are Smartex and Gruppo SIGLA (Italy), CERTH and Hypertech (Greece), and AGE Platform Europe (Belgium).

1.1 Overview of FrailSafe Data Collection

During FrailSafe project 438 participants, men and women, will be enrolled in the study. This will involve the following:

A. Participant's data known only to local research team

Collection of personal data i.e. personal demographic data (name, address, telephone numbers, emails)

B. Participant's anonymised data, known to FrailSafe research team

The FrailSafe research team involved with handling of data are based in Cyprus, France, Greece, and Italy. These data include:

- General demographic data, i.e. living condition, housing, place of residence
- Social Interaction data, i.e. time spent with others, social contacts
- Past and current medical history, current treatment
- Clinical assessment i.e. biometric data, assessment of cognition and mood, pain, vision, hearing balance and gate, activities of daily living
- Recording of adverse events i.e. falls, fractures, hospitalization, date and cause of death
- Collection of previously typed or written text (only if they agree to provide), and samples of typed or written text obtained during clinical assessment visits
- Self filled in questionnaires on the use of internet and social media platforms, and personality traits
- Nutrition data from questionnaires
- Collection of blood specimen from all participants to be send to INSERM
- Collection of blood specimen from participants in Greece to be analysed locally
- Provision of guidelines on healthy eating habits and physical exercise
- Satisfaction interviews
- Data from wearable sensors i.e. heart and respiratory rate, balance, posture, indoor and outdoor activities (via IMUs) and spatial mobility (via GPS)
- Data from indoor sensors (beacons) i.e. time spent in each room of the house (with no body image recording)
- Data collected whilst playing electronic games
- Data from dynamometers for strength evaluation
- BP (via BP monitors), weight (via scales), arterial stiffness (via mobil-o-graphs), waist and chest circumference (via tape measure)
- MRI or DEXTA will be carried out in a small number of participants from the Greek centre

It is anticipated that the FrailSafe project will involve continuous recording of sensors' data in real time, and that these data will be processed offline as well as in real time using methods and models to detect relevant clinical information and events; and that these data will be associated with the Clinical Health Profile, held in database, which will not include personal identifiers, as data from all sources will be carefully anonymized and encrypted.. Whilst sensor data will not include video recording, the in-door location of the participant will be recorded via beacons. The data recorded in real time will reveal how long the participant stays in each room of his/her house and how often moves and changes rooms within his habitation, including toilet. The activities of the participant in each location will not be known to the researchers, as this information cannot be recorded by the chosen system of beacons. Participants' spatial mobility will also be measured, via GPS, in their out-door activities.

It is needed to highlight that FrailSafe is also based on the concept of IoT (Internet of Things) based architecture, as understandable by the devices mentioned above. Then, it is of paramount importance to assure security and privacy, ideally in near real-time, particularly in the following major components: Data Acquisition, Data Transmission, Cloud Processing.

2 Overview of Health, Safety and Wellbeing

A. In this research we will ensure the following areas:

- **a.** personal dignity (including treating the individual with respect)- ability to try to achieve personal daily living aims and follow choices and preferences with undiminished dignity and privacy
- **b.** physical and mental health and emotional wellbeing

If the technology recognizes or foresees danger with potential impact upon its participant, there is an opportunity to respond in order to prevent or minimize the danger

- **c.** protection from abuse and neglect

Each potential participant will be informed about any risks identified and they will be supported to decide whether they wish to give consent to engage with the project.

- **d.** control by the individual over their day-to-day life (including over the care and support provided and the way they are provided)

Agreement to participate in the project must be entirely voluntary and participants should be able to withdraw their consent at any point in the project without requirement to explain the reason behind their decision to withdraw.

B. Information gathering, data protection and sensitivities

Personal privacy of participants will be respected. For this reason, the reporting process of research outcomes will ensure the participants' privacy and will fulfil all relevant data protection requirements. All data gathered are going to be anonymised and encrypted, and furthermore, access to any sensitive data will be restricted. Access to such data will be implemented by staff authorised to do so in accordance with the terms of the project and in compliance with local security of information and confidentiality policies. Therefore, all researchers will be made aware of this requirement and responsibility will be assigned to specific individuals for the timely assessment of and response to such concerns (research outcomes will not contravene fundamental rights such as privacy and data protection).

Participants will be fully informed about all the ways in which information will be gathered, exchanged and shared. Also, they will be informed that are free to leave the study anytime, if so wish; in this case, the recording of any further information will be prevented and all gathered data will be erased. In the event that participants discontinue their participation, without withdrawing their consent, the recording of any further information will be prevented, but gathered data will be used according to protocol specifications and ethics guidelines. Participants will be informed that all devices, wearable or not, will have an "off" function designed to pause recording of information to be used any time, for whatever reason, in order to protect privacy at certain times.

Personal health data must be treated as 'sensitive personal data'. The dignity of each participant will be respected, by following consent procedures, appreciating the voluntary nature of their participation, and ensuring the security of any gathered personal data. The wearable device will be designed with respect for the integrity of the participant. No unauthorised information will be gathered, nor will the devices interfere with normal functioning in any way without prior consent of participants. The device will pose no risk to short or long-term health. Procedures will be in place to identify any possibility of misuses or abuses of data, as soon as these arise, and safeguards will be applied to prevent this occurring.

3 Legal Framework for Privacy Protection

Under the European Union (EU) law, personal data is defined as “any information relating to an identified or identifiable natural person”. The collection, use and disclosure of personal data at a European level are regulated in particular by the following directives:

- Directive 95/46/EC on protection of personal data (Data Protection Directive) [1]
- Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) [2]
- Directive 2009/136/EC (Cookie Directive) [3]
- European Human Rights Convention [4]
- UK Data Protection Act 1988 deals with similar issues [5]
- formulated recommendations of previous FP7 research projects (ICT FP7 Ethical Guidelines) [6] with respect to privacy and data protection,
- Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data [7]

Directives generally do not directly apply in the EU countries and need to be nationally implemented by each country through laws and regulations. As countries have some freedom in the implementation of directives, stricter requirements than those prescribed by the directives may apply in certain EU countries. Furthermore, the national data protection legislation is, in many respects, complemented or overlapped by sector specific legislation that also needs to be considered. Therefore, in order to get a clear and comprehensive picture of the data protection requirements, it is important to check the national frameworks, national data protection laws, unfair competition legislation, telecommunications laws and any other local data protection regulations.

Privacy issues arise in platform development projects where testing and pilot execution phase exists, as collection of information about individuals, will be required. A crucial aspect of the discussion around personal data processing and protection is related to the deployment of the offered services in a cloud computing environment, as additional risks have to be taken into consideration in this case. The majority of these risks fall within two broad categories:

- Lack of control over the data
- Insufficient information regarding the processing operation itself (absence of transparency)

3.1 EU Legal Framework for Privacy Protection

Privacy is enabled by protection of personal data. According to Regulation EU 2016/679, personal data “means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” [7].

The same Regulation also defines personal data processing as “or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

There are several legal acts within the EU Law that address and regulate these issues:

Charter of Fundamental rights of the EU

- **Article 1** on Human dignity: "Human dignity is inviolable. It must be respected and protected."
- **Article 3** on Right to the integrity of the person: (1) Everyone has the right to respect for his or her physical and mental integrity; (2) in the fields of medicine and biology, the following must be respected in particular: (a) the free and informed consent of the person concerned, according to the procedures laid down by law, […], (b) the prohibition of eugenic practices, […], (c) the prohibition on making the human body and its parts […], (d) the prohibition of the reproductive cloning of human beings"
- **Article 7** states that "everyone has the right respect for private and family life, home and communications"
- **Article 8** regulates that "everyone has the right to the protection of personal data concerning him or her" and that processing of such data must be "on the basis of the consent of the person concerned or some other legitimate basis laid down by law"

Directive 95/46/EC (Data protection Directive)

The Directive regulates the processing of personal data regardless of whether such processing is automated or not. The principle is that personal data should not be processed at all, except when certain conditions are met.

- Article 6 (b): Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."
- Article 7 defines criteria for making personal data processing legitimate:

✓ the data subject has given his consent
✓ processing is necessary for the performance of or the entering into a contract the data subject is party
✓ processing is necessary for compliance with a legal obligation the controller is subject
✓ processing is necessary in order to protect the vital interests of the data subject
✓ processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed
✓ processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Directive 2002/58/EC (Directive on privacy and electronic communications, also known as e-Privacy Directive)

e-Privacy Directive concerns the processing of personal data and the protection of privacy in the electronic communications sector and deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies [2].

- **Article 5** Confidentiality of the communications

✓ Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by

persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

- ✓ Paragraph 1 shall not affect any legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.
- ✓ Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

European Human Rights Convention:

It is also required that any research undertaken complies with the Article 8 of the European Human Rights Convention [4] on the Right to respect for private and family life: “Everyone has the right to respect for his private and family life, his home and his correspondence”.

Directive 2009/136/EC (Cookie Directive)

This Directive amended Directive 2002/58/EC, requiring end user consent to the storing of cookies on their computer. Cookies are hidden information exchanged between an Internet user and a web server stored in a file on the user’s hard disc. They can be used to monitor Internet activities of the user [3].

The Directive states that the measures referred to in paragraph 1 Article 4 of the Directive 2002/58/EC shall at least:

- ensure that personal data can be accessed only by authorized personnel for legally authorized purposes,
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure, and,
- ensure the implementation of a security policy with respect to the processing of personal data.

According to UK Data Protection Act 1988 [5]

Data means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 684, or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject, (b) his/her political opinions, (c) his/her religious beliefs or other beliefs of a similar nature, (d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his/her physical or mental health or condition, (f) his/her sexual life, (g) the commission or alleged commission by him/her of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. In particular, if you are processing sensitive personal data you must satisfy one or more of the conditions for processing which apply specifically to such data, as well as one of the general conditions which apply in every case. The nature of the data is also a factor in deciding what security is appropriate.

The conditions for processing data

Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

- The individual who the personal data is about has consented to the processing.

The processing is necessary: (a) in relation to a contract which the individual has entered into; (b) or because the individual has asked for something to be done so they can enter into a contract.

The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract). The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions. The processing is in accordance with the "legitimate interests" condition.

According to ICT FP7 Ethical Guidelines [6]

FP7 2.1 notes that there are new dangers associated with Information and Communications Technology (ICT) research, and therefore prior risk assessment and "identification of precautionary actions proportional to the potential risk or harm" must be undertaken.

FP7 also notes that:

- "researchers have a duty to alert public authorities to the ethical and practical implications of their ICT research outcomes, as and when particular issues become apparent within the research process"
- researchers must respect each volunteer's right to remain anonymous. Furthermore, "researchers must comply with Data Protection legislation in the Member State where the research will be carried out regarding ICT research data that relates to volunteers"

- it is required "to the extent that an individual, via an ICT implant or wearable computing device, becomes part of an ICT network, the operation of this whole network will need to respect privacy and data protection requirements."
- It is stated that "ICT implants or wearable computing devices must not: allow individuals to be located on a permanent and/or occasional basis, without the individual's prior knowledge and consent; allow information to be changed remotely without the individual's prior knowledge and consent; be used to support any kind of discrimination; […]"

FP7 3.2 ("eHealth12 and genetics") specifies that personal health data must be treated as 'sensitive personal data'. ICT researchers using it have a duty of confidentiality equivalent to the professional duty of medical confidentiality. Therefore:

- The use of personal health data in ICT research for the purposes from which society as a whole benefits must be justified in the context of the personal rights.
- The security of ICT in healthcare is an ethical imperative to ensure the respect for human rights and freedoms of the individual, in particular the confidentiality of data and the reliability of ICT systems used in medical care.

Finally, FP7 3.3 states that

- "Researchers involved in ICT-bio/nano-electronics research proposals should be aware that certain applications, e.g. miniaturised sensors, may have specific implications for the protection of privacy and personal data."

Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data [7]

This recent Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. On 15 December 2015, the European Parliament, the Council and the Commission reached agreement on the new data protection rules, establishing a modern and harmonised data protection framework across the EU, paving the way towards a Digital Single Market Strategy. On 14 April 2016 the Regulation and the Directive were adopted by the European Parliament, on 24 May 2016 the Regulation will enter into force, and it shall apply from 25 May 2018. The Directive enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018 [8]. As a consequence, the FrailSafe project needs to be in accordance with this most recent EU Regulation. In this case, EU Regulations are addressed to all member states and are applied in full; it must be applied in its entirety across the EU without the need for national legislation.

The Regulation regulates the processing of personal data as such:

- Article 5, "Principles relating to processing of personal data":
    - 1. Personal data shall be:
        - (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
        - (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

        - (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
        - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
        - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
        - (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- Article 6, "Lawfulness of processing"
    - 1. Processing shall be lawful only if and to the extent that at least one of the following applies:
        - (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
        - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
        - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
        - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
        - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
        - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
        - Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
    - 2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
    - 3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
        - (a) Union law; or
        - (b) Member State law to which the controller is subject.

- The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

- 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
  - (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
  - (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
  - (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
  - (d) the possible consequences of the intended further processing for data subjects;
  - (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

3.2 Privacy Protection related to FrailSafe

This Ethics Blueprint aims to satisfactorily identify the central ethical considerations, as well as indicating the measures required to prevent unnecessary exposure to risk for the participants and researchers in the FrailSafe project. Contributors to specific Tasks of the FrailSafe project should take specific responsibility for the periodic review of any relevant implications or issues that arise, and also the responsibility for necessary dissemination of this information to appropriate authorities, organisations, and/or bodies.

FrailSafe will involve “sensitive personal data” and in particular about participants physical and mental health condition. Hence, participants must give informed consent and data must be handled with appropriate arrangements (see below). These “sensitive personal data” will be handled only by the local clinical research personnel

bound by local confidentiality rules. These data will not be transferred, merged or exchanged. All other collected or recorded data will be anonymised with no personal identifiers and no means to link these to personal identifiers – hence falls outside the scope of legislation concerning personal data. Anonymised data stored in the cloud will also be encrypted.

Handling of "sensitive personal data"

1. Data collected during the clinical assessment by members of the research team will be anonymised by the same research staff and will contain no identifying information. These data will then be passed to other members of the FrailSafe consortium to be used freely, without requiring consent from the participant or any additional regulatory approval.

2. Data collected during previous approved research projects, which has been anonymised, may be passed to members of the FrailSafe consortium to be used freely, without requiring consent from the participant or any additional regulatory approval.

3. Data to be collected require Research Ethics Committee approval.

Note that in (1) and (2) the key issues are that the data are anonymised and that the researchers cannot link the data back to any personal identifiers; and that no additional research-specific procedures are needed as part of the FrailSafe project.

Compliance is required with "national legislation, European Union legislation, [respect for] international conventions and declarations and [researchers must] take into account the Opinions of the European Group on Ethics". Within this Blueprint all relevant documents will be considered, as well as a broader assessment of appropriate ethical issues. The 'whole FrailSafe network' will cover all involved countries and, therefore, all countries will be held to the standard of whichever member state has the most stringent requirements.

The authors cannot be certain that identical permissions would be granted in other jurisdictions, especially outside the EU, but note that the principles here should be applicable in all EU member states. The FrailSafe data are not planned to be used outside EU, but in case of uncertainty arises, advice should be sought from local Research Ethics Committees and Data Protection Authorities.

During the duration of the FrailSafe project, data, as specified by the protocol, gathered in one country will be shared with researchers in other member states. Therefore, in order to appropriately respect the rights of the volunteers, all participating researchers must comply with the most stringent Data Protection legislation of all involved countries, effectively holding those involved with the project to the highest standard, whilst ensuring that data collected in one member state is not then treated with less care when transferred to a second or third member state.

Informed consent will be required from all research participants, and the consent given must be voluntary and "based on knowledge of the purpose, procedures and outcomes of the research". In order to satisfy the knowledge requirements of a satisfactory consent, all those considering participating in the study will have a private discussion with an appropriate member of the research team, an information sheet will be given that they can read and reflect upon, have the freedom to ask questions about the project (both prior to agreeing to participate and throughout their participation, as needed), as well as knowing that they are free to leave the project whenever they wish without the need to give an explanation and without this action having a detrimental effect on the standard of medical care that they receive. Furthermore, each participant will be aware of their freedom to access their own data gathered, as well as the power to have this information permanently deleted should they so wish. During the time that a participant is involved in the research, they will be informed of any and all changes in the method, application, funding, etc. of the study to a sufficient level in order to ensure

a fully informed and valid consent. All information conveyed to those involved (those considering participation, those participating, and those that leave the study) will be communicated in the clearest way possible, and every effort will be made to ensure that all information has been adequately understood; this will avoid uninformed consent being given due to excessively technical language being used, or other such complications. The autonomy of the participant will be respected throughout the entire process of the study.

Personal privacy of participants should be respected, especially as ICT in the context of healthcare is "likely to raise privacy issues". For this reason, the reporting of research outcomes must be conducted in a manner which protects participant privacy and complies with all relevant data protection requirements. All data gathered should, therefore, be anonymised wherever possible and, furthermore, access to any sensitive personal data should be restricted. Access to such data will be granted to those that have a legitimate need to process the information in a way relevant to the FrailSafe project and certain safeguards will be in place including (but not limited to): responsibility for the appropriate use of and access to the data being assigned to a specific individual in each 'research team'; an access log being maintained where appropriate; a proper level of security and encryption being used for the storage and sharing of sensitive information (both data in-transmission and at-rest); an end-date being agreed upon and responsibility assigned to a person or organisation for the complete deletion of all sensitive data when that time is reached.

It is also required that "researchers must carefully evaluate and report the personal privacy implications of the intended use or potential use of the research outcomes". Wherever possible, they must ensure that research outcomes do not contravene these "fundamental rights" (to privacy and data protection). Therefore, all researchers will be made aware of this requirement and, again, responsibility will be assigned to specific individuals for the timely assessment and response to such concerns.

When prospective participants are being given information about the research as part of the consent procedure they will be fully informed about all the ways in which information will be gathered, exchanged and shared. In this way 'prior knowledge' will be ensured. Furthermore, to ensure that participants are free to leave the study whenever they wish (and from this moment prevent any further information being gathered), any computing device, wearable or not, will be produced with an 'off' function that is easily usable by the participant. The devices will also be designed with the possibility of pausing information gathering if the participant so wishes, in order to protect privacy at certain times but allowing the participant to remain in the study. With discrimination against the participant in mind, in case of the device being worn outside of a 'safe/private' environment (such as the home or research laboratory) the design of the device will be as discreet as its proper functioning will allow.

FrailSafe involves the use of electronic sensors, which may have specific implications for the protection of privacy and personal data. A detailed elaboration will be carried out following all the above mentioned legislation and restrictions.

The dignity of each participant will be respected, particularly by properly following consent procedures, by appreciating the voluntary nature of their participation, and by ensuring the security of any personal data gathered.

The wearable and portable devices will be designed with a respect for the integrity of the participant in mind. No unauthorised information will be gathered, nor will the device interfere with normal functioning in any way without consent. The device will pose no serious risk to short or long-term health. Procedures will be in place to identify any possibility of misuses or abuses of data as soon as they arise, and safeguards will be applied to prevent this occurring.

There will be a well-developed data management process in place to ensure the security of data. The FrailSafe Ethics committee that has been already appointed will be charged with protecting the rights and safety of participants by guaranteeing that FrailSafe researchers will strictly adhere to this ethics blueprint and management protocol. The data management plan will be addressed in details in D8.6. Similarly, the technical approach to support the security and privacy subsystem will be presented in detail in D.6.2

There shall be no interference by a public authority with the exercise of the right to respect for private and family life, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

3.3 Data Quality

From the General Provisions section of the Directive, Article 6 (principles relating to data quality):

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Therefore, all data must be relevant, accurate, anonymised when possible, and used only for the specified purposes. A controller must be appointed and will be the one to ensure that the directive is adhered to. According to Article 2(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; […] [1]

2. Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as

- the recipients or categories of recipients of the data

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply

- the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific

circumstances in which the data are collected, to guarantee fair processing in respect of the data subject. These requirements will be met as part of the consent procedure.

3.4 Data Security and Legal Framework

Data should be secure from viruses, hacker attacks, forgery etc. Security means protection of information and information systems by ensuring confidentiality, availability, integrity, authentication, and non-repudiation. [2]

Confidentiality: Information is not made available or disclosed to unauthorized individuals and entities.

- Availability: Data/information have to be available, only authorized persons can remove it, in accordance to law
- Integrity: only authorized persons can modify the data/information, in accordance to law
- Authentication must be preserved (data/information must be authentic)
- Non-repudiation – participants will not be able to successfully challenge the authorship of the data provided

Directive 95/46/EC (Data Protection Directive)

The following requirements will be met [1]:

(1) Applicants need to identify the appropriate/competent data protection authority that will provide the relevant authorisations;

Responsibility must be assigned (country specific) for the identification of the relevant authority and the request from that authority for any necessary authorisations. Depending on the legal environment, applicants need to provide the appropriate authority with a detailed description of the proposed data collection (and their usage) and the methodology that will be employed for collecting, using and storing of personal data.

(2) Improper use and data protection: as previously noted, researchers must be conscious of the possible misuse or dual use of any information gathered. If such a possibility is considered to exist, appropriate safeguards will be put in place. Researchers will need to consider the following questions:

- Can the data obtained within the project have another, reasonably foreseeable, usage?
- If this is the case, which safeguard measures will be put in place so as to protect and control data flow?
- Have the necessary authorizations for data circulation obtained? Who shall be contacted to assess this need?

These questions will be answered (with a prepared answer accessible when required by the relevant authorities) by an appropriate representative of the FrailSafe project.

Directive 95/46/EC: On the protection of individuals with regard to the processing of personal data and on the free movement of such data

This is a very extensive document, covering the uses of data in a variety of contexts. Below are those clauses or aspects which are most relevant to FrailSafe project, and which need to be incorporated or kept in mind. They have been included in full in order

to ensure that they are fully adhered to in the case that an aspect of FrailSafe changes (so that a specific interpretation does not become redundant).

(1) It is required that the processing of data in a particular EU member state be governed by the law of that state:

- Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State.

For this reason, under the list of recommendations is the requirement that all those involved with data processing in any way are familiar with the data protection legislation of the involved member states. It must also be considered that of those involved with FrailSafe, the majority are experienced in dealing with this sort of data in the appropriate way and that, furthermore, Directive 95/46/EC is intended to standardise data protection legislation across the EU, and now surpassed by the newly approved Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data [7]

In order to ensure that participants' rights are protected at all times, there will be one standard that will cover the processing of data in all involved member states. Procedures will be in place to ensure this (including consent, data protection):

- Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

These procedures will ensure a uniformity in the treatment of the data, meaning that in practice there will be no difference in the way the data is handled between the place it is gathered and the place it is processed (when distinct).

(2) It is acknowledged that those processing the data have certain responsibilities which must be upheld, but that the subject of the data also must have the possibility of reviewing the data, altering it (where appropriate) and withdrawing from the study:

- Whereas the principles of protection must be reflected, on one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

The participants of the study will be informed of these rights during the consent procedure, and they will also be listed on the information sheet that will be available to keep. Data which contain information sufficient to identify a person must be covered by a principle of protection; this principle will not apply to that data that has been sufficiently anonymised:

Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable,

account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

(3) Use of the data gathered - that it must be demonstrably relevant to the project, that the planned use of the data must have been consented to by the participant, and that there shall not be a secondary, unrelated use of the data (without prior consent):

- Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

This requirement is especially relevant when making finally decisions about the type and extent of data that will be gathered: all data that is gathered must be demonstrably relevant to the study itself, not gathered without reason or because a lack of focus when gathering data is in any way easier.

All countries involved in the gathering, transfer, or processing of data must ensure that they meet the requirements of all member states (and, particularly, of this Directive):

- Whereas, […] the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

Data is not to be shared with a third country (specifically, an non-EU member state) without first meeting the requirements of this directive.

Directive 2002/58/EC (e-Privacy Directive): Article 4. Security [2]

1.The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Council Framework Decision (2005/222/JHA) [13] addresses the most significant forms of criminal activity against information systems, such as hacking, viruses and denial of service attacks. The Framework Decision seeks to approximate criminal law across the EU to ensure that Europe's law enforcement and judicial authorities can take action against this form of crime. At the moment, there is a proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA.

Regulation EU 2016/679 (On General Data Protection Regulation) [7]

The Regulation says about this point:

"Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association. ".

3.5 National Frameworks

This section describes national frameworks of the four countries involved with handling of data within the FrailSafe project.

3.5.1 *Greece*

Greek legislation regarding public participation, electronic communication, personal data protection and ethics:

- Greek Law 3242/2004 and Greek Law 3448/2006. Self-imposed search of documents by the public authorities, use of information of the public sector: Direct communication among competent Authorities for issuing certain types of documents which might be needed for environmental authorization and environmental control should be requested by the Environmental Authority through direct communication with other competent Authorities.
- Greek Law 2472/1997 concerning the protection of personal data. (Governmental Gazette Vol. A/50/10.04.1997). "Protection of the individual against processing of personal data")
- The 2003 Ministerial Decision ΔΥΓ/89292, which harmonised national legislation with the EU Directive 2001/20
- The Council's of Europe Convention on Human Rights and Biomedicine, known as the Oviedo Convention, that Greece has incorporated to national legislation by law 2619/1998

3.5.2 *France*

- Directive 95/46/EC is incorporated into French Law Nr. 2004-801 of 6 August 2004 relating to the Protection of Data Subjects as Regards the Processing of Personal Data. Data protection is overseen by the Commission Nationale de l'Informatique et des Libertés (CNIL)

All work involving the use of human biological samples will be performed following the Bioethics law. All clinical trials or work involving human beings will follow the French Code of Public Health (1st part book II bis) on “The protection of persons in biomedical research” (www.legifrance.gouv.fr).

3.5.3 *Cyprus*

Research must comply with the Principles of the Processing of Personal Data (Protection of Individual Law 2001 (138(1)/2001.) The Act contains eight governing Principles relating to the collection, use and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves.

Data acquisition and evaluation in Cyprus are both subjected to scrutiny by the Cyprus National BioEthics Committee (CNBEC). MATERIA will inform CNBEC about the data that will be collected and will formally ask for advice about ethical issues. In the case of FrailSafe a formal application to the CNBEC will be made for the collection and analysis of the data. The laws governing ethical issues are also conveniently kept at the CNBEC web page (http://www.bioethics.gov.cy /Law/cnbc/cnbc.nsf/All/C68D8A0952500F56C22571C9002A6917?OpenDocument) . Special care will be given to law 37(I) of 2003 that was voted as an amendment to earlier laws, specifically for aligning Cyprus legal regiment to the provisions of Directive 95/46/EC of the EU. T

3.5.4 *Italy*

In Italy protection of personal data is guaranteed by the Italian Legislative Decree 30 June 2003, 196, in compliance with the EU Law. The Law n. 547, 23th December 1993, defines the Criminal Code and the Criminal Procedure Code on the subject of computer crime.

The Law n.150, 7th June 2000, addresses the issue of transparency, acknowledging the right of access of citizens to administrative institutions and to administrative proceedings, including the use of consultation and active participation action. A specific law (Legge Stanca, Art. 4, 9 January 2004) has been defined to face the issue of accessibility, intended as the “ability of computer systems, in the manner and to the extent permitted by technological knowledge, to provide services and usable information, without discrimination, even for those who, because of personal disabilities, require assistive technology or special configurations". The Italian Legislative Decree 7 March 2005, n. 82, the so called “Public Administration Digital Code” (http://www.digitpa.gov.it/cad), addresses a set of ethical issues such as:

- Privacy of data transmitted electronically (“Persons working with electronic transmission of documents, data and documents drawn up by computer cannot take cognizance of electronic correspondence, duplicate by any means or transfer to any third parties information about the existence of correspondence, communications or messages transmitted over the Internet and the related content and any part/extract of it, except in the case of information by their nature or by express indication of the sender intended to be made public”)

4 Legal & Ethical Framework for Involvement of Human Subjects

ICT research may cause harm related to: systems assurance (confidentiality, availability, integrity); individual and organizational privacy; reputation, emotional well-being, or financial sensitivities; and infringement of legal rights (derived from constitution, contract, regulation, or common law) [14]

Therefore, two main ethical questions should be asked about participants involved in the FrailSafe project:

- Will they be exposed to any harm?
- Will they represent all social groups that will use the service?

The FrailSafe protocol foresees that in the evaluation period feedback from the participants will be collected, processed and analyzed to establish user satisfaction and acceptance, as well as ease of use.

The FrailSafe partners should, as it is also mentioned previously:

- inform participants on the research protocol, risks they could face (if any), and research and society benefits
- obtain consent from participants
- inform participants that they can withdraw from research at any time without suffering negative consequences
- ensure anonymous participation
- ensure not to harm
- provide necessary help and support to participants

5 Cloud Computing on Privacy Issues

The European Digital Agenda [14] promotes the development of an EU-wide strategy on cloud computing, however, the current legislation, both at European and at National level, did not explicitly address the cloud/software as a service environment, before the Regulation EU 2016/679 [7].

'Cloud computing' is the storing, processing and use of data on remotely located computers accessed over the internet. Services such as web-based e-mail or social networks are often based on cloud technology. For professional IT users and public authorities cloud computing can mean a high degree of flexibility as to the amount of computing power needed. It also saves on money, office space and in-house IT support staff. The take-up of cloud computing in local and regional authorities has so far been slowed down by concerns about a lack of privacy, data security, lack of standardization, and jurisdictional issues relating to applicable law and law enforcement access to data.

Private or commercially sensitive data may be stored in a Cloud computing environment, accessed and processed in remote locations, including different countries. Thus, data protection and identity management become increasingly important to assure continued trust in and uptake of these services.

This previous lack of a common and clear regulation, in terms of cloud-computing had lead to some uncertainty in the design of Cloud solutions. The requirements to be taken into consideration are those proposed by the new Regulation EU 2016/679 [7] and to those related to the management of data [13-14]. Data is subject to specific legislative requirements that may depend on the location where they are hosted or on the purposes for which they are processed. In the cloud case, there was a lack of clarity on applicable law, due to the cross-border situations where the data subject, the data, the controller, the processor and the processing may be located in different countries (Articles 25 and 26 of Directive 95/46/EC) [1]. Now according the new Regulation clearly states "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (Article 3, Regulation EU 2016/679).

Privacy protection is one of the main concerns to be taken into account in the design of services to be deployed on the Cloud, as trust in Cloud computing is a key prerequisite. Different countries have different laws regarding which kind of data may be hosted in a cloud, where and how it is to be protected and may be accessed or made public. Within the cloud, technically data may be hosted anywhere within the distributed infrastructure, i.e. potentially anywhere in the world. The Regulation EU 2016/679 principles and, where needed, the national legal frameworks will guide platforms to be developed on cloud.

Sensitive personal data from FrailSafe project participants will not be stored in the cloud; the handling and protection of these data has been extensively analyzed previously. Anonymised and encrypted data, however, will be transferred or streamed via net.

Two specific actions are waited from the European Commission

1) The EC should ensure the review of the Data Protection Directive delivers a result that facilitates Cloud computing in Europe and at a global level and consider the impact of the national implementations of the Data Protection and ePrivacy Directives on the Cloud.

2) The EC should work with other jurisdictions/regions to develop interoperable requirements that facilitate information flows with appropriate security and privacy protection, including the opportunity to build upon recognised existing global initiatives.

Meanwhile the following recommendations are placed:

- FrailSafe will define the responsibilities of the cloud provider in accordance with the current legislation on management of data protection
- The specification of security measures that the cloud provider complies will be examined depending on the risks represented by the processing and the nature of the data to be protected
- Specification of the conditions for returning data or destroying the data once the FrailSafe project is concluded. Furthermore, it must be ensured that personal data are erased securely at the request of the cloud client
- Only authorized persons can have access to data
- Obligation on the provider's part to support the client in facilitating exercise of data subjects' rights to access, correct or delete their data
- It should be expressly establish that the cloud provider may not communicate the data to third parties
- Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data
- It should be contractually fixed that the cloud provider must inform the client about relevant changes concerning the respective cloud service, such as the implementation of additional functions
- Notification of cloud client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited
- A general obligation on the provider's part to give assurance that its internal organization and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards

6 FrailSafe Ethics Guidelines

Data privacy is the right of any individual to expect that his/her personal information directly or indirectly collected are processed securely and are not disseminated without their written consent. Information collected with permission for one purpose should not be used without permission for other reasons. Data protection is the framework of

security measures designed to guarantee that data are handled in such a manner as to ensure that they are safe from unintended, unwanted or malevolent use. Data protection is the technical mechanism to ensure data privacy.

Horizon 2020 for ethical & legal issues has provided guideline for self-assessment of proposals [17], as ethics issues arise in many areas of research. Research and innovation projects often involve the voluntary participation of subjects and collection of data that might be considered as personal.

FrailSafe, as it has been mentioned previously, collects personal data, including demographics, social status, living conditions, current and past medical history, current medical treatment, clinical assessment regarding frailty, capture of physiological measurements (ie. weight, height, bioimpedance, grip strength, arterial rigidity), continuous physiological measurements (i.e. heart rate, respiratory rate, body movement, etc), which will be analyzed off-line initially, and later online streamed and analysed, detection of in-door movement via beacons, detection of out-door movement via GPS. Data from gaming will also be recorded and WEB transmitted; typed text, as well as written text, will be obtained, digitalized, and then analyzed. An aspect to be considered is the deployment of cloud computing. Transmitted data will be anonymised and encrypted, however, a number of data protection risks may exist; mainly a reduced control over how, where and by whom the data is being processed/sub-processed.

A crucial aspect to be considered in this context is the wide scale deployment of cloud computing services, which can trigger a number of data protection risks, mainly a reduced control over personal data, as well as insufficient information with regard to how, where and by whom the data is being processed or sub-processed. These risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider.

The lawfulness of the processing of personal data in the cloud depends on the adherence to basic principles of the EU data protection law, on the basis of which it's possible to define the following recommendations:

Recommendations for FrailSafe:

- **Minimization**: anonymise data.
- **Transparency**: FrailSafe participants will be informed about which data will be stored, who these data will be transmitted to and for which purpose, and about the cloud provider.
- **Consent**: The consent text will explain the purpose of the project, the type and frequency of clinical assessments, the nature of data recording, storing and the way of transmission, including the entities involved in the analysis of data. Obviously, no consent indicates no participation. The consent legal text must be customized for each pilot country with references to the local legislation that applies.
- **Defaults**: By default data is not automatically shared. Data sharing and diffusion applies just to data for which consent has been given, and in accordance with the diffusion terms expressed by the consent.
- **Purpose specification and limitation:** personal data must be collected just for the specified purposes of the participation process and not further processed in a way incompatible with those purposes. It must be ensured that personal data are not (illegally) processed for further purposes.
- **Erasure of data:** personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Data should also be erased when informed consent is withdrawn.

- **Accountability:** it shall be possible to establish what an entity did at a certain point in time in the past and how.
- **Cookies:** The system shall not store cookies on the users' computers to prevent any unauthorized tracking of the users' activities on the Internet.
- **Security:** Appropriate protocols should be used to ensure security of data

6.1 Protection of Personal Data

Data collected during the clinical assessment by members of the research team will be anonymised by the same research staff and will contain no identifying information. Name, addresses, telephone numbers, email, and signed consent forms will be stored and secured locally within the clinical partner's medical institutions following procedures that are dictated by national legislation, and local guidelines and procedures. It should be noted that medical institutions have in place their own data privacy and security policies which should be compliant with National and EU regulations. The anonymised data will then be passed to other members of the FrailSafe consortium to be used freely, without requiring further consent from the participant or any additional regulatory approval. Therefore, the consortium guarantees that all personal data collected during the project will be kept secure and unreachable by unauthorized persons. The data will be handled with appropriate confidentiality and technical security, as required by law in the individual countries and EU laws and recommendations.

All activities will be carried out ensuring the ethical principles in accordance with Regulation EU 2016/679 and with Directive 95/46/EC of the European Parliament, about the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as DIRECTIVE 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, as modified by Directive 2009/136/EC. All national data protection and privacy laws for pilot countries will be also followed.

6.2 FrailSafe Technical Approach

The technical approach that we will follow in FrailSafe will consider the recommendations drafted in this document which will evolve throughout the project's duration. The technical approach to support the security and privacy subsystem will be presented in detail in D.6.2. Similarly, the data management plan will be addressed in detail in D8.6. The platform will provide authorization, authentication and user access control mechanisms to assure authorized access to the platform's data. It will also provide additional security mechanisms for protecting data and eliminating risks; it will support secure protocols and encryption mechanisms, where needed, to allow secure transmission of sensitive information. The FrailSafe platform will be hosted on a secure infrastructure and will be designed considering the cloud computing recommendations and technical requirements in deliverable D1.3 FrailSafe technical specifications and end-to-end architecture.

6.3 Ethics Approval

Copies of ethical approvals for the collection of personal data or the respective notifications (depending on the type of personal data that will be collected and according to the national data protection legislation of each country) by National Data Protection authorities or Ethics Committee will be submitted to the Research Executive Agency (REA).

6.4 Biological samples for research

Blood specimen will be collected according the local medical institution procedures, only after consent has been obtained. A protocol will address issues including the intended use of the collected samples, the length of time the samples will be stored, sample coding procedures, management and limits of access of the data collected, maintenance of subject privacy and confidentiality, sample storage locations and storage conditions, sample destruction, publication and dissemination of results. Country-related and global regulatory efforts are currently ongoing to harmonize the regulations governing sample banking for future clinical research. The International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) published guidance documents addressing efficacy, joint safety/efficacy (multidisciplinary), quality and safety. These guidance documents are the ICH's attempt to harmonize standards between Europe, Japan and the USA [18]. The EU provides the requirements of conduct of clinical trials in the " Directive 2001/20/EC", which was concretised further by " Commission Directive 2005/28/EC". [19] Genetic information will not be recorded, not even as family history of disease and also genetic samples of any kind will not be collected.

6.5 Protection of geolocation data (GPS and Bluetooth beacons)

The European Data Protection Working Party has adopted "Opinion 13/2011 on Geolocation services on smart mobile devices" [20], which addresses the protection of data exposing the location of users, collected with technologies such as GPS and WiFi. This opinion regards the protection of geolocation data, focusing mainly on data obtained from GPS and WiFi technologies. However, it states that the regulations also apply on smaller area technologies, such as Bluetooth and RFID. It is thus related to the geolocation functionalities included in FrailSafe, namely the outdoor and indoor localization services, which will use GPS and Bluetooth technologies, respectively.

Geolocation data can be combined with unique IDs obtained from the mobile devices of the users, achieving indirect identify ability. Geolocation data are thus considered personal data. The regulation identifies three functional entities involved in geolocation data usage:

- The controller of the geolocation infrastructure
- The provider of the specific geolocation application or service
- The developer of the operating system of a smart mobile device

Each of these entities processes personal data when they are directly or indirectly use geolocation data of the users, thus they are under the obligations of the data protection directive [1]. Within the context of FrailSafe, the regulations related to the providers of geolocation applications apply.

Collectively, regarding the providers of geolocation applications to be installed in the smart mobile devices of the users, the regulation states the following:

An application that wants to use geolocation data clearly informs the user about the purposes for which it wants to use the data, and asks for unambiguous consent for each of the possibly different purposes. The user actively chooses the level of granularity of geolocation (for example, on country level, city level, zip code level or as accurately as possible). Once the location service is activated, an icon is permanently visible on every screen that location services are 'ON'. The user can continuously

withdraw his consent, without having to exit the application. The user is also able to easily and permanently delete any location data stored on the device.

The users of the smartphones must be adequately informed about the purposes of the data processing, the type of data, the duration of the processing, their rights to access, rectify or cancel their data and their right to withdraw consent. This information must be aimed at a broad audience, not assuming that the users are technically skilled persons, especially in the context of FrailSafe, which targets older people. The users must also be kept informed for as long as the providers of geolocation applications process their location data.

The users have the right to access the collected data in a human-readable format. They also have the right to access possible profiles based on these location data. It must be ensured that geolocation data are deleted after they are no longer needed for the purposes for which they were collected, while collected user IDs must be anonymized after 24 hours from their storage.

6.6 Web and social media mining, monitoring and classification tools

Participants data monitoring, mining and classification tools

The tools that will be developed in order to monitor, collect and classify the participants' data will process public and personal data, abiding to all relevant rules and recommendations of the national legislation and the respective EU recommendations and directives. [2]

Participants clinical reports, questionnaires, social media posts & profiles and other sources of data will be collected and preprocessed in order for the dataset to be created.

The collected data will be transferred from Tasks 4.3, 4.4 and 6.1 using encryption technology in various forms of communication services. Furthermore, to ensure that no participant can be correlated to its medical data, the dataset will pass through an anonymization process where the actual participants' names will be removed and the dataset instances will be referenced as numeric IDs. All data will be stored locally, along with the server, which will be placed in a secure room. None third party will be able to alter information as access to information that is collected will be restricted only to the related tasks. For the deliverable of Tasks 4.5 and 6.1, all processing steps will be utilized. All steps will be thoroughly executed in order to avoid crossreference of older people data. The output of classification software related to the participant's mental state will be distributed to all other related tasks using state of the art Secure Socket Layer (SSL) API thus securing the flow of information.

Social media mining and monitoring tools

The social media mining and monitoring tools to be deployed in the project will collect and/or process publicly available personal data, abiding to all relevant rules and recommendations of the national legislation and the respective EU recommendations and directives. For data collection, the official APIs that are made publicly available from the respective online sources will be used, and always in full compliance with their terms of service. Social media posts and basic profile information from the users social media account is collected based on keywords and data from social media are processed and aggregated to create data summaries. Furthermore, some individual items are shown to the user interface of the visualization component. All data collected from social media (and concretely for T4.4) will be stored in a NoSQL database installation in the FrailSafe servers. No cross-referencing takes place in the social

media mining component. The data is stored in the form they are collected from the respective APIs. No further accuracy assurance is performed. Subjects will not be able to alter information, as this is already published information that is collected from third party services. The collected social media data may be disclosed to researchers working only on the project and to pilot partners testing the system based on the guidelines and consortium agreement.

In a more general context, anonymization is a primary research topic as well as a main concern in social media analysis whose importance cannot be overstated. The main motivation behind several studies [21-22] is that simple anonymization techniques such as random IDs instead of account names are not sufficient since users can be still identified from the social network graph structure using tools such as egonet analysis or spectral vertex ranking. Hence, more efficient techniques should be deployed like those proposed in [23-24]. These rely on inserting controlled structural noise in the social graph, leading thus to higher anonymization levels at the expense of reduced quality of analysis results. An alternative lies in the direction of protection measures based on Privacy Enhancing Technologies (PETs) and Attribute-based Authentication methods (ABCs).

Additionally, front- and back-end databases should integrate suitable access control systems, safeguarding both data and metadata. The latter is important, as certain data properties can be deduced from careful metadata analysis. Thus, by integrating a metadata protection layer, unauthorized disclosure risk is minimized.

6.7 Right to be forgotten

All participants have the right to obtain the erasure of personal data relating to them and the abstention from further dissemination of such data according to the General Data Protection Regulation [8]. They will be informed about this right in the information sheets. Applications for erasure of data will be carried out without delay. In case the personal data has been made public, the consortium will take all reasonable steps, including technical measures, to inform third parties that are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. A procedure for exercising the right to be forgotten and to erasure will be provided, and will include appointment of a data protection manager, checking the validity of the request, identifying data which should be erased, monitoring the erasure process, and informing the pilot user.

7 Conclusion

This deliverable aims to identify key issues regarding ethics, legislation and data protection and security that apply to FrailSafe framework both at EU and National level. This ethics blueprint will govern all activities of the FrailSafe consortium throughout the duration of the project including all partners, but even more so those involved with handling of participants' data.

Initially, we provided a brief overview of the scope of FrailSafe project together with the nature of the observations, interventions and data collection. The European directives were then investigated regarding Data Protection Directive, biological samples for research, e-Privacy Directive, Cookie Directive, Cloud computing, as well as Protection of Geolocation data and Web and social media mining, monitoring and classification tools. Specific recommendations were then made considering the structure of FrailSafe including aspects of privacy & data protection; EU and National legislation were considered.

8 References

[1] Directive 95/46/EC on protection of personal data . http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri= CELEX:31995L0046:en:HTML

[2] Directive 2002/58/EC on privacy and electronic communications. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058: en:HTML

[3] Directive 2009/136/EC (Cookie Directive). http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ:L:2009:337:0011: 0036 :en:PDF

[4] European Human Rights Convention. http://www.echr.coe.int/Documents/ Convention_ENG.pdf

[5] UK Data Protection Act 1988. http://www.legislation.gov.uk/ukpga/ 1998/29/contents

[6] ICT FP7 Ethical Guidelines. ftp://ftp.cordis.europa.eu/pub/fp7/docs/guidelines-annex5ict.pdf

[7] Directive (EU) 2016/680. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri= uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[8] Reform of EU data protection rules. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[10] Charter of Fundamental Rights of the European Union (2000/C 364/01, http://www.europarl.europa.eu/charter/pdf/text_en.pdf)

[11] Digital Agenda for Europe COM(2010)245. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0245&from=en

[12] UN Convention on the Rights of persons with disabilities. http://www.un.org/ disabilities/convention/conventionfull.shtml

[13] Council Framework Decision 2005/222/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222&from=EN

[14] The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, D. Dittrich and E. Kenneally, eds., US Dept. Homeland Security, 2011; www.cyber.st.dhs.gov/wp-content/uploads/ 2011/12MenloPrinciples CORE-20110915-r560.pdf .

[16] Cloud computing: How to protect your data without falling from a cloud, Italian Guarantor for the Protection of Personal Data, http://www.garanteprivacy.it/ documents/10160/2052659/1912744, 24-05-2012

[17] Horizon 2020 How to complete your ethics Self-Assessment, 2014

[18] The International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH). http://www.fda.gov/ RegulatoryInformation/Guidances/UCM122049

[19] Commission Directive 2005/28/EC. http://ec.europa.eu/health/human-use/ clinical-trials/ directive/ index_en. htm)

[20] ARTICLE 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[21] L. Backstrom, C. D. (2007). Wherefore art thou r3579x? anonymized social networks, hidden patterns, and structural steganography. In Proceedings of the 16th international conference on World Wide Web, WWW, pp. 181–190

[22] Shmatikov, A. N. (2009). De-anonymizing Social Networks. In Proceedings of the 2009 30th IEEE Symposium on Security and Privacy (SP), pp. 469–478

[23] Terzi, K. L. (2008). Towards identity anonymization on graphs. In Proceedings of the ACM SIGMOD International Conference on Management of Data, pp. 93–106.

[24] M. Hay, G. M. (2007). Anonymizing Social Networks. Technical report, UMass Amherst

9 Appendix

9.1 Data protection check list

The following protection check list is produced to aid identification of the privacy issues that may arise during operational implementation and execution of FrailSafe project.

- Who will collect information?
- Has ethical approval been obtained?
- Has an independent "controller" been nominated?
- Is there a data management plan in place?
- Has informed consent been obtained?
- Are data anonymised?
- Are cloud data encrypted?
- How is each type of data being used?
- Where each type of data is stored?
- Have uses of data defined?
- Are specific individuals accountable for mishandling personal sensitive data?
- How long data are retained, and are there procedures to erase data at a predefined date?
- Are there procedures to erase data of participants who withdraw consent?
- Is accuracy of collected data assured?
- Are mechanisms in place to update inaccurate data?
- Are there data collected without participant's consent?
- Has the participant full prior knowledge of the place and timing of face to face and telephone assessments?
- Are policies in place to share and transfer data among research partners?
- Are policies in place to prevent data or information released to third parties, even within your own organization or establishment?
- Are there procedures to identify persons with the right to access data?
- Is password security assured?
- Is access to sensitive data revoked from employees who quit their position?
- Are management policies for obtaining, storing, and transferring biological samples defined?
- Is participant's comfort and un-intrusiveness guaranteed?
- Is short and long term participant's safety guaranteed?