



# ACTOVAGE PROJECT

ACTivating InnoVative IoT smart living environments for AGEing well

## Ethics and Privacy Protection Manual

<b>Deliverable No.</b>	D1.5	<b>Due Date</b>	30-Jun-2017
<b>Type</b>	Report	<b>Dissemination Level</b>	Public
<b>Version</b>	1.0	<b>Status</b>	Release 1
<b>Description</b>	Identify main ethical issues and how will address them during its lifetime.		
<b>Work Package</b>	WP1 – Project Coordination, IPR and Ethics Management		



## Authors

Name	Partner	e-mail
Eleni Chalkia	08 CERTH	<a href="mailto:hchalkia@certh.gr">hchalkia@certh.gr</a>
Mary Panou	08 CERTH	<a href="mailto:mpanou@certh.gr">mpanou@certh.gr</a>
Olga Gkaitatzi	08 CERTH	<a href="mailto:ogkait@certh.gr">ogkait@certh.gr</a>
Votis Konstantinos	08 CERTH	<a href="mailto:kvotis@iti.gr">kvotis@iti.gr</a>
Dimitrios Papageorgiou	08 CERTH	<a href="mailto:dimpapag@iti.gr">dimpapag@iti.gr</a>

## History

Date	Version	Change
24-March-2017	0.0	Ethics questionnaire sent to the Consortium
17-May-2017	0.1	Structure of the document and task assignments
28-May-2017	0.2	Structure finalized & section 1 finished
28-June 2017	0.3	Version ready for peer review
06-July 2017	0.4	Final version after peer review
12-July-2017	1.0	Official Release

## Key data

<b>Keywords</b>	Ethical issues, security, privacy, legal framework
<b>Lead Editor</b>	Eleni Chalkia, 08 CERTH
<b>Internal Reviewer(s)</b>	Alexandre Duclos, 16 Madopa Rauno Sarnio, 45 SEN

## Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

# Abstract

This document contains the Ethics and Privacy Protection Manual for the ACTIVAGE project. The Ethics and Privacy Protection Manual will guide the principles and the main procedures regarding privacy, data protection, legal issues and ethical challenges in ACTIVAGE project. This reference document includes the guiding principles and the main procedures regarding privacy, data protection, security, legal issues and anticipated ethical challenges foreseen in ACTIVAGE.

ACTIVAGE interoperability framework will address the specificities of oriented solution including the security of medical data and the safeguarding of the doctor-patient confidentiality. The project's Ethics and Privacy Protection Manual (D1.5) will form the basis of the project in this direction as it will summarize the fundamental requirements for data security, safety, privacy and confidentiality not only for the scheduled large scale trials and in regards to the legal environment of each deployment site but will also set the framework for the quality requirements of the services, applications and platforms integrated with AIoTES.

The Ethics and Privacy Protection Manual will be used throughout ACTIVAGE project as a document serving three primary purposes:

- to be a reference document for all activities that consideration for ethics should be taken;
- to provide the guiding principles and the main procedures regarding privacy, data protection, security, legal issues and ethical challenges will be included;
- to summarize the fundamental requirements for data security, safety, privacy and confidentiality not only for the scheduled large-scale trials as well as set the framework for the quality requirements of the services, applications and platforms integrated with AIoTES (ACTIVAGE IoT Ecosystem Suite).

The 1<sup>st</sup> Chapter of this document is an introduction on the current report. The role of ethics in the IoT and especially IoT in AHA (Active and Healthy Aging) is presented in **Chapter 2**. ACTIVAGE has delegated the task of ethical management to CERTH and project's Policy, Legal and Gender Board -PLGB that includes experts representing the diversity of views of all projects' stakeholders, as presented in **Chapter 3**. ACTIVAGE ethical policy (**Chapter 3**) addresses critical ethical issues, such as data protection, confidentiality, anonymization, sharing, transparency, and risk assessment. The strategy that will be followed at the Large Scale pilots by the DSs in relation to the communication with the participants is presented in **Chapter 3** that includes information about all the procedures that should be followed. Following, the legal aspects that should be taken into account in AVTIVAGE are presented in **Chapter 4**. Data privacy and protection issues are discussed in **Chapter 5**. **Chapter 6** presents the first initial idea of the risks related to the ethical issues thorough the project, as well as some initial mitigation strategies that could be followed. **Chapter 7** refers to the connection of the ethics guidelines of the current document with the ethical and safety layer of AIoTES and specifically the SecKit. Finally, Chapter 7 includes the conclusions of all the aforementioned chapters, as well as the planned future steps.

This deliverable, includes the project's ethical principles and process to be followed during all phases of user involvement and a preliminary list of ethical issues and instruments, to be taken into account in the Ethical review of ACTIVAGE. Detailed plans on each year's ethical activities throughout the project will be reported on D1.6.1: Ethical and legal report which will be available at the end of every reporting year.

# Table of contents

<b>TABLE OF CONTENTS</b> .....	<b>3</b>
<b>LIST OF TABLES</b> .....	<b>5</b>
<b>LIST OF FIGURES</b> .....	<b>6</b>
<b>1 ABOUT THIS DOCUMENT</b> .....	<b>7</b>
1.1 DELIVERABLE CONTEXT.....	7
<b>2 IOT AND INFORMATION ETHICS</b> .....	<b>8</b>
2.1 THE FUTURE OF IOT.....	8
2.2 THE FUTURE OF IOT IN AHA .....	10
2.3 INFORMATION ETHICS IN IOT.....	12
2.4 INFORMATION ETHICS IN IOT AND AHA.....	16
<b>3 ACTIVAGE ETHICS FRAMEWORK</b> .....	<b>18</b>
3.1 INTRODUCTION.....	18
3.2 POLICY, LEGAL AND GENDER BOARD -PLGB ORGANIZATION .....	20
3.3 ACTIVAGE DS ETHICAL STRATEGY .....	23
3.3.1 <i>ACTIVAGE DS description</i> .....	23
3.3.2 <i>ACTIVAGE DS ethics strategy</i> .....	23
3.3.3 <i>ACTIVAGE DS incentives schemes</i> .....	41
3.3.4 <i>Gender issues at DSs</i> .....	41
3.4 ACTIVAGE PARTICIPANTS .....	42
3.4.1 <i>Ethical concerns for the participants</i> .....	42
3.4.2 <i>Safety and well-being of participants</i> .....	43
3.4.3 <i>DS participants' recruitment process &amp; communication strategy</i> .....	44
3.4.4 <i>Informed consent</i> .....	45
3.4.5 <i>Guidelines for recruitment &amp; interviews with pilot users (with or without impairment)</i> 47	
3.4.6 <i>Incidental findings (IFs)</i> .....	49
3.5 DELEGATION OF CONTROL .....	50
<b>4 LEGAL ASPECTS IN ACTIVAGE</b> .....	<b>51</b>
4.1 INTERNATIONAL AND EUROPEAN INSTRUMENTS IN THE FIELD OF DATA PROTECTION .....	51
4.2 RELEVANT LEGISLATION, DIRECTIVES AND GUIDELINES .....	52
4.3 GDPR LEGISLATION.....	55
4.3.1 <i>GDPR Strengths and Challenges</i> .....	56
<b>5 ACTIVAGE DATA PRIVACY POLICY</b> .....	<b>58</b>
5.1 INTRODUCTION.....	58
5.2 CONFIDENTIALITY AND DATA PROTECTION .....	58
5.3 CODING ANONYMIZED DATA AND STORING.....	59
5.4 PRIVACY OF ACTIVAGE SYSTEM .....	60

<b>6</b>	<b>ETHICAL RISK ASSESSMENT AND MITIGATION STRATEGY IN ACTIVAGE.....</b>	<b>61</b>
6.1	RISK ASSESSMENT STRATEGY .....	61
6.2	ETHICAL RISKS IN ACTIVAGE .....	61
<b>7</b>	<b>ACTIVAGE ETHICAL DESIGN MODEL .....</b>	<b>65</b>
7.1	SECURITY AND IDENTITY MANAGEMENT .....	65
7.2	ETHICAL DESIGN AND SECKIT.....	66
7.2.1	<i>Introduction to SecKit.....</i>	66
7.2.2	<i>Main usages and implementations.....</i>	66
7.2.3	<i>Rule Model Specification.....</i>	69
7.2.4	<i>Potential for Integrating SecKit with ACTIVAGE.....</i>	71
<b>8</b>	<b>CONCLUSION/ FUTURE WORK .....</b>	<b>73</b>
	<b>REFERENCES .....</b>	<b>74</b>
	<b>APPENDIX A ACTIVAGE ETHICS CHECKLIST .....</b>	<b>77</b>
	<b>APPENDIX B ACTIVAGE CONSENT FORM (TEMPLATES).....</b>	<b>79</b>
B.1	INFORMED CONSENT FORM (BASED ON A CLINICAL STUDY TEMPLATE) .....	80
B.2	INFORMED CONSENT FORM.....	90
B.3	DOCUMENTATION OF CONSENT.....	95
B.4	INFORMED CONSENT DOCUMENTATION FOR AN ILLITERATE PARTICIPANT .....	97
B.5	INFORMED CONSENT CONCERNING PRIVATE INFORMATION.....	98
	<b>APPENDIX C OFFICIAL DEFINITIONS / PRINCIPLES APPLIED .....</b>	<b>99</b>
	<b>APPENDIX D TEMPLATE ON ETHICAL AND LEGAL ISSUES PER DS .....</b>	<b>104</b>

# List of tables

TABLE 1: DATA PRIVACY AND ETHICAL ISSUES AT FINNISH DS.....	28
TABLE 2: DATA PRIVACY AND ETHICAL ISSUES AT SPANISH DS .....	29
TABLE 3: DATA PRIVACY AND ETHICAL ISSUES AT FRENCH DS.....	31
TABLE 4: DATA PRIVACY AND ETHICAL ISSUES AT SPANISH (MADRID) DS.....	32
TABLE 5: DATA PRIVACY AND ETHICAL ISSUES AT ITALIAN DS .....	33
TABLE 6: DATA PRIVACY AND ETHICAL ISSUES AT UK DS .....	34
TABLE 7: DATA PRIVACY AND ETHICAL ISSUES AT SPANISH (VALENCIA) DS .....	36
TABLE 8: DATA PRIVACY AND ETHICAL ISSUES AT GERMAN DS .....	37
TABLE 9: DATA PRIVACY AND ETHICAL ISSUES AT GREEK DS.....	39
TABLE 10: LEGISLATION, DIRECTIVES AND GUIDELINES CONSIDERED BY THE ACTIVAGE PLG BOARD .....	52
TABLE 11 : CONSIDERATIONS REGARDING ACTIVAGE ETHICS RISK MANAGEMENT .....	61
TABLE 12: ACTIVAGE ETHICS CHECKLIST .....	77

# List of figures

FIGURE 1: THE IOT CONNECTED DEVICES PREDICTIONS (IHS MARKIT, 2016) .....	8
FIGURE 2: THE IOT MARKET PREDICTIONS (IHS MARKIT, 2016).....	9
FIGURE 3: SENSORS CONNECTED TO OBJECTS & TRANSFORMED INTO DATA-GENERATING “THINGS”. (ELECTROCHEMICAL SOCIETY, 2012).....	9
FIGURE 4: IOT MAIN COMPONENTS .....	10
FIGURE 5: ECONOMIC VALUE CREATION FROM IOT. (MCKINSEY, 2016).....	11
FIGURE 6: GLOBAL WEARABLES FORECAST 2016-2020. (CCS INSIGHT, 2015) .....	12
FIGURE 7: PLGB PLACE IN THE ORGANISATIONAL AND MANAGEMENT STRUCTURE OF THE ACTIVAGE PROJECT.....	20
FIGURE 8: SECKIT ARCHITECTURE DEPICTING ENFORCEMENT COMPONENTS.....	66
FIGURE 9: SECKIT GUI THAT CONTROLS RULE MODEL SPECIFICATION .....	69
FIGURE 10: CONTEXT-BASED RULE TEMPLATES .....	70
FIGURE 11: ACTIVAGE HIGH-LEVEL ARCHITECTURE .....	71

# 1 About This Document

This document contains the Ethics and Privacy Protection Manual for the ACTIVAGE project. The Ethics and Privacy Protection Manual will guide the principles and the main procedures regarding privacy, data protection, legal issues and ethical challenges in ACTIVAGE project. This reference document includes the guiding principles and the main procedures regarding privacy, data protection, security, legal issues and anticipated ethical challenges foreseen in ACTIVAGE.

## 1.1 Deliverable context

Project item	Relationship
<b>Objectives</b>	<p><u>Main objective</u> (... prolong &amp; support the independent living of older adults in their living environments ... enable the deployment and operation at large scale of Active &amp; Healthy Ageing IoT based solutions and services ...): The guidelines in D1.5 will increase the success chances not only in achieving the main objective but also in the sustainability of its impact.</p> <p><u>O4</u> (... co-creation framework ... assessing needs, preferences and perceptions regarding user acceptance, trust, confidentiality, privacy, data protection and safety ...): D1.5 influences the ACTIVAGE co-creation framework, esp. in the areas cited.</p>
<b>Exploitable results</b>	N/A
<b>Work plan</b>	This deliverable is the outcome of T1.4 on Ethical and privacy protection. It is the main reference for future work within this task and will guide many other project tasks, esp. T1.3 and the WP9 tasks.
<b>Milestones</b>	<u>MS1</u> ( <i>BUILD</i> ): D1.5 guidelines are prerequisites for the preparation of the deployment sites.
<b>Deliverables</b>	<p><u>D1.4</u> “<i>Data Management Plan</i>” will use the framework for data protection sketched in D1.5 as a basis for the data management plan of the project.</p> <p><u>D3.3</u> “<i>Security and privacy report</i>” will take into account the ethical principles of D1.5 and will implement them properly to the ACTIVAGE architecture.</p>
<b>Risks</b>	<p><u>Rk20</u> “<i>Harm to participants or violation of their fundamental rights</i>”: D1.5 helps to mitigate this risk by the Ethics Design Concept (Sekcit) as specified in Section 7.</p> <p>In addition, D1.5 identifies in Section 6 a set of specific risks related to the ethical issues of the ACTIVAGE project. The Risk &amp; Quality Manager of the project will enhance the project risk registry based on this list.</p>

## 2 IoT and information ethics

### 2.1 The future of IoT

According to Internet Live Stats, around 40% of the world population has an internet connection today, while in 1995, it was less than 1%. With elaboration of data by International Telecommunication Union (ITU), World Bank, and United Nations Population Division we conclude that the number of internet users has increased tenfold from 1999 to 2013. The first billion was reached in 2005, the second billion in 2010 and the third billion in 2014 (Internet Live Stats, 2016). According to EU study on ethics of information and communication technologies (EGE, 2012), more than 250 million Europeans connect to the Internet every day, to work, learn, communicate, play and socialise. Digital economy and also work and play have changed drastically and will change more during the upcoming years, as personal interactions continue to change from word of mouth and personal meetings to include interactions unlimited by place or time with the usage of internet. At the moment the Internet is a nearly 50 petabyte data repository. This repository is rapidly populated by massive numbers of entries that derive from individuals who either typed on a keyboard, pressed a button on a mouse or other device, took a picture, scanned a bar code, or otherwise performed a human interaction with a machine (Ebersold and Glass, 2016). Google CEO Eric Schmidt has pointed out that every two days we now create as much information as we did from the dawn of civilization up until 2003 (Schmidt, 2010). The internet, despite its enormous size, still lacks of the ability to connect back to the real-world in the direct way, as machine-to-machine (M2M) technology can. This M2M communication will be enabled with the spread of the IoT. With the IoT, the Internet will evolve into a more dynamic and integrated entity and it will be able to provide effective human-to-human (H2H), human-to-thing (H2T), and machine-to-machine (M2M) interactions (Ebersold and Glass, 2016).

IHS forecasts that the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025. (IHS Markit, 2016) That is being verified by the Business Insider, which quotes one of Morgan Stanley's predictions (Danova, 2013), that more than 75 billion of objects will be connected to the Internet of Things by 2020, 200 unique consumer devices or equipment that could be connected to the Internet that have not yet done so.

Additionally, McKinsey estimates the total IoT market size in 2015 was up to \$900M, growing to \$3.7B in 2020 having the potential economic impact of \$2.7 to \$6.2T trillion USD until 2025 (McKinsey, 2016), while Cisco predicts that the IoT will generate as much as 400 zettabytes (ZB) of data a year by 2018 (Cisco, 2014).



Figure 1: The IoT connected devices predictions (IHS Markit, 2016)

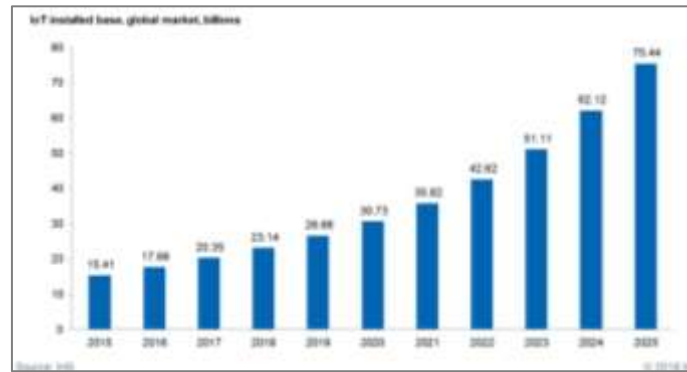


Figure 2: The IoT market predictions (IHS Markit, 2016)

The IoT can be broadly defined as a global network infrastructure, linking uniquely identified physical and digital objects, things and devices through the exploitation of data capture (sensing), communication and actuation capabilities (Wikipedia, 2016). A primary goal of interconnecting devices is to create situation awareness and enable applications, machines, and human users to better understand their surrounding environments. The understanding of a situation, or context, potentially enables services and applications to make intelligent decisions and to respond to the dynamics of their environments (Barnaghi et. al., 2005).



Figure 3: Sensors connected to objects & transformed into data-generating “things”.  
(Electrochemical Society, 2012)

The IoT is not a specific device or technology, but the term rather describes a system where items in the physical world and sensors within or attached to these items, are connected to the Internet via wireless and wired Internet connections. Thus, the basic concept of IoT is to bring as many things as possible into the digital era and create an ultimate sense of interconnection through hardware and software.

Looking at the literature, one can find numerous definitions for the IoT. Guillemin defines the IoT as: “The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service”. (Guillemin, 2009) While Haller et al., declares that the Internet of Things is “a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these ‘smart objects’ over the Internet,

query their state and any information associated with them, taking into account security and privacy issues.’ (Haller et al., 2009) Despite that dissimilarity, all the different definitions have in common that it is related to the integration of the physical world with the digital world of the Internet. (Haller, S. 2011) Nevertheless, many have defined IoT as a global network infrastructure, linking uniquely identified physical and digital objects, things and devices through the exploitation of data capture (sensing), communication and actuation capabilities (CASAGRAS, 2009. Internet of Things. Wikipedia, Miorandi et al. 2012, Dechesne et al. 2012). Emerging IoT services and applications will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability. (Dechesne et al. 2012)

Despite the fact that the IoT can be considered an evolution of the Internet, since it is breaking the boundaries between the Internet and the physical world, new categories of

electronic devices will be included in IoT, which did not exist in the conventional Internet where users access the web through a personal computer interface. These include small electronic devices and wearable sensors, remote healthcare systems which can monitor the health of an individual at any time, M2M systems which are used in an industrial context and intelligent home, smart cars connected with themselves and a fixed infrastructure to support intelligent traffic and safety applications. The list could continue with new devices and applications which are not even foreseeable at the present time. (Baldini et al. 2016) The main shared technologies behind the usage and communication of these devices are the continuous connectivity (wide range of wireless communications standards) and the capacity to collect data from the real world or to act on the real world (including from an individual or data that often can be related to each other through identification of time and (geo)location).



Figure 4: IoT main components

According to ETICA (ETICA final report, 2011) the emerging technologies that will be core of IoT are the following:

1. Affective computing
2. Ambient intelligence
3. Artificial intelligence
4. Bioelectronics
5. Cloud computing
6. Future internet
7. Human/ machine symbiosis
8. Neuroelectronics
9. Quantum computing
10. Robotics
11. Virtual/ Augmented Reality

## 2.2 The future of IoT in AHA

The evolution of IoT world has opened the door for technological applications that can monitor health and well-being outside of formal healthcare systems. The health-related Internet of Things, or in the case of ACTIVAGE the IoT related to Active Health and Aging (AHA) increasingly plays a key role in health management by providing real-time tele-monitoring of patients, testing of treatments, actuation of medical devices, and fitness and well-being monitoring. Given its numerous applications and proposed benefits, adoption by medical and social care institutions and consumers may be rapid. (empirica and WRC, 2010)

As we can see from the figure below, the IoT will unlock tremendous value across the Healthcare industry which based to McKinsey will reach more than 6,7 \$ trillions, in 2020. 1 trillion more than the next category which is automation and 4 trillion more than the next one, advanced electronics.

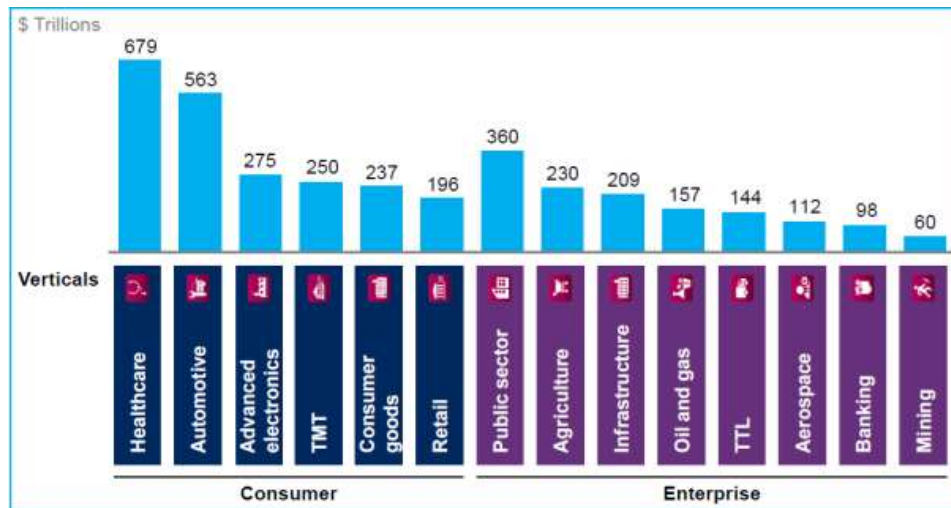


Figure 5: Economic value creation from IoT. (McKinsey, 2016)

Throughout Europe and all around the world, mortality rates have fallen significantly over the past decades (EU, 2014) leading to considerable changes in the age distribution of societies. This situation will be increased since people aged 60 are now expected to survive an additional 18.5 to 21.6 years and soon the world will have a higher number of older adults than children. (UN, 2013; Rechel et al, 2013) For EU governments, these users are seen as a problem since they are ageing in greater numbers; becoming sick and increasingly demanding, thus demanding advances in the health and social care services. Thus, these users, as well as their carers and care providers are also the most significant population groups targeted by the telecare and smart home industry are (Schmitt 2002; Harmo et al 2005). The EC believes that *“Europe’s over 65s are estimated to be worth over €300 billion and the smart homes market is expected to triple between 2005 and 2020. New markets such as tele-health could help older people to get out of hospital and back home more quickly, thereby improving the sense of well-being and reducing society’s health costs.”* (European Commission, 2010)

Internet of Things (IoT) is enabling consumer to live healthy life by monitoring their health in a highly personalized manner through connected devices such as wearable devices, tablets, and other hand-held devices. This trend seems to be fast accelerating, since according to a new report, 80 million fitness and sports-related wearable devices are expected to ship by 2020 and healthcare-focused wearables already account for 34 million shipments. Additionally, the global medical wearable devices market was worth more than 3.2 \$ billion in revenue in 2016 and is expected to cross 7.9 \$ billion in 2021, growing at a healthy CAGR of over 19.5% during the forecast period. The following figure with CCS insight predictions provides a complete image of the market potential.

The benefits of the implementation of IoT in AHA could include the following:

- Patient Engagement,
- Adjustable patient monitoring,
- Enhanced Drug Management,
- Augmented Asset Monitoring and Tracking, and
- Early intervention.

These benefits have individual risks, threats and weaknesses. These exist, are will be considered and will be developed in another D1.6 in detail.



Figure 6: Global Wearables Forecast 2016-2020. (CCS Insight, 2015)

## 2.3 Information ethics in IoT

This rapidly emerging trend of IoT, with great interconnectedness and more massive amounts of data, raises many questions in the field of ethics and information ethics. Even though public awareness about privacy risks in the Internet is increasing, in the evolution of the Internet to the Internet of Things (IoT) these risks are likely to become more relevant due to the large amount of data collected and processed by the “Things”. Information ethics is the branch of ethics that focuses on the relationship between the creation, organization, dissemination, and use of information, including the ethical standards and moral codes that govern human conduct in society. Areas of interest in terms of information ethics include privacy, moral agency and behaviours and problems arising from the information life-cycle. It stands on the edge of the fields of computer ethics and philosophy of information, so it has been considered important to be included in this Section of the Deliverable.

Ethical considerations are a new topic in the context of IoT. The large increase in the amount of information gathered and the potential loss of control over the information and types of actions that the IoT may initiate, autonomously raises significant ethical issues. Additionally, another key aspect of the work on ethics with respect to IoT is that it is hard to get people engaged in describing the issues involved, even though everyone agrees that ethics is important, since the point of the IoT is to provide autonomy to the devices involved and this may rise important ethical issues related to autonomy of things and humans, privacy, security, freedom, liberty, equity, equality, justice, fairness, access, discrimination and others. As a matter of fact, the European Group on Ethics in Science and New Technologies asserts that IoT will bring a radical change to the control that humans have over their environment by providing interconnected autonomous objects the ability to communicate with each other and take actions that impact the lives of individuals without those individuals being involved in the process (Freeman and Peace, 2005).

If one is looking for a simple definition of IoT, one could find it on Wikipedia, which defines the information ethics as the following:

*“Information ethics has been defined as “the branch of ethics that focuses on the relationship between the creation, organization, dissemination, and use of information, and the ethical standards and moral codes governing human conduct in society”. (Joan, 2010)*

Information ethics focuses on the relationship between the creation, organization, dissemination, and use of information, including the ethical standards and moral codes that govern human conduct in society. It also determines a framework to define moral issues concerning informational privacy, moral agency, new environmental issues, problems arising from the life-cycle of information.

Among experts in ethics there is no consensus rather a debate on how the IoT impact ethical issues. Thus, there are ethical arguments among experts in favour and also against IoT. Ethical arguments in favour, focus on the benefits it brings in terms of wellbeing, health, utility, safety and security, and the moral responsibilities it brings in terms of promoted ethically motivated decision making (i.e. better decision-making) – or not? Thus, there is a number of ethically relevant characteristics of IoT including ubiquity, invisibility, ambiguous ontology identification, connectivity, etc. Specifically, according to Jeroen Van Den Hoven, a member of the Ethics IoT Subgroup of the European Commission, Delft University of Technology there are specific characteristics of IoT which may raise ethical and moral concerns (Hoven, 2012) and these are quoted below:

1. **Ubiquity and pervasiveness.** The user is engulfed and immersed by IoT and there are no clear ways of opting out of a fully-fledged IoT, except for a retreat into a pristine natural and artefact less environment, which will be hard to come by in the remainder of the 21st century.
2. **Miniaturization and invisibility:** The desk top computer as we know it will gradually disappear or will stop to serve as the paradigm case of a computing device. Computing technology will become translucent and has the tendency to disappear from human sight. So, although the functionality is prominent and ubiquitous, it will for a good part be inconspicuous or invisible. This calls for special design measures to make the technology visible and amenable to inspection, audit, quality control and accountability procedures.
3. **Ambiguity and ontology:** The distinctions between natural objects, artefacts and human beings tends to blur as a result of the facile transformation of entities of one type into the other by means of tagging, engineering and absorption into a networks of artefacts. We will have to deal both practically and conceptually with ambiguous criteria of identity and system boundaries.
4. **Identification:** Electronic identity of things and objects achieved by tagging and networking of objects. We will have to get used to the fact that – apart from special and cherished objects and artefacts, many more and seemingly insignificant objects and artefacts will have unique identities. This feature is crucial for the idea of IoT. Who gets to assign, administrate and manage these identities, will access to them and to what they entail in a globalizing world is a non-trivial governance issue.
5. **Connectivity:** High and unprecedented degree of connectivity between objects and persons in networks. High degree of production and transfer of data.
6. **Mediation and autonomous agency:** The IoT environment provides ways of extending and augmenting human agency, even to the point that it may exhibit artificial and spontaneous and emerging agency. IoT environments may present spontaneous interventions in the course of human events which are not directly caused by human agents or operators and which are unforeseen and unexpected. Human beings will act in IoT environments together and in concert with artefacts, devices and systems, thus constituting hybrid systems.
7. **Embedded intelligence and extended mind:** Smart and dynamic objects, with emergent behaviour, embedding intelligence and knowledge function as tools and become (external) extension to the human body and mind. As is already the case to a certain extent with traditional computing artefacts, access the intelligent and data carrying IoT environment may come to be considered as necessary for human agents to get around. Similar to the info available through a mobile phone, and access to your Social Networking Site, people would feel cognitively and socially handicapped.
8. **Seamless transfer:** Interaction, information flow with IoT context will be effortless, with potentially very low transaction and information cost.
9. **Distributed control:** The locus of control and governance of IoT will not be a central one, because of its vast amount of nodes, hubs and data. It will see emergent properties and phenomena, and will have to be governed and monitored in ways adequate for its distributed nature. This has implications for the locus of accountability.
10. **Big Data:** IoT is the locus of tremendous data generation, storage and flow and processing at Exabyte level and beyond.

**11. Unpredictability and uncertainty:** Incremental development of IoT will lead to emerging behaviours without the user having full or even relevant knowledge of the IoT environment.

The aforementioned characteristics of IoT, are rising an additional set of ethical and moral issues that should also be taken into account in the Ethical Design process.

### 1. Trust

In the IoT sector, boundaries between private and public entities get blurred, and sometimes they get invisible. Thus, users may feel a sense of unease since they do not know what information they actually share and with whom. This may raise the quandary of trust. The fear of privacy offense, the idea of a ubiquitous network, and reliability issues challenge trust in IoT.

Therefore, IoT and its applications should be designed to be trustworthy. This means that the design of the IoT should include components to support trust while using the IoT services and provide mutual trust among the IoT users. For example, the provision of authentication functions to ensure that only authenticated and certified entities can provide the IoT services is an element to build trust because the user can have confidence in using those IoT services and authenticated users can be held accountable and liable. Another example more related to the data privacy protection is to explicitly respect data collection relating to purpose, and provide transparency of data collection and distribution, thus limiting risks in terms of use of personal data.

### 2. Digital divide

The “digital divide” is seen as one of the policy challenges for the development of IoT. The digital divide will be increased in the IoT, as it will be understood only by few experts. It is questionable whether there is a possibly fair distribution of benefits and costs, as well as equal opportunities for all in accessing the IoT, since it could easily end up amplifying the divide between capable users and those intimidated or outpaced by this new technology. Moreover, the communication from one device to another will influence people’s lives in ways which are hard to imagine as long as there will not be a coherent, legal and democratic frame to depict the limits of this process. Digital divide from unwanted data transfers and processing may also result into user distress and even legal appeals as far as accountability is concerned.

The digital divide – that the IoT may end up reinforcing – goes beyond the commonly described term. It may also describe other divides that the IoT features like automations, transfers and ubiquity may create due to overwhelming consent demands. Hoven (Hoven, 2010) introduces the term “consent fatigue”, explaining that more divides may occur since users do not have the time to keep pace with all consent activities they need to respond to.

### 3. Transparency and accountability

Transparency is a fundamental condition for enabling individuals to control their own data and to ensure personal data protection. It is therefore essential that individuals should be well and clearly informed, in a transparent way, by data controllers about how and by whom their data are collected and processed (for what reasons, for how long, how it will be shared with others and what their rights are if they want to access, rectify or delete their data) (Articles 10 and 11 of Directive 95/46/EC).

According to the European Commission<sup>1</sup>, “*basic elements of transparency are the requirements that the information must be easily accessible and easy to understand, and*

---

<sup>1</sup> Communication “COM(2010) 609 final” <[ec.europa.eu/justice/news/consulting\\_public/0006/com\\_2010\\_609\\_en.pdf](http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf)>, dated November 4, 2010, from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, with the title “A comprehensive approach on personal data protection in the European Union”.

*that clear and plain language is used.*” These requirements apply also to IoT, where privacy boundaries are unclear, difficult to assess, non-transparent and not always fully regulated.

The existing legal protection framework for consumers and citizens was not developed to include the IoT. Thus there is a need to establish an IoT environment that respects the existing legal framework, while preparing the evolution of the regulatory framework to reflect a changing future world. In this context, connected IoT devices based on Ethical Design with commonly agreed standards for trust and privacy allowing the IoT to innovate and grow also in a beneficial way for society are an important element to support this framework. Thus, investment in transparency and openness of the design and development of IoT should be encouraged and realized.

#### 4. Moral Agency

As the IoT created an environment where objects act and take options in invisible but intentional ways, on behalf of human users, a hybrid moral agency (e.g. whether artificial agents are moral) on behalf of the user comes into being. Moral agency becomes an IoT ethical issue since the intentionality of delegated actions of the objects, is not controlled by the user, it does not identify with the user’s identity and compromises their integrity and eventually their freedom. There are a lot of common points with this and the research in robotics, particularly about Care-Robots, and robot companion. Those robots were already encompassing IoT and the research on ethics about them can be used in the future (Ruiz et al. 2014).

IoT is characterized by high degree of connectivity and numerous interconnected and interacting entities, including both objects and also users. This system is overwhelmed by pervasiveness, invisibility, ubiquity, seamless transfers and leads the user to stop noticing presence, transactions, and eventually actions taken on their behalf. But, who are the agents of this system in the first place? The users, the objects, or both?

In such an automated, ubiquitous and translucent environment, *unpredictability*, described as unpredictable emergent behaviours due to potentially accessible IoT infrastructure from anywhere at any time (Wright et al. (EDS). 2008), is a major issue. Thus, under the moral agency discussion, unpredictability is a key feature, since there will always be incremental developments and deployments, leading into emerging relationships and behaviours and making decisions on behalf for people, without them having full realisation of it.

#### 5. Autonomy: Informed consent vs. obfuscation of functionality

While some autonomy is beneficial, absolute autonomy is frightening. For one thing, it is clear that legal systems are not yet prepared for high autonomy systems, even in scenarios that are relatively simple to envisage, such as the possession of personal information.

We have already described in detail the tendency of IoT environments to become transparent and to disappear from the users’ sight. The tags, sensors and micro-electronics technologies that are supporting the IoT move towards the nano-scale and literally disappear from sight, as they autonomously react in the users or the environments priming. While some autonomy is beneficial, absolute autonomy is frightening. For one thing, it is clear that legal systems are not yet prepared for high autonomy systems, even in scenarios that are relatively simple to envisage.

In addition to the aforementioned ethical issues, ETICA projects has launched in its final report (Stahl et. al., 2011) a set of ethical concerns related to IoT that we should not neglect and these include the following:

- Autonomy, freedom, agency,
- Possibility of persuasion or coercion,
- Responsibility, liability,
- The possibility of machine ethics,

- Access, digital divides, power issues
- Consequences of technology for our view of humans
- Conceptual issues (e.g. notions of emotions, intelligence),
- Link between and integration of ethics into law, and
- Culturally different perceptions of ethics.

## 2.4 Information ethics in IoT and AHA

As described in the previous section, many ethical questions in relation to IoT are raising. This gets even more intense when the IoT is implemented to the Active Health and Aging (AHA) sector. While continuous monitoring of homes and human activity can offer a safer environment for older people, many wary about ethical issues like constant surveillance and lack of control over data collected; while the situation gets more complex in the care of older people with cognitive impairments who may not be in a position to participate in the decision-making process around privacy settings.

An ethically designed IoT for AHA is very important since it will assist medical professionals, carers and other health service providers in meeting their moral responsibilities in providing healthcare and management. Likewise, users will be empowered and protected from exploitation and harm coming from the IoT for AHA. By creating and adopting an ethical framework and guidelines, also developers can demonstrate a serious commitment to meeting their legal and moral responsibilities to users, care providers and other stakeholders. Further, adoption will prevent many foreseeable ethical problems in the design and roll out of IoT for AHA devices and protocols, for which developers would be legally or morally liable.

In order to develop a framework of ethical guidelines in relation to IoT for AHA, we start from the European Union policies including the Digital Agenda and ICT Governance Promoting, which are promoting a framework of ethical values, together with the commitment to peace and the well-being of the Union's peoples. Thus, in its Opinion No. 26 on Ethics of Information and Communication Technologies (EGE, 2012) emphasizes especially the importance of the following principles:

**Human dignity:** The Charter of Fundamental Rights of the European Union states that 'Human dignity is inviolable. It must be respected and protected' (Article 1) and also discussed with users themselves.

**Respect of freedom** which secures, inter alia, the right to uncensored communication and agency in the digital era.

**Respect for democracy, citizenship and participation** which includes, inter alia, protection against unjustified exclusion and protection against unlawful discrimination;

**Respect of privacy** which secures, inter alia, the personal private sphere against unjustified interventions;

**Respect of autonomy and informed consent** which secures, inter alia, the right to information and consent to the use of data or actions that are based on the data-processing;

**Justice** which secures, inter alia, the equal access to ICT, and a fair sharing of its benefits;

**Solidarity** among European citizens aims, inter alia, at the inclusion of everyone who wishes to participate in ICT, but also aims to secure the social inclusion of those who, for example, either cannot participate in online practices or wish to maintain alternative social interactions.

In addition to the aforementioned principles, another crucial set of guidelines that should be taken into account while designing for IoT for AHA, is the Internet of Things "Bill of Rights" published by Pachube in 2011. This bill of rights can be used as a starting point for building an ethics framework for AHA and includes the following principles:

- People own the data they (or their “things”) create.
- People own the data someone else creates about them.
- People have the right to access data gathered from public space.
- People have the right to access their data in full resolution in real-time.
- People have the right to access their data in a standard format.
- People have the right to delete or backup their data.
- People have the right to use and share their data however they want.
- People have the right to keep their data private.

To contribute to the ethical design of the Active Health and Aging (AHA) IoT, taking into account the EGE principles and the Bill of rights, a set of ethical principles has been proposed, as abstract requirements for the design of the devices and data protocols used in such an environment. This list derives from the principlist approach to medical ethics (Beauchamp & Childress, 2009) and the OECD’s Privacy Framework (OECD, 2013). These principles are the following:

1. Collect the minimum required data and store them locally, ensuring data processing protocols are transparent and accountable
2. Support the ethical capabilities of human beings such as agency, awareness and reflexivity (requiring transparency on how data are collected and distributed);
3. Create and maintain trust and confidentiality between users and providers
4. Embed inclusiveness in design
5. Facilitate public health actions and user engagement with research via IoT for AHA

These abstract ethical principles provide the baseline for developing actual technical requirements to be implemented in the IoT for AHA developments in order to assist developers in addressing real world ethical challenges with the IoT for AHA. These abstract ethical principles can be translated into guidelines used as a starting point to embed the proposed ethical principles in the design of IoT for AHA, prior to adoption by users and subsequent assessment of acceptability:

1. Give users control of the collection and distribution of data or services related to them.
2. Create protocols to protect user privacy at the early design process, using security and privacy layers in the architecture.
3. Use consent mechanisms when sharing personal data.
4. Include transparency mechanisms in data protocols
5. Provide users with practically useful mechanisms to exercise meaningful data access rights
6. Design unobtrusive systems according to the needs of specific user groups

All the aforementioned guidelines will be taken into account during ACTIVAGE process and detailed ethics plans will follow on how these guidelines have been incorporated in D1.6 that follows.

## 3 ACTIVAGE Ethics framework

### 3.1 Introduction

ACTIVAGE can be seen as a fundamental step towards improving independent living and smart living environments for ageing well of older adults and creating a harmonized IoT for AHA. Besides scientific advance, the potential benefit of ACTIVAGE will be on a social, cultural, economic and individual basis. Nevertheless, its ethical complications are not neglected and on the contrary, they are taken into account horizontally through the whole duration of the project.

ACTIVAGE's position with respect to ethical issues:

- The project targets **older adults** (healthy or not). ACTIVAGE will monitor older users with the ambition to maintain their right on active and healthy aging. Thus, the project by definition will, in most cases, involve older people that may be patients in medical terms or not.
- ACTIVAGE will screen human participants with respect to their ability to give informed consent; users with cognitive decline might not being able to provide consent (i.e. legally incapable of giving informed consent). However, the researcher will nevertheless provide appropriate explanation, consider such person's best interests and preferences, and obtain appropriate permission from the legally authorised person, if such substitute consent is permitted or required by law (APA, 2002).
- Complies fully with Horizon 2020 guidelines (see Appendix A: ACTIVAGE Ethics checklist), as they define that research conducted within the framework must comply with ethical principles and relevant national, EU and international legislation, for example the Charter of Fundamental Rights of the European Union (EU, 2000) and the European Convention on Human Rights (European Convention on Human Rights, 2005).

ACTIVAGE aims to prolong and support the independent living of older adults in their living environments and responding to real needs of caregivers, service providers and public authorities, through the deployment of innovative and user-led Large Scale IoT Pilot across nine Deployment Sites in seven European countries based on the IoT technologies. While the trends and developments of ICT in healthcare have given rise to many positive developments, concerns about the use of ICT and the IoT in healthcare can have been issued in the previous Sections, and can be summarised as following (adapted from opinion 13 from EGE):

- The pervasiveness of a technology, which many people do not understand;
- The lack of transparency of the work of healthcare professionals and its effects on the doctor/ patient relationship;
- The difficulty of respecting privacy and confidentiality when third parties may have a strong interest in getting access to electronically recorded and stored personal health data; and
- The difficulty in ensuring the security of shared personal health data.

While acknowledging that

- Personal health data necessarily touch upon the identity and private life of the individual and are thus extremely sensitive; and

- ICT creates the potential for the free circulation of personal health data, across local, national and professional borders, giving such data an enhanced European dimension;

the ACTIVAGE Consortium commits to

- The principles of the European Convention of Human Rights,
- The rules of the Convention of the Council of Europe for the protection of individuals with regards to automatic processing of personal data, and especially
- The European Directive 95/46/EC, for the protection of personal data will be strictly followed when addressing the ethical questions of ACTIVAGE.

Therefore, the ACTIVAGE Ethics and Privacy Protection Manual aims at covering the EGE principles along with the following:

- The ACTIVAGE ethical policy.
- The ethical issues and hindrances that may arise when carrying out evaluations with people suffering from various age-related and chronic conditions, such as cognitive impairments.
- Ethical considerations for health care professionals and carers involved with patients.
- EU, national and regional requirements to meet when carrying out research with humans and specifically people with age-related conditions and overall health status (national legislation per DS will be discussed in the Ethics chapter of the “Detailed experimental plan” (D9.1; M9).
- The ethical related templates (i.e. consent form, information sheets, ethics committee application form).
- Data privacy and security in data and results communication.
- Open Data Policy Planning and Ethics constraints and management.
- Mitigation strategy in case of breach of confidentiality and other ethical-related issues.
- ACTIVAGE Policy, Legal and Gender Board (PLGB) members, structure and organization.

As for the definition of partner responsibilities related to ethical issues, the following project partner regulations related to compliance, approvals, privacy, personal health information and collaboration within the project shall apply:

1. Each party shall be responsible for ensuring its own compliance with all laws and regulations applicable to its activities. Such laws include, but are not limited to, those in respect of rights of privacy, intellectual property rights and healthcare.
2. Each party represents that it has all necessary third party, hospital and/or patient consents to permit distribution and use of the data (including medical data) and any other information provided to other parties.
3. Any party which provides any data or information to another party in connection to the project will not include any personal information relating to an identified or identifiable natural person or data subject.
4. To this end, the providing party will anonymise all data delivered to other parties to an extent sufficient to ensure that a person without prior knowledge of the original data and its collection cannot, from the anonymised data and any other available information, deduce the personal identity of subjects.
5. Each party shall be solely responsible for the selection of specific database vendors/data collectors/data providers, and for the performance (including any breach) of its contracts between it and such database vendors/data collectors, (to which no other project partner

shall be a party, and under which no other partner assumes any obligation or liability) and shall further warrant that it has the authority to disclose the information, if any, which it provides to the other parties, and that where legally required and relevant, it has obtained appropriate informed consents from all the individuals involved.

- Partners supplying special data analysis tooling, shall have the right on written notice and without liability to terminate the license that it has granted for such tooling to be used in connection with the project, if the supplying partner knows or has reasonable cause to believe that the processing of particular data through such tooling infringes the rights (including without limitation privacy, publicity, reputation and intellectual property rights) of any third party, including of any individual.

## 3.2 Policy, Legal and Gender Board -PLGB organization

The **Policy, Legal and Gender Board -PLGB** of ACTIVAGE will be responsible the project's Ethical issues and will act as supervisors of the ethical activities of the project and the local ethics committees at each DS, in order to take into account both European and national ethical and legal requirements. The Ethical, Policy, Legal and Gender Board (PLGB) includes experts representing the diversity of views of all projects' stakeholders. It is formed by legal experts from industry and demand users of the consortium (**one per local Deployment site**), as well as by policy makers and gender equality officers from the demand cites in the consortium. The work of this board will be carried out in the context and with the resources of WP1 and especially T1.4. The place of the PLGB in the project is depicted in the figure below.

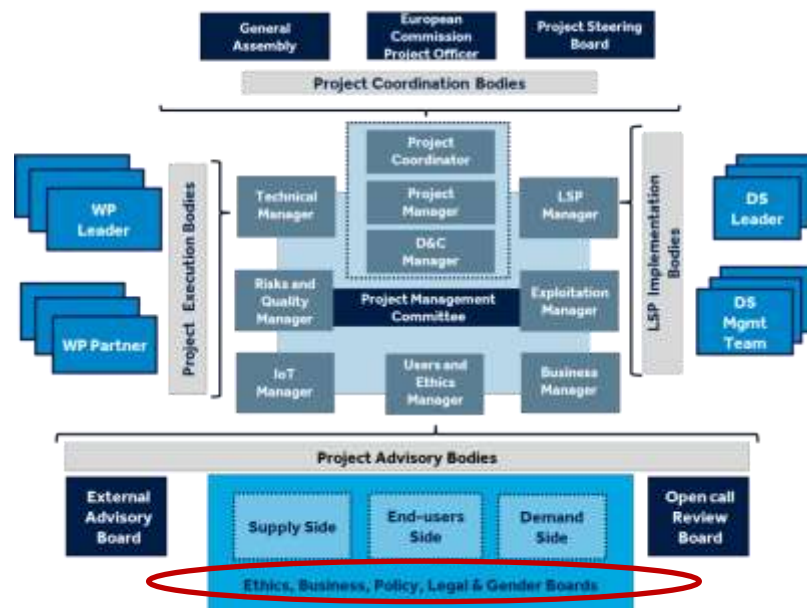


Figure 7: PLGB place in the organisational and management structure of the ACTIVAGE project.

The Ethical, Policy, Legal and Gender (PLG) Board includes experts representing the diversity of views of all projects' stakeholders. It is formed by legal experts from industry and demand users of the consortium (one per local DS), as well as by policy makers and gender equality officers from the demand cites in the consortium. The ACTIVAGE PLG Board has a duty to:

Protect private and sensitive information and ensure that participants will not be harmed during the Large Scale IoT Pilots. Collected data will be anonymous and treated as confidential.

Respect participant's free will and treat them as intelligent being who decide for themselves about any type of gathered data that are indeed outcomes of their participation.

Inform in full about how data will be collected, processed shared, and disposed before signing the consent form.

Communicate their findings through open-access journals to other researchers and academic communities (especially true if it is requested by the funder).

Include experts representing the diversity of views of all projects' stakeholders.

All used assessment tools and protocols within ACTIVAGE Large Scale IoT Pilot will be verified beforehand by its PLG Board, regarding their impact to users' well-being before being applied to the DSs. The PLG Board works for implementing and managing the ethical and legal issues of all procedures in the project, ensuring that each of the partners provides the necessary participation in ACTIVAGE and its code of conduct towards the Large Scale IoT Pilot participants.

The members of the Ethics Board are the following:

**Users and Ethics Manager (UEM) Dr Dimosthenis Ioannidis** is a Senior Researcher Associate in CERTH. He received the Diploma degree in electrical and computer engineering and the MSc. in Advanced Communication Systems and Engineering from the Electrical and Computer Engineering department of the Aristotle University of Thessaloniki in 2000 and 2005 respectively and he has been a teaching assistant at TEI Thessaloniki (2006-2010). During the last five years, he has been the (co)author of more than 25 papers and he has also been involved in more than 10 research projects. He is also currently acting as an Ethics evaluator of running projects executed under the auspices of EC, providing services such as monitoring of research activities performed in projects in respect to assigned ethics requirements. Services are related to the assessment of the human participation in real-life trials, privacy enhancing technologies used for the protection of personal data as well as other ethics issues that shall be tackled within a project lifetime (i.e. dual use, misuse and personal sensitive data).

As the Users and Ethics Manager (UEM), Dr Dimosthenis Ioannidis will be responsible for dealing with the following issues:

Legal aspects: the legal issues associated to the deployment of ACTIVAGE tools and actions (e.g. IPR, data protection and access, privacy issues, ethical aspects, etc.),

Policy issues: how the technologies deployed have an impact (positive or negative) on current policies and vice versa, i.e. how new policies could help innovative smart living technologies get users acceptance and market uptake, gender issues.

### DS Ethic's managers

#### 1. GAL, Spain DS

Leader: TELEVES, Sebastian Pantoja ([spantoja@televes.com](mailto:spantoja@televes.com))

Demand Side partners: CRE, SERGAS

Supply Side partners: TELEVES, UPV, FVE

**Ethics manager: Trinidad de Lorenzo ([delorenzo@cruzroja.es](mailto:delorenzo@cruzroja.es)), Javier Quiles ([javier.quiles.delrio@sergas.es](mailto:javier.quiles.delrio@sergas.es))**

#### 2. VLC, Spain DS

Leader: InnDEA Foundation, Elena Rocher ([elena.rocher@lasnaves.com](mailto:elena.rocher@lasnaves.com))

Demand Side partners: InnDEA Foundation, ATENZIA, ISI BENESTAR

Supply Side partners: MYSPHERA

**Ethics manager: J. Mario Lecumberri ([jmlcumberri@isibenestar.com](mailto:jmlcumberri@isibenestar.com))**

#### 3. MAD, Spain DS

Leader: TEA, Angeles Mata ([amata@terceraedadactiva.es](mailto:amata@terceraedadactiva.es))

Demand Side partners: TEA

Supply Side partners: TECNALIA, LST-UPM

**Ethics manager: Angeles Mata Dias ([amata@terceraedadactiva.es](mailto:amata@terceraedadactiva.es))**

#### 4. RER, Italy DS

Leader: C2K, Stefano Nunziata ([stefano.nunziata@cup2000.it](mailto:stefano.nunziata@cup2000.it))

Demand Side partners: C2K, LHA Parma, AURORA

Supply Side partners: CNR-ISTI, UNI PR, IBM, WIND

**Ethics manager: Enrico Montanari ([emontanari@ausl.pr.it](mailto:emontanari@ausl.pr.it))**

#### 5. GRC, Greece DS

Leader: CERTH/ITI Kostas Votis ([kvotis@certh.gr](mailto:kvotis@certh.gr))

Demand Side partners: MM, IDS-DC-CGR

Supply Side partners: CERTH, ICCS, INFOTRIP, GNOMON

**Ethics manager: CERTH/ITI Dimos Ioannides ([djoannid@iti.gr](mailto:djoannid@iti.gr))**

#### 6. ISE, France DS

Leader: CEA Isabelle Chartier ([isabelle.chartier@cea.fr](mailto:isabelle.chartier@cea.fr))

Demand Side partners: CD38, TASDA, MADOPA, KORIAN, IMA

Supply Side partners: CEA, FFD, STM, TECHNO

**Ethics manager: Alexandre Duclos ([alexandre.duclos@madopa.fr](mailto:alexandre.duclos@madopa.fr))**

#### 7. WOQ, Germany DS

Leader: SL, Reiner Wichert ([reiner.wichert@sageliving.de](mailto:reiner.wichert@sageliving.de))

Demand Side partners: AJT

Supply Side partners: SL, Fh-IGD

**Ethics manager: Reiner Wichert ([reiner.wichert@sageliving.de](mailto:reiner.wichert@sageliving.de))**

#### 8. LEE, UK DS

Leader: Rohit Ail ([rohit.ail@samsung.com](mailto:rohit.ail@samsung.com))

Demand Side partners: LCC, UniS

Supply Side partners: Samsung, CSEM

**Ethics manager: Suzanne Moton ([Suzanne.morton@leedsbeckett.ac.uk](mailto:Suzanne.morton@leedsbeckett.ac.uk)) and Rohit Ail ([rohit.ail@samsung.com](mailto:rohit.ail@samsung.com))**

#### 9. FIN, Finland DS

Leader: SEN, rauno.saarnio@seniorsome.com & vesa-pekka.ala-siuru@seniorsome.com

Demand Side partners: SEN, GoodLife, eHoiva

Supply Side partners: SEN, GoodLife, eHoiva

**Ethics manager : Vesa-Pekka Ala-Siuru ([vesa-pekka.ala-siuru@seniorsome.com](mailto:vesa-pekka.ala-siuru@seniorsome.com))**

The ACTIVAGE PLG Board is supported by the Project Coordinator (PC), Mr German Gutierrez (MEDTRONIC), and the technical manager Giuseppe Fico (UPM). The WP1 leader (MEDTRONIC) is in close collaboration with both the project's PLG Board and the project management team.

Among the PLG Board roles is the resolution of any potential ethics related conflicts and the mitigation of risks that might arise. If a situation arises, then a decision will be centrally reached, in collaboration with the site where the problem exists and a solution will be found and communicated. The resolution of any ethical related emerging issues will be dealt first by the local site responsible and, if necessary, the issue will be discussed with the WP9 Large Scale IoT Pilot manager. In any case, the WP 9 leader will be informed about any communications and will act as mediator between the DS managers and the PLG Board committee. In case there is a possibility the situation to affect the work carried out in several packages/domains of the project, then it will be addressed by the ACTIVAGE PLG Board. Regardless of level of involvement, the central PLG Board will be informed by any arising

issues, even if they are happening and being resolved – at the local sites they firstly have arisen. All Ethics applications to regional/ national boards submitted for approval before any testing commences, will be first approved by the project's PLG Board.

Different levels of ethics management ensure time-efficient address of issues and risks during the lifetime of the project, especially when a large number of services and tools will be evaluated for long periods of time by large number of users.

## 3.3 ACTIVAGE DS ethical strategy

### 3.3.1 ACTIVAGE DS description

ACTIVAGE targets citizens living in European cities for supporting and extending their independent living based on an advanced, interoperable, secure and privacy-aware IoT ecosystem. In particular, ACTIVAGE will include a large number of user groups being representative of the respective population stratification within each DS foreseen in seven European countries (France, Germany, Greece, Italy, Spain, Finland, UK). The consortium is fully aware of the ethics and privacy issues stemming from the deployment of IoT - related technologies that are able to collect, distribute and exchange information within intelligent environments as the one to be introduced as end-to-end ecosystem of ACTIVAGE.

### 3.3.2 ACTIVAGE DS ethics strategy

Each DS nominates an ethics responsible person (Section 3.2) as responsible for adhering ACTIVAGE Ethics policy, as well as protecting the confidentiality and anonymity of local participants. Therefore, this person is responsible to contact and obtain ethics approval by the local/ regional ethics committee(s) and for securely and anonymously storing user data (i.e. different data will be gathered in different pilot sites).

The DS ethics manager, as presented in Section 3.2, is the person who represents each DS participating in ACTIVAGE Large scale IoT Pilots. In case the DS technical managers decide to place another person in charge of ethics, then Section 3.2 has to be updated. The DS ethics manager will be the main contact point for any ethics related issues (e.g. submission of research protocols for approval, etc.). The ACTIVAGE LGP Board will train and monitor the ethics site responsible to abide to the European and national regulation, laws, and guidelines.

The ACTIVAGE LGP Board is closely collaborating with the DS ethics manager at each DS and the WP9 leader acting as an evaluation responsible partner who will act as the moderator and communicator between the pilot sites and the project's Ethics Board team. The local pilot site responsible partners will co-ordinate and will be responsible for obtaining approval by the local/regional/institutional ethics committee before any pilot related activities take place (e.g. even before recruitment starts).

The DS ethics manager at site will train and appoint the person who will be managing and organising recruitment processes and safekeeping of participants contact details. The DS ethics manager will inform the LGP Board of any recruitment issues and threats that may appear with regards to data protection and end-user involvement in pilots. The LGP Board is obliged to obey the national and European legislation and code of practices and has to fully support and scrutinize any plans, operational documents, and research protocols to guarantee that the Ethics policy is applied in all activities and foremost when and where users are involved. Any required or requested authorisations and approvals remain official project documents at any times. Partners should ensure timely submission of research

protocols based on their previous experience with relevant bodies in order to avoid any delays in the pilot's instantiation.

All DS ethics managers have been asked, in Month 3 to fill in a specific ethics questionnaire, available in Appendix D of the current document. In this document, the ethics managers were asked to report specific details on their DS, for example the participants they aim to include and the profile of the specific devices that will be tested, in order to have a holistic view of what will be tested and where. The following table provides the details described from the DS ethics managers.

Country	Deployment site	Site partner	Ethics responsible	DS profile (types of services to be tested)	DS participants (main targeted user groups)
Finland	DS FIN	Turku	Niina Katajapuu / Paula Ailio	<ul style="list-style-type: none"> <li>- Daily activity monitoring</li> <li>- Integrated care</li> <li>- Exercise promotion</li> <li>- Pain monitoring</li> </ul>	- Older people (specific groups to be defined)
		Helsinki	V-P Ala-Siuru /and repr. of Helsinki Service Center	<ul style="list-style-type: none"> <li>- Daily activity monitoring</li> <li>- Integrated care</li> <li>- Exercise promotion</li> <li>- Pain monitoring</li> </ul>	- Older people (specific groups to be defined)
		Oulu	Vesa-Pekka Ala-Siuru / and representative of city of Oulu	<ul style="list-style-type: none"> <li>- Daily activity monitoring</li> <li>- Integrated care</li> <li>- Exercise promotion</li> </ul>	<ul style="list-style-type: none"> <li>- Special groups (Foster care families)</li> <li>- Other special groups older and younger people</li> </ul>
		Tampere	V-P Ala-Siuru /and repr. of Sopimusvuori Oy	<ul style="list-style-type: none"> <li>- Daily activity monitoring</li> <li>- Exercise promotion</li> </ul>	- Older people (specific groups to be defined)
Spain	DS GAL	TVES, UPV, FVE, SERGAS, CRE.	<ol style="list-style-type: none"> <li>1) Loreto Somoza (temporaly: we will inform with the contact of a new person as soon as possible)</li> <li>2) Javier Quiles</li> <li>3) Álvaro Sanchez</li> <li>4) Ana Arroyo</li> </ol>	<ul style="list-style-type: none"> <li>- Home tele-care.</li> <li>- Social monitoring through the use of sensors to register the behaviour.</li> <li>- Monitoring of health through the use of medical devices to register medical measures.</li> <li>- Cognitive stimulation.</li> </ul>	<ul style="list-style-type: none"> <li>- Older people.</li> <li>- People with chronic diseases: pathologies like Atrial fibrillation.</li> <li>- People at the risk of chronic disease: hypertension, obesity, diabetes.</li> <li>- People with low social participation and/or problems of loneliness.</li> <li>- People with difficulties in following a healthy lifestyle and/or patterns of self-care related to health.</li> <li>- People with dependency needs.</li> <li>- People with mild level of cognitive impairment.</li> </ul>
France	DS ISE	CEA STM	Alexandre Duclos	<ul style="list-style-type: none"> <li>- Daily activity monitoring,</li> <li>- Emergency trigger,</li> </ul>	<ul style="list-style-type: none"> <li>- UC 1 Autonomous seniors</li> <li>- UC 2 FALLERS person who have</li> </ul>

Country	Deployment site	Site partner	Ethics responsible	DS profile (types of services to be tested)	DS participants (main targeted user groups)
		Technosens Tasda MADOPA : IMA Institut du Bien Vieillir - Korian		<ul style="list-style-type: none"> <li>- Exercise promotion,</li> <li>- Prevention of social isolation,</li> <li>- Safety &amp; comfort at home</li> </ul>	<ul style="list-style-type: none"> <li>- fallen twice / 12 month</li> <li>- UC 3 Hospitalized Person in a rehabilitation center after an accident</li> </ul>
Spain	DS MAD	TEA TECNALIA UPM	Angeles Mata	<ul style="list-style-type: none"> <li>- Beacon kits</li> <li>- Wristband</li> <li>- Blood pressure health monitoring device</li> <li>- Pulse pressure health monitoring device</li> <li>- Android Phone</li> <li>- Laptop</li> <li>- Equimetrix</li> <li>- Mobile data connections</li> <li>- Wireless magnetic door contact sensor</li> </ul>	PARTICIPANTS IN FRAILTY SCALE 3 TO 6
Italy	DS RER	LHA PARMA	Enrico Montanari	<ul style="list-style-type: none"> <li>- Monitoring sensors to detect contingent situation that could be of interest of the informal care giver;</li> <li>- Monitoring sensors to detect trends and analyse these trends for the benefit of the case and care manager</li> <li>- Video conference to assist physiotherapist for a tele check up</li> </ul>	<ul style="list-style-type: none"> <li>- Practitioners, Nurse Coordinator, assistant operators engineers; computer technician</li> </ul>
England	DS UK	Leeds City council	Suzanne Morton	<ul style="list-style-type: none"> <li>- Daily activity monitoring</li> <li>- Emergency triggers</li> <li>- Reduction in social isolation</li> </ul>	<ul style="list-style-type: none"> <li>- Over 65s living in Leeds, from frailty 2 - 6 on scale. May be healthy or have one or more co-morbidities</li> </ul>

Country	Deployment site	Site partner	Ethics responsible	DS profile (types of services to be tested)	DS participants (main targeted user groups)
Spain	DS VAL	Valencia	J.M. Lecumberri	<ul style="list-style-type: none"> <li>- Magnetic sensor (indoor)</li> <li>- Movement sensor (indoor)</li> <li>- Smart phone (outdoor)</li> <li>- Smart watch (indoors/outdoors)</li> <li>- App mobile</li> </ul>	<ul style="list-style-type: none"> <li>- Older people</li> <li>- Caregivers</li> </ul>
Germany	DS WOQ	SL	Reiner Wichert (SL)	<ul style="list-style-type: none"> <li>- Emergency trigger</li> <li>- Safety, comfort and security at Home</li> </ul>	<ul style="list-style-type: none"> <li>- Primary end users are the inhabitants of the apartments</li> <li>- Secondary users are the neighbours and relatives of the inhabitants</li> </ul>
Greece	DS GR	Cities Net, MPH, MP.	Each Pilot Site (Cities Net, MPH, MP) as well as Mrs. Eleni Chalkia (CERTH), Mr. George Dafoulas (Cities Net)	<ul style="list-style-type: none"> <li>- Daily activity behavior monitoring at home and outdoor for formal and informal carers support and follow up</li> <li>- Tele-Health services: Basic health telemonitoring devices (spirometer, blood pressure), tablets</li> <li>- Monitoring of behavioral and mobility patterns</li> <li>- Personalised trip alerts</li> <li>- Advanced cooperative mobility services adapted for ageing population (C-ITS)</li> </ul>	<p>The Greek pilot site involves the following direct categories of users.</p> <ul style="list-style-type: none"> <li>- elderly people (65+), older adults living alone</li> <li>- Healthcare professionals/ relatives/social environment /caregivers</li> <li>- Health care providers - Service providers / Care centers,</li> <li>- The whole smart living -AAL ecosystem and Integrated care in general</li> <li>- Mobility and transport providers, SMEs</li> </ul>

Additionally, the DS Ethics managers were asked to define the local DS data privacy and ethical issues of their country. The following tables 1 to 9 present the conditions at each DS.

Table 1: Data privacy and Ethical issues at Finnish DS

	DS FIN
National ethics controlling body.	The Finnish Advisory Board on Research Integrity (TENK)
National ethics controlling body procedure	<a href="http://www.tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf">http://www.tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf</a>
National legislation in application of AHA IoT practices in your country.	No
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	No
Doctors who apply IoT in AHA practices should be authorized by a legal authority.	No
National legislation or law direction for the applying of medical devices to the patients	<a href="http://www.valvira.fi/web/en/healthcare/health-technology">http://www.valvira.fi/web/en/healthcare/health-technology</a>
Ethics controlling committee for the organizations and hospitals who apply IoT practices.	Each research organization has their own ethics committees that analyze the research activities.
Established Data Protection Authority which should be followed	<a href="http://www.tietosuoja.fi/en/index.html">http://www.tietosuoja.fi/en/index.html</a>
Official national or international guidelines on protecting data privacy	<a href="http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf">http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf</a> -personal data protection act in Finland and the coming in EU EU General Data Protection Regulation ( GDPR) <a href="http://www.euqdp.org/">http://www.euqdp.org/</a>
National laws or legislation for protecting patient's information	<a href="http://www.tietosuoja.fi/en/index.html">http://www.tietosuoja.fi/en/index.html</a> 785/1992 English Act on the Status and Rights of Patients
Access to health records and databases should be authorized by a legal authority	9.2.2007/159 Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (Law on the digital handling of client data in social and healthcare) Information system handling this kind of data has to be accepted by Valvira The National Supervisory Authority for Welfare and Health
Are patient data allowed abroad	Not yet. Current guidelines can be found here: the current guidelines: <a href="https://www.choosehealthcare.fi/healthcare-in-finland/medical-records-in-finland/">https://www.choosehealthcare.fi/healthcare-in-finland/medical-records-in-finland/</a>
Patient data collecting system	The Finnish Kanta system is the official Health Data

used in your country	<p>Repository in the Finnish Health System.</p> <p><a href="http://www.kanta.fi/en/earkisto-esittely">http://www.kanta.fi/en/earkisto-esittely</a></p> <p>We have to take to account how the system, which is going to be further developed in the ACTIVAGE project, is connected to the Kanta system. In this situation we have to take care also that our system is interoperable and meets the standards (HL7 etc.) and data security is guaranteed.</p>
----------------------	---

Table 2: Data privacy and Ethical issues at Spanish DS

	DS GAL
National ethics controlling body.	<p>In the health field, the ethics controlling bodies depend on a Regional structure. The ethics controlling body in the region of Galicia is the “Galician Ethics Committee” depending on the Regional Ministry of Health.</p> <p>In the social field, there is no controlling body for ethical issues.</p>
National ethics controlling body procedure.	<p>Standard working procedures of the ethical committee on clinical research (CEIC) of Galicia:</p> <p><a href="http://www.sergas.es/cas/servicios/docs/investigacionclinica/procedimientos_normalizados_de_trabajo.htm">http://www.sergas.es/cas/servicios/docs/investigacionclinica/procedimientos_normalizados_de_trabajo.htm</a></p> <p>Spanish Red Cross can only contribute to this question with the information about their Fundamental Principles and Conduct Code that are always applied in the development of the Spanish Red Cross’ activity:</p> <p><a href="https://www.cruzroja.es/principal/documents/16917/420436/Código+de+conducta+CRE.pdf/d1584b0e-c470-468a-96f5-2ced8a4c6c33">https://www.cruzroja.es/principal/documents/16917/420436/Código+de+conducta+CRE.pdf/d1584b0e-c470-468a-96f5-2ced8a4c6c33</a></p>
National legislation in application of AHA IoT practices in your country.	No
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	No
Doctors who apply IoT in AHA practices should be authorized by a legal authority.	<p>In the health field, every clinical practice not considered under R&amp;D activities must be approved by the “National Ministry of Health” and included in the “National Health Services Catalogue”. Related regulations:</p> <p>“Real Decreto 1030/2006, de 15 de septiembre”</p> <p>“Ley 14/1986, de 25 de abril”</p> <p>“Real Decreto 63/1995, de 20 de enero”</p> <p>“Ley 16/2003, de 28 de mayo”</p>
National legislation or law	Directive 93/42/EEC is the European directive that regulates

	DS GAL
direction for the applying of medical devices to the patients.	what is considered a health product and which rules apply to those products. This directive is adapted for Spain in “Real Decreto 1591/2009, de 16 de octubre”
Ethics controlling committee for the organizations and hospitals who apply IoT practices.	The ethics controlling body for all Hospitals and Health Organizations that use IoT in the region of Galicia is the “Galician Ethics Committee” depending on the Regional Ministry of Health
Established Data Protection Authority which should be followed	The Data Protection Act (Law 15/1999 on the protection of personal data) implemented Directive 95/46/EC on data protection (Data Protection Directive). It protects individuals with regard to the processing of personal data and the free movement of data.  The Regulation developing the Data Protection Act was approved by Royal Decree 1720/2007 of 21 December (Data Protection Regulations).
Official national or international guidelines on protecting data privacy.	All the partners involved in the Galician DS apply the “Law 15/1999” in our procedures and projects
National laws or legislation for protecting patient’s information.	In Galicia, patient information is protected by the following specific regulations: “Ley 14/1986, de 25 de abril”, general health. “Ley 41/2002, de 14 de noviembre”, basic regulation of the autonomy of the patient and of rights and obligations in the matter of information and clinical documentation. “Ley 3/2001, de 28 de mayo”, Regulator of informed consent and the medical history of patients. “DECRETO 29/2009, de 5 de febrero”, by which regulates the use and access to electronic medical records. “DECRETO 164/2013, de 24 de octubre”, by which modifies the Decree 29/2009, of 5 of February, that regulates the use and access to the electronic medical history. “DECRETO 89/2016, de 30 de junio”, by which regulates the creation, the use and the access to the unique social history electronic. “ORDEN de 19 de septiembre de 2016”, by which the personal health folder is created and regulated.
Access to health records and databases should be authorized by a legal authority.	In Galicia, Access to health records and databases is governed by the following normatives: “DECRETO 29/2009, de 5 de febrero”, by which regulates the use and access to electronic medical records. “ORDEN de 26 de octubre de 2011” Which specifies technical and / or scientific criteria for access to medical records for epidemiological and public health purposes.

	DS GAL
Are patient data allowed abroad	No
Patient data collecting system used in your country	<p>Clinical data (UC1, UC2): Clinical data are collected in the system "SiSENS", and can be consulted from the Electronic Clinical History of Sergas (IANUS / HCEPRO)</p> <p>URL: Not accessible from the internet (intranet sergas)</p> <p>Social Data (UC1, UC2, UC4, UC6, UC7): Social data are collected in the system "Carelife" (Anonymised with a key)</p> <p>URL: <a href="https://user.carelifeliveservices.com/CareLife/">https://user.carelifeliveservices.com/CareLife/</a></p>

Table 3: Data privacy and Ethical issues at French DS

	DS ISE
National ethics controlling body.	<p><a href="http://ansm.sante.fr/">http://ansm.sante.fr/</a> (biomedical engineering)</p> <p>CPP (ethical research committees)</p>
National ethics controlling body procedure.	<a href="https://vrb.sante.gouv.fr/vrb/">https://vrb.sante.gouv.fr/vrb/</a>
National legislation in application of AHA IoT practices in your country.	CCTIRS : <a href="http://www.enseignementsup-recherche.gouv.fr/cid20537/cctirs.html">http://www.enseignementsup-recherche.gouv.fr/cid20537/cctirs.html</a>
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	<a href="http://cache.media.enseignementsup-recherche.gouv.fr/file/Mediatheque/84/2/20842_20842.pdf">http://cache.media.enseignementsup-recherche.gouv.fr/file/Mediatheque/84/2/20842_20842.pdf</a>
Doctors who apply IoT in AHA practices should be authorized by a legal authority.	No
National legislation or law direction for the applying of medical devices to the patients.	Loi Jardé : <a href="https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=CC895B0A0D9DEA7EEDCC9781ABEC7FBA.tpdila18v_1?cidTexte=JORFTEXT000025441587&amp;dateTexte=20161117">https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=CC895B0A0D9DEA7EEDCC9781ABEC7FBA.tpdila18v_1?cidTexte=JORFTEXT000025441587&amp;dateTexte=20161117</a>
Ethics controlling committee for the organizations and hospitals who apply IoT practices.	No
Established Data Protection Authority which should be followed	<a href="https://www.cnil.fr">https://www.cnil.fr</a>
Official national or	<a href="https://www.cnil.fr/fr/declarer-un-fichier">https://www.cnil.fr/fr/declarer-un-fichier</a>

international guidelines on protecting data privacy.	
National laws or legislation for protecting patient's information.	<a href="https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee">https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee</a>
Access to health records and databases should be authorized by a legal authority.	<a href="https://www.cnil.fr">https://www.cnil.fr</a>
Are patient data allowed abroad	Yes
Patient data collecting system used in your country	SNDS ( <a href="https://www.cnil.fr/fr/snds-systeme-national-des-donnees-de-sante">https://www.cnil.fr/fr/snds-systeme-national-des-donnees-de-sante</a> )

Table 4: Data privacy and Ethical issues at Spanish (Madrid) DS

	DS MAD
National ethics controlling body.	AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (for data protection) AGENCIA ESPAÑOLA DEL MEDICAMENTO (for medical devices authorization)
National ethics controlling body procedure.	(1) Consultation if the device can be considered medical to the controlling body mentioned before (2) Fulfilment of the Law Protection Data
National legislation in application of AHA IoT practices in your country.	No
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	No
Doctors who apply IoT in AHA practices should be authorized by a legal authority.	No
National legislation or law direction for the applying of medical devices to the patients.	No
Ethics controlling committee for the organizations and hospitals	No

	DS MAD
who apply IoT practices.	
Established Data Protection Authority which should be followed	AGENCIA ESPAÑOLA DE PROTECCION DATOS
Official national or international guidelines on protecting data privacy.	No
National laws or legislation for protecting patient's information.	PROTECTION DATA LAW
Access to health records and databases should be authorized by a legal authority.	No
Are patient data allowed abroad	No
Patient data collecting system used in your country	In Spain there is no National Health System Electronic records like in other countries. Spanish health service has management competencies and digital records highly decentralized and within a region there is a diversity of health records that fully comply with Data Protection Law.

Table 5: Data privacy and Ethical issues at Italian DS

	DS RER
National ethics controlling body.	Ethical Committee for Parma (Comitato Etico per Parma)
National ethics controlling body procedure.	<a href="http://www.ao.pr.it/comitatoetico/">http://www.ao.pr.it/comitatoetico/</a>
National legislation in application of AHA IoT practices in your country.	No
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	National Plan Crhonic diseases
Doctors who apply IoT in AHA practices should be authorized by a legal authority.	No
National legislation or law	Legislative Decree (Decreto Legislativo) 46/97 (transposes EU

	DS RER
direction for the applying of medical devices to the patients.	<p>general directive 93/42/CEE on Medical device class III, II and I), changes to Legislative Decree (Decreto Legislativo) 25/01/2010 n.37.</p> <p>Legislative Decree (Decreto Legislativo) 507/92 (transposes EU general directive 90/385/CEE on Medical device active implanted), changes to Legislative Decree (Decreto Legislativo) 25/01/2010 n.37.</p> <p>Legislative Decree (Decreto Legislativo) 332/00 (transposes EU general directive 98/79/CE relativa ai Medical - diagnostic in vitro device), changes to Legislative Decree (Decreto Legislativo) 25/01/2010 n. 37</p>
Ethics controlling committee for the organizations and hospitals who apply IoT practices.	If installation made following clinical trials, the clinical trials must be approved to Ethical Committee for Parma (Comitato Etico per Parma)
Established Data Protection Authority which should be followed	LHA guidelines privacy law in application to Legislative Decree (Decreto Legislativo) 30 Jun 2003, N. 196
Official national or international guidelines on protecting data privacy.	Legislative Decree (Decreto Legislativo) 30 Jun 2003, n. 196
National laws or legislation for protecting patient's information.	LHA guidelines privacy law in application to Legislative Decree (Decreto Legislativo) 30 Jun 2003, N. 196
Access to health records and databases should be authorized by a legal authority.	LHA guidelines privacy law in application to Legislative Decree (Decreto Legislativo) 30 Jun 2003, N. 196
Are patient data allowed abroad	YES; patient data are allowed abroad semi-identified
Patient data collecting system used in your country	network SOLE (servizio Sanità On LinE ) <a href="https://www.progetto-sole.it/pubblica/">https://www.progetto-sole.it/pubblica/</a>

Table 6: Data privacy and Ethical issues at UK DS

	DS UK
National ethics controlling body.	HRA - Health Research Authority, NHS England. White paper from Department of Health
National ethics controlling body procedure.	<a href="http://www.hra.nhs.uk/research-community/before-you-apply/">http://www.hra.nhs.uk/research-community/before-you-apply/</a> <a href="https://www.gov.uk/government/uploads/system/uploads/attach">https://www.gov.uk/government/uploads/system/uploads/attach</a>

	DS UK
	<a href="http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/139565/dh_4122427.pdf">ment_data/file/139565/dh_4122427.pdf</a>
National legislation in application of AHA IoT practices in your country.	There is no national legislation, but there is a coordinating body, IoTUK. Find them at <a href="http://www.iotuk.org.uk">www.iotuk.org.uk</a>
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	If concerning health then the same legislation as above applies <a href="http://www.hra.nhs.uk/research-community/before-you-apply/">http://www.hra.nhs.uk/research-community/before-you-apply/</a> <a href="https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/139565/dh_4122427.pdf">https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/139565/dh_4122427.pdf</a>
Doctors who apply IoT in AHA practices should be authorized by a legal authority.	If concerning health then the same legislation as above applies <a href="http://www.hra.nhs.uk/research-community/before-you-apply/">http://www.hra.nhs.uk/research-community/before-you-apply/</a> <a href="https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/139565/dh_4122427.pdf">https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/139565/dh_4122427.pdf</a>
National legislation or law direction for the applying of medical devices to the patients.	Medical devices are covered under the regulatory guidance for medical devices in the UK. There are different stages whether a device is CE marked yet or not, all information can be found on the <a href="http://www.gov.uk">www.gov.uk</a> website below <a href="https://www.gov.uk/government/collections/regulatory-guidance-for-medical-devices">https://www.gov.uk/government/collections/regulatory-guidance-for-medical-devices</a>
Ethics controlling committee for the organizations and hospitals who apply IoT practices.	No
Established Data Protection Authority which should be followed	The Information Commissioner's Office is an independent body providing guidance on data protection <a href="https://ico.org.uk/for-organisations/guide-to-data-protection/">https://ico.org.uk/for-organisations/guide-to-data-protection/</a>
Official national or international guidelines on protecting data privacy.	The Data Protection Act (1998) covers all data privacy in the UK. <a href="https://www.gov.uk/data-protection/the-data-protection-act">https://www.gov.uk/data-protection/the-data-protection-act</a>
National laws or legislation for protecting patient's information.	This would come under the Data Protection Act.
Access to health records and databases should be authorized by a legal authority.	This is covered under the Access to Health records Act, 1990 <a href="http://www.legislation.gov.uk/ukpga/1990/23/contents">http://www.legislation.gov.uk/ukpga/1990/23/contents</a> Also comes under the Data Protection Act, as above.
Are patient data allowed abroad	Data Protection Act (and GDPR from May 2018) allows for data sharing within the EEA, although it will still have to be mandated through agreements and mentioned explicitly in the PIA and signed off by the IAO (outside the EEA it'd have to fulfil a Data Protection Act Schedule 4 condition).

	DS UK
Patient data collecting system used in your country	EMIS ( <a href="https://www.emishealth.com/home/">https://www.emishealth.com/home/</a> ) and SystemOne - TPP ( <a href="https://www.tpp-uk.com/products/systemone">https://www.tpp-uk.com/products/systemone</a> )

Table 7: Data privacy and Ethical issues at Spanish (Valencia) DS

	DS VAL
National ethics controlling body.	AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (for data protection) AGENCIA ESPAÑOLA DEL MEDICAMENTO (for medical devices authorisation)
National ethics controlling body procedure.	There is a law about R&D projects but is centered in biomedical investigations: “Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.” and doesn’t apply for the Valencian DS.
National legislation in application of AHA IoT practices in your country.	No doctors participate in Valencia’s DS
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	No doctors participate in Valencia’s DS
Doctors who apply IoT in AHA practices should be authorized by a legal authority.	If a biomedical project with clinical research, yes: There is a law about R&D projects but is centered in biomedical investigations: “Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.”
National legislation or law direction for the applying of medical devices to the patients.	Doesn’t apply about hospitals. About Valencia DS there is the ACTIVAGE ETHICS BOARD.
Ethics controlling committee for the organizations and hospitals who apply IoT practices.	Ley Orgánica 15/1999 de Protección de Datos (LOPD) Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre
Established Data Protection Authority which should be followed	Ley Orgánica 15/1999 de Protección de Datos (LOPD) Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre
Official national or international guidelines on protecting data privacy.	Ley Orgánica 15/1999 de Protección de Datos (LOPD) Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre
National laws or legislation	Agencia Española de Protección de Datos

	DS VAL
for protecting patient's information.	
Access to health records and databases should be authorized by a legal authority.	No health records will be kept in Valencia's DS
Are patient data allowed abroad	No patients are involved in Valencia's DS and no access to health records are foreseen
Patient data collecting system used in your country	No patients are involved in Valencia's DS and no access to health records are foreseen

Table 8: Data privacy and Ethical issues at German DS

	DS WOQ
National ethics controlling body.	<p>No concrete national procedures defined for the focus group participating in the tests (People living in the planned rental homes will be mostly older retired adults who feel vulnerable; they pay for the rented flats).</p> <p>There is the Central Ethical Committee controlling adherence to ethical principles in medicine and frontier areas (Zentrale Ethikkommission zur Wahrung ethischer Grundsätze in der Medizin und ihren Grenzgebieten)</p> <p>The Ethical Committee of the German Society for Nursing Sciences (Ethikkommission DG-Pflegewissenschaft e.V.) was founded by the department of ethics and the board of the German Society for Nursing Sciences; a German-wide operating ethical committee. It aims to add to the spectrum of nursing sciences in the following areas: medicine, psychology, sociology, pedagogy, as well as other areas in science. The committee intends to watch over scientific nursing and health projects from an ethical standpoint, in cases when separate ethical committees do not have access to or whose incentives do not fit the usual proceedings.</p>
National ethics controlling body procedure.	<p>The Ethical Committee of the German Society for Nursing Sciences is joined by experts from ethics and research, they are to</p> <ul style="list-style-type: none"> <li>- review projects in the area of nursing sciences critically in terms of ethical guidelines</li> <li>- develop standards for ethical review</li> </ul> <p>In coordination with the department of ethics, the ethical committee does PR and counseling in order to draw attention to the topic. The committee also designs brochures and trains multipliers.</p>

	DS WOQ
National legislation in application of AHA IoT practices in your country.	<p>There is no National legislation in application of AHA IoT practices.</p> <p>With the universal health care law concerning supply structure passing, the assessment board of doctors and health insurances was appointed the tasks of defining which medical services can be done telemedically and how the register of medical services (EBM) is to be adjusted in consequence. This includes the charge for other services such as postage for letters containing medical documents to other practitioners. A framework agreement settled between superordinate organizations of the assessment board has made out the key points for the review of the EBM.</p> <p>A shared research paper concerning telecare is the aim of the Federal Association of Nursing Management. After the successful work group “IT in Care” in early summer this year, the work group “Telecare” was founded. With the research paper, information gaps are to be closed concerning care in telemedicine.</p>
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	No, since WQZ DS is not directly medical health related.
Doctors who apply IoT in AHA practices should be authorized by a legal authority.	<p>This is not relevant for the WOQUAZ DS since its services are not directly medical health related</p> <p>In Germany, permits for medical practice are granted by the German Medical Chamber (Ärztchammer); the additional offer is to be regulated by them as well. Telemedicine is to be an extra option, and not replace the patient-doctor relationship.</p>
National legislation or law direction for the applying of medical devices to the patients.	This is not relevant for the WQZ DS since its services are not planned with medical devices.
Ethics controlling committee for the organizations and hospitals who apply IoT practices.	This is not relevant for the WQZ DS since its services are not planned in hospitals.
Established Data Protection Authority which should be followed	Patient data is protected under strict privacy laws. In order to prevent projects being publicly funded which violate data protection regulations, the federal data protection officer should be informed.
Official national or international guidelines on protecting data privacy.	<p>In Germany, the Federal Data Protection Act regulates privacy protection; further, every Germany state (Land) has its own legislation.</p> <p>Above all, the European Data Privacy Act dictates the general direction.</p>

	DS WOQ
National laws or legislation for protecting patient's information.	The doctor-patient and client-lawyer confidentiality laws protect data; in Germany, there is an obligation of confidentiality for some professions: It prohibits them to share information with third parties (regulated within the Penal Code [§ 203 Strafgesetzbuch]). Furthermore, regulations of the "Fünftes Buch Sozialgesetzbuch (SGB 5) mentioned by GEMATIK should be considered ( <a href="https://dejure.org/gesetze/SGB_V/291b.html">https://dejure.org/gesetze/SGB_V/291b.html</a> ).
Access to health records and databases should be authorized by a legal authority.	These professions carry a lot of responsibility, since patient data is of a very personal nature and presents sensitive information. Adherence to confidentiality should be regulated and controlled.  Since in WQZ no access to health records are foreseen, this issue must not be considered.
Are patient data allowed abroad	No patients are involved in WQZ and no access to health records are foreseen
Patient data collecting system used in your country	No patients are involved in WQZ and no access to health records are foreseen.

Table 9: Data privacy and Ethical issues at Greek DS

	DS GRE
National ethics controlling body.	Regarding the IoT services of ACTIVAGE they do not require an approval from an Ethics Control Body. The National Bioethics Committee ( <a href="http://www.bioethics.gr/">http://www.bioethics.gr/</a> ) and the local Institutional Review Boards of Hospitals and Research Insitutions/Universities are dealing with experimental services.
National ethics controlling body procedure.	The providers of the IoT ACTIVAGE services in Greece in cooperation with the local technical partners will prepare a formal notification to the Hellenic (Greek) National Data Protection Authority.  The file of the notification can be submitted online: <a href="http://www.dpa.gr/portal/page?_pageid=33,19247&amp;_dad=portal&amp;_schema=PORTAL">http://www.dpa.gr/portal/page?_pageid=33,19247&amp;_dad=portal&amp;_schema=PORTAL</a>
National legislation in application of AHA IoT practices in your country.	No
Guidelines or legislation for the training of doctors who apply IoT in AHA practices.	No
Doctors who apply IoT in	Minimum conditions met for applying telemedicine (including

	DS GRE
AHA practices should be authorized by a legal authority.	IoT AHA services of ACTIVAGE Use Case 2 on integrated care) in Greece (Official Government Gazette- ΦΕΚ 150/27-6-11 , article 66, paragraph 16) .The specific article of the legislation, allows telemedicine, after written consent only (as in the case of a surgery , unless the case of an emergency). In addition, it make clear that telemedicine, has specific limitation in diagnosis, so it is an advisory –additional method, serving the clinical practice. The legislation allow telemedicine services to run in Greece, but sets special minimum regulations.
National legislation or law direction for the applying of medical devices to the patients.	All medical devices in Greece should have a CE/DOC certificate from a Notifying Body in accordance with the EU Directive on Medical Devices.  The respective Notifying Body in Greece is the “National Evaluation Center of Quality and Technology in Health” <a href="http://www.ekapty.gr/en/">http://www.ekapty.gr/en/</a>  The respective body is responsible to facilitate the application and implementation of the EU Medical Device Vigilance System in Greece in cooperation with the National Organisation of Medicines and Medical Devices <a href="http://www.eof.gr/web/guest/vigilance">http://www.eof.gr/web/guest/vigilance</a>
Ethics controlling committee for the organizations and hospitals who apply IoT practices.	Regarding the IoT services of ACTIVAGE they do not require an approval from an Ethics Control Body. The National Bioethics Committee ( <a href="http://www.bioethics.gr/">http://www.bioethics.gr/</a> ) and the local Institutional Review Boards of Hospitals and Research Institutions/ Universities are dealing with experimental services.
Established Data Protection Authority which should be followed	Some of IoT services of ACTIVAGE will require approval from the Hellenic (Greek) National Data Protection Authority <a href="http://www.dpa.gr/portal/page?_pageid=33,40911&amp;_dad=portal&amp;_schema=PORTAL">http://www.dpa.gr/portal/page?_pageid=33,40911&amp;_dad=portal&amp;_schema=PORTAL</a>
Official national or international guidelines on protecting data privacy.	The legislation that transfers in Greece the Data Protection Directive of the European Union :  Law 2472/1997 Protection of Individuals with regard to the Processing of Personal Data
National laws or legislation for protecting patient’s information.	The legislation that transfers in Greece the Data Protection Directive of the European Union includes special provisions for the protection of patient’s information.
Access to health records and databases should be authorized by a legal authority.	Although there is an exemption from the obligation to notify and receive a permit from the National Data Protection Authority when the processing involves medical data is carried out by doctors or other persons rendering medical service, provided that they are bound by medical confidentiality or other obligation of professional secrecy ( provided for in Law or code of practice, and data are neither transferred nor disclosed to third parties), the present

	DS GRE
	exemption does not apply to processing personal data within the framework of programs of telemedicine or provision of health care services via Internet. In that case, a special security plan has to be submitted to the National Data Protection Authority and a permit has to be received.
Are patient data allowed abroad	Yes Under the requirement of Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended) ,Article 9 "Transboundary flow of personal data"
Patient data collecting system used in your country	The regional Hospital Information System (HIS) and the National e-prescription system of Greece : <a href="https://www.e-prescription.gr/shs/portal/eprescription!/ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfljo8zijS1cTDwcLQx83EM9DAwcAwMCvByDg4wNvE31wwkpiAJKG-AAjgZA_VGEIBTkRhikOyoqAgCmSZaD/dz/d5/L0IDUmITUSEhL3dHa0FKRnNBLzROV3FpQSEhL2Vu/">https://www.e-prescription.gr/shs/portal/eprescription!/ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfljo8zijS1cTDwcLQx83EM9DAwcAwMCvByDg4wNvE31wwkpiAJKG-AAjgZA_VGEIBTkRhikOyoqAgCmSZaD/dz/d5/L0IDUmITUSEhL3dHa0FKRnNBLzROV3FpQSEhL2Vu/</a>

### 3.3.3 ACTIVAGE DS incentives schemes

Each DS will define the incentives appropriate for the participants to be recruited. Large number of participants is considered for the ACTIVAGE Large scale IoT pilots and ensuring participation and attendance at follow-up sessions is – in some occasions – critical for not only the success but the everyday running of pilots. It is a fine line between creating a culture of incentives when recruiting people and the ACTIVAGE PLG Board will oversee and approve (or not) the incentive schemes chosen by each pilot site, apart from the research protocol. Therefore, based on the evaluation plans (D9.1), appropriate incentives will be chosen. As commitment is essential for the success of the project, users will receive some form of reimbursement.

Participants should be informed of the presence/ absence of incentives when recruited and a statement needs to be added in the consent form; it will be part of the information sheet. In case of legal restrictions or policies, the ethics responsible at each pilot site should inform the PLG Board. An alternative to cash is using vouchers; sometimes it is easier for evaluation moderators to carry/use and they should be representative of the demographics (i.e. have an added value for older citizens).

It is upon the discretion of each partner to decide the incentive scheme to use (if not to use). Other options include sharing the results of the study, making charitable donations, creating a prize draw and offer non-monetary gifts.

### 3.3.4 Gender issues at DSs

Any potential gender issues are not foreseen as gender distribution and participation is anticipated to (and will be sought) be equally distributed due to the highly multidisciplinary teams representing diverse disciplines participating in the ACTIVAGE project (e.g. medicine, bioinformatics, psychology, and engineering). Gender equality is based on equal treatment and opportunities as defined by the European and UN Policies (e.g. Council Directive 75/117/EEC) and is adapted by the members of this consortium.

During the course of the project, equal gender participation is sought and maintained in all activities. Balanced gender distribution will be an objective during recruitment and will be recorded. Constant gender equality monitoring across the project is based on the following criteria:

- Equal opportunities and work conditions for both men and women;
- Equal access to employment;
- Equal pay;
- Equal opportunities to training and retirement;
- No discrimination.

## 3.4 ACTIVAGE Participants

### 3.4.1 Ethical concerns for the participants

The main **target user group of ACTIVAGE are older adults** (healthy or not) as well as patients, families and caregivers. In the Large Scale IoT Pilot (WP9) targeted in ACTIVAGE, the participants will have the competence to understand the informed consent information. In the unlikely case that they are unable to do so, no activity related to the project will be conducted. The protection of privacy rights will be ensured by the application of a number of best practice principles. These include the following:

Data will not be collected without the explicit informed consent of the individuals under observation. This involves being open with participants about what they are involving themselves in and ensuring that they have agreed fully to the procedures/research being undertaken by giving their explicit consent.

Data will not be collected will be sold or used for any purposes other than the current project.

A data minimization policy will be adopted at all levels of the project and will be supervised by each DS manager (one per each country involved and managed by the central PLG Board (T1.4) of the project). This will ensure that no data which is not strictly necessary to the completion of the current study will be collected. Data sharing with external parties will be defined in Data Management Plan (D1.4, Month 6).

Any shadow (ancillary) personal data obtained during the course of the pilots will be immediately cancelled. However, the plan is to minimize this kind of ancillary data as much as possible. Special attention will also be paid to complying with the Council of Europe's Recommendation R(87)15 on the processing of personal data for police purposes, Art.2.

The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law will be prohibited.

The collection of data concerning these factors may only be carried out -if absolutely necessary- for the purposes of a particular inquiry; however such data are out of scope for ACTIVAGE.

Compensation – if and when provided – will correspond to a simple reimbursement for working hours lost as a result of participating in the study; special attention will be paid to avoid any form of unfair inducement;

If employees of partner organisations, are to be recruited, specific measures will be in place in order to protect them from a breach of privacy/confidentiality and any potential discrimination. In particular, their names will not be made public and their participation will not be communicated to their managers. Identification details will be removed from raw data

collected and all participants will be collected. Any identification details will be held separately from data collected and only one authorized person will have access to them (i.e. they will be securely and safely stored).

In addition, any data or information that is disclosed or otherwise made available between ACTIVAGE Parties during the implementation of the Action or for any Exploitation activities (“Shared Information”), shall not include personal data as defined by Article 2, Section (a) of the Data Protection Directive (95/46/EEC) (hereinafter referred to as “Personal Data”). Accordingly, each Party agrees that it will take all necessary steps to ensure that all Personal Data is removed from the Shared Information, made illegible, or otherwise made inaccessible (i.e. de-identify) to the other Parties prior to providing the Shared Information to such other Parties.

Each Party who provides or otherwise make available to any other Party Shared Information will represent that:

1. It has the authority to disclose the Shared Information, which it provides to the Parties.
2. Where legally required and relevant, it has obtained appropriate informed consents from all the individuals involved, or from any other applicable institution, all in compliance with applicable regulations.
3. There is no restriction in place that would prevent any such other Party from using the Shared Information for the purpose of this Action and the exploitation thereof.

Considering the proposed approach and goals, there is no risk for users since all tests will be executed based on the informed consent of the participants involved. This consent will be obtained via a document outlining the elements of the participants’ participation in the project and its implications. Users will be warned that participation is not obligatory and the research can be abandoned at any time. In addition, approval from the local Ethics manger will be obtained before beginning the study. On the other hand, test data will be anonymised in order to prevent relating research results back to the performance or actions of specific individual participants. Thus, risks of violation of privacy based on the test data are minimal. Particularly, in fields trials the following specific issues should be considered:

### 3.4.2 Safety and well-being of participants

The users, informal carers and social and health care professional joining ACTIVAGE Large Scale IoT Pilot testing will be required to use electronic devices to validate the functionality. These devices are entirely safe and non-invasive, and will not cause any type of psychological or physical stress to the volunteer patient. It is NOT expected to record the experiments on video but to monitor and analyse their behaviour in order to improve the quality of care and of the developed applications. The consortium deems the safety risk to participants as extremely low due to their long experience with conducting user studies in various contexts of design and evaluation of interactive technology. The consortium will use the Code of Conduct of Usability Professionals (Usability Professionals Association, UPA <http://www.usabilityprofessionals.org>) which is the most established set of guidelines for conducting usability studies.

Necessary measures will be implemented to assure the security of the research and to reduce the risks and discomfort for the involved individuals. Medical decisions related to the health of the participants correspond to the responsible attending physician. The investigation should not delay or deprive participants of preventive medical procedures, diagnostic or therapeutic that may be necessary for their state of health. If the investigation results in information relevant to the health of the participants, e.g. for providing assistance or a specific advice, such information will be made available.

The main principles arising from these regulations are:

1. **Informed consent:** Informed consent is required for data collection, data storage, data processing and publication of raw or processed data. Before consent is sought, information must be given, specifying the alternatives, risks, and benefits for those involved, in a way users understand.
2. **Voluntary participation:** Participation is on a voluntary basis.
3. **Participation of disabled people:** It is essential that the consortium project team considers other issues of an ethical nature, such as the personal autonomy and integrity of the person and respect for rights and especially confidentiality aspects.
4. **Minimal risk:** Participants should not be exposed to more than minimal risk.
5. **Anonymity:** Volunteers have the right to remain anonymous. All data analyses are performed on an anonymous basis.
6. **Feedback:** Participants shall be provided with the possibility to retrieve feedback on the results of research.
7. **Privacy:** Researchers must ensure that the manner in which research outcomes are reported does not contravene the right to privacy and data protection.
8. **Confidentiality:** Confidentiality is different from the participant's right to privacy; it refers to how data about the participants will be stored.
9. **Data control:** The data subject has the right to access all data processed about him or her, and has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (art. 12 of Directive 95/46/EC)
10. **Informed stakeholders:** Informing stakeholders in detail on ethical aspects of research and evaluation/validation in reporting activities

### 3.4.3 DS participants' recruitment process & communication strategy

Before recruiting subjects for validation, the potential volunteers will be given a thorough explanation of the project and its possible benefits to their well-being, as well as the possible implications of being involved in such a project.

The ACTIVAGE pilots will involve existing habitants of selected districts in each of the selected Large Scale IoT Pilot along with volunteers wishing to participate in some of the envisioned pilot sites. All people that will be actively participating and/ or being affected by the execution of each of the Large Scale IoT Pilot use case, will take part in a thorough recruitment and informed consent procedure, that will be particularly stringent to ensure no coercion (not even soft or indirect) is exerted. The specific criteria for the selection of the volunteer participants will be determined by the pilot requirements, while there will be participants with various roles.

Furthermore, specific measures to protect the participants from a breach of privacy/confidentiality and potential discrimination will be applied, as it follows:

1. **Confidentiality:** The names of the employees participating in the pilots will be never revealed in any document and their participation will not be communicated to other pilot participants. As already stated above, all personal data stored during the pilots will completely and irreversibly anonymised and will be erased at the completion of the ACTIVAGE Project. As an absolute minimum anonymised process, data will not contain any of the following, or codes for the following:
  - Name, address, phone/fax number(s), e-mail address, full postcode.
  - Any identifying reference numbers, photographs, information about relatives.

2. **Right to get more information about the Large Scale IoT Pilot:** The pilot participants will be able to ask any questions about the pilots at any time throughout the pilot realisation phase. The corresponding pilot site responsible partner will be available to answer any questions, interests or concerns about the Large Scale IoT Pilot executions. During the pilot executions, each of the pilot participants will have the right to withdraw from the pilots at any time, without having to give any explanation and without being affected in any way.
3. **Informed Consent (see Appendix B):** A detailed informed consent will be carefully prepared for each pilot site, fully outlining the scope of the pilot and its purposes along with the data collected and analysed.

Communication with participants should abide with fundamental human rights principles. Participants should not feel coerced, threatened, stressed (resulting from investigator's behaviour). Researchers do not deceive by any means prospective participants about research that is reasonably expected to cause physical pain or severe emotional distress. Researchers explain any deception that is an integral feature of the design and conduct of an experiment to participants as early as feasible, preferably at the conclusion of their participation, but no later than at the conclusion of the data collection, and permit participants to withdraw their data (APA, 2002). No deception will take place within ACTIVAGE pilots and the user will be informed at all evaluation stages about the objectives and the procedures related to the pilots and how their data will be handled, processed, and stored.

Researchers provide a prompt opportunity for participants to obtain appropriate information about the nature, results and conclusions of the research, and they take reasonable steps to correct any misconceptions that participants may have of which the researchers are aware. Researchers also inform the participants about symptoms or diagnoses of diseases that have been discovered during the observation; especially if the symptoms have not discovered yet by a physician. Relevant test results will be provided to participants General Practitioner. The debriefing has to be documented and will be signed by both sides.

Summaries and copies of research reports will be given to research participants in appropriate accessible formats (e.g. larger font size, use of simple text accompanied by photographs, oral communication, etc.).

### 3.4.4 Informed consent

Researchers will obtain written (or oral) consent by participants prior any involving in user testing. An information sheet will accompany the consent form describing the main objectives of the project and of the evaluation to be carried out. The informed consent forms will first be approved by ACTIVAGE PLG Board and the local ethics committee's prior distribution to potential participants. They will be sent (or handed out) to participants a few days before the actual session or the testing period instantiates. Participants with cognitive impairment (if they are included) who can provide written (or oral) consent will only participate in the ACTIVAGE studies and evaluation sessions.

- The participants will have sufficient time to read and understand the aims of the project and the evaluations before they participate. They will be able to ask questions to the responsible person who's the contact details are included in the consent form document. The consent form will be written in a way that by no means states or implies that the moral or legal rights of the person are affected or not respected (see Appendix B) for the informed consent templates based on the information to be included bases on the WHO consent form templates).
- The information will be provided in **simple language** and **short sentences** in order to be understood by people with mild cognitive impairment and any jargon will be avoided. The consent form will be translated and distributed in the language of the country the pilot site

is conducted. After the approval of the template, its translated consent form will be used with a small group of participants to validate that the included information and the chosen form of presentation is appropriate and understood by the participants.

- Obtaining consent is a very important process, especially within the ACTIVAGE project, as users will participate for a long period of time and, therefore, consent is rather a process than just signing the consent form. In all cases, the person will decide if they want to participate or not. In case, **their condition deteriorates and they will no more be able to give consent, they will be withdrawn for the study**. Participants will be examined by their medical professionals in scheduled follow-ups, in the cases this is needed, to check their memory and functional level of activity and if they will continue to participate in the programme.
- The **procedure will be described in detail with all necessary steps** to be taken or completed by the participants accompanied by an estimation of the duration of the session or the whole participation in the study. The participant by no means should feel any discomfort or inconvenience and they will not be harmed or be put in risk during the evaluation process. These are fundamental ethical aspects to be followed by researchers in any type of contact with participants.
- The participant should be informed about the study aims and benefits for the specific user group. **If participants receive reimbursement or honoraria for their participation, then the amount/voucher. etc., should be relevant to the involved effort** and by no means should be perceived as a mechanism of coercion or expectations to be fulfilled by all participants.
- The **main investigator's/ researcher's contact details** will be included in the form in order the participant to be able to ask questions about the project and the study and receive answers. Medical related questions should be answered by the medical professional who collaborates with the pilot site and ethics or legal related questions will be answered by the ethics responsible at each site.
- The participant should be aware at all times that **their participation is volunteer and they can withdraw from the study any time they wish without any consequences to the care they receive** (i.e. users might also be patients in hospitals or care units, acting as pilot sites, therefore they might be hesitant to withdraw from the study believing that their provided care might be affected if they refuse to participate or if they wish to withdraw during the evaluation session or during the course of the longitudinal study). Thus, it is critical to ensure that their rights and care provision will not be affected.

The consent procedures will be carefully determined and managed by the Large scale IoT Pilot-specific tasks (WP9) that will manage the Large scale IoT Pilots which will be performed in selected DSs. Thus, it will require the enrolment of people voluntarily declaring their consent to participate in each of the pilot sites. However, the design of the Large scale IoT Pilots will be prepared in strict collaboration with the PLB Board of the ACTIVAGE consortium, in order to respect privacy and ethical issues implied by the data to be collected and analysed. In particular, the consortium will take the appropriate action for excluding that:

1. Data can be collected without the explicit informed consent of people under observation; no person unable to express a free and informed consent for age-related reasons, ongoing medical and / or psychological conditions, mental incapacity, will be enrolled in the study;
2. Data collected may be sold or used for any different purposes from the ACTIVAGE project;
3. Any data, which is not strictly necessary to accomplish the current study, will be collected; data minimisation policy will be adopted at any level of the project and will be supervised by the ethical/privacy component of the project.

4. Any shadow (ancillary) personal data obtained during the observation will be immediately cancelled. However, we plan to minimize as far as possible this kind ancillary data. Special attention will be also paid to comply with Council of Europe's Recommendation R (87)15 on the processing of personal data for police purposes, Art.2: "The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry". Some sessions between technical and ethical components of the project will be devoted to this.

Here we oppose the guidelines for seeking informed consent according to American Psychological Association (APA, 2002). APA guidelines refer to the information that should be made available to the participant when seeking informed consent:

- The purpose of the research, expected duration, and procedures;
- The possible risks, discomfort, adverse effects, and side effects (if any);
- A description of any benefits to the participant or to others which may reasonably be expected from the research;
- Explanations on confidentiality (and limits) of the data;
- Their right to decline to participate and to withdraw from the research once participation has begun and the foreseeable consequences of declining or withdrawing;
- Whom to contact for questions about the research and research participants rights.
- Appropriate insurance or indemnity to cover the participant in trial should be provided.

When appropriate, one or more of the following elements of information shall also be provided to each participant:

- A statement that the particular procedure may involve risks to the participant which are currently unforeseeable (not foreseen in ACTIVAGE project);
- Anticipated circumstances under which the participant's participation may be terminated by the investigator without regard to the participant's consent;
- The consequences of a participant's decision to withdraw from the research and procedures for orderly termination of participation by the participant;
- A statement that significant new findings developed during the course of the participation will be provided to the participant; and
- The approximate number of participants involved in the study.

### 3.4.5 Guidelines for recruitment & interviews with pilot users (with or without impairment)

The Interview and Recruitment Guidelines presented here are based on the Interview and Recruitment Guidelines by Manpower Inc.<sup>2</sup>. They are primarily aimed at employers, as an informative and above all practical guide to interviewing and recruiting people with disabilities but they are adapted to the needs of ACTIVAGE Large scale IoT Pilots.

<sup>2</sup> [http://sid.usal.es/docs/F8/FDO7146/interview\\_recruitment\\_guidelines.pdf](http://sid.usal.es/docs/F8/FDO7146/interview_recruitment_guidelines.pdf), originally addressing people with disabilities, also due to aging.

## Setting up pilot sessions

Expect the same measure of punctuality from elderly participants as from users without any health issues.

When setting up an evaluation session, consider the distance, weather conditions and physical obstacles that the participant may be presented with, and ensure that the participant is aware of how much time may be needed to arrive at the evaluation location.

Be aware that a participant may need to arrange to be picked up after the session has concluded - provide a good estimate of how long the session will last.

Elderly with visual difficulties: when giving directions, use very clear specifics including estimated distances where possible, for example, “turn right coming out of the lift and it’s about five metres to the office door.”

Familiarise the participant in advance with the names of all people that will be met during the visit.

Location: the proposed evaluation site/premise should be reviewed to ensure it is accessible and appropriate for carrying out tests/pilots with elderly with cognitive impairment and other health and mobility issues they might encounter. Some important things to consider are:

- Availability of parking spaces;
- Ready access to public transport systems;
- Step-free entrance;
- Lifts, where relevant;
- Clear signage on outside identifying the premises;
- Layout of session room. – does it interfere in any way with the mobility of the participant?

If any of these are inadequate and alterations cannot readily be made, inform the participant about them prior to the evaluation session and offer to arrange an alternative test/pilot site or room.

## Meeting and Greeting at sessions with participants

- Use a normal tone of voice when extending a welcome.
- Look and speak directly to the participant rather than to any companion, helper or carer that may be present and maintain eye contact with the participant.
- Offer assistance with dignity and respect and be prepared to accept instructions.
- Offer to hold or carry packages in a respectful manner.
- Do not offer to handle a cane (if the older person uses one) or the person unless requested.

## Conducting the Interview

- Do not ask questions that would not be asked to any other participant in similar circumstances, for example:
- Do not ask how anything about their diagnosis and condition.
- Avoid focusing on the cognitive impairment unless it is the only way to find out what adjustments are required.
- Eliminate any medical questions that are not strictly justified by the inherent requirements of the evaluation session and do not impose medical checks on participants with

cognitive impairment that would not be applied to participants without cognitive impairment.

- Ask what requirements may be needed to enable the person to carry out the session (f any) comfortably and be prepared to discuss how to cater for any difficulties that might be envisaged.
- Treat the person with the same respect you would treat any participant.
- Assume the participant is of normal intelligence.
- Always look and speak directly to the participant.
- Be willing to repeat questions and if not understood a second time, ask in another way.
- Show patience when speaking and listening.
- Do not pretend to understand if you are having difficulty doing so - do not be embarrassed to ask for clarification.
- Do not touch the person in overly familiar ways, unless you are familiar with them.

Common mistakes: openly admiring the participant's courage, expressing sympathy, staring or avoiding eye contact, avoiding essential questions, assuming help is needed, asking about their memory difficulties.

### **In General**

- Put the person first and cognitive impairment second.
- Do not make assumptions about the participant needs.
- Remember that some difficulties might be hidden.
- Talk to each participant about individual needs.
- Look into what help is available for the smooth organization and conduction of pilots.

## 3.4.6 Incidental findings (IFs)

Incidental finding are defined as the findings that maybe by-products or outcomes of the study that were not part of the main research questions and objectives but could be of importance for the physiological, psychological and mental wellbeing of the participant. Each DS will include different services during the Large scale IoT Pilots and for quite a long time, therefore, the number and type of incidental findings could be different for each site and valuable for both the person and the other stakeholder groups (e.g. carers or medical professionals). Until now there is no consensus in research about the path the researchers should follow in case of findings that are found during the course of the evaluation. In case of incidental findings, the research team will share this information with the participant according to the Council of Europe recommendation, in Article 27 of the Additional Protocol to the Convention on Human Rights and Biomedicine, Concerning Biomedical Research (Council of Europe, 2005).

A separate question will be included in the consent form about asking the participant if they wish to share any incidental findings with their physician and/or person who cares for them. If they agree to share any incidental findings with their doctor, then the doctor will be informed about these findings. In case, the participant refuses, they will be the only person informed about the findings and no one else. The person will be responsible with sharing this information with others or not. In this project, any incidental findings might be linked to possible deterioration in the future or the emergence of a co-morbid condition, therefore any accidental findings may prove to be very important for the person. However, the consortium strongly believes that the person is responsible for their own decisions, unless, of course,

they rapidly deteriorate during the lifetime of the project and a guardian is appointed to decide upon these findings. Wherever, a legal guardian is appointed, the participant can no longer participate in the study but there might be occasions where decisions should be taken for previously collected data (i.e. data gathered when the individual was still a participant in the study). **It is imperative, though, to clarify that there are several criteria set in the literature with no clear consensus** (Petrini & Alleva, 2013). However, there seems to be an agreement on the following two main criteria:

Any clinical incidental findings should be revealed for conditions that treatments exist. Researchers advocate that when treatment does not exist then sharing it with the participant will only make them feel stressed and helpless.

Avoid sharing/ revealing incidental findings that are not confirmed or seem dubious and not certain.

**An important note:** decisions should be made only by researchers/or affiliated professionals who have the skills and training to reach such decisions.

## 3.5 Delegation of control

Control delegation refers to two different dimensions within the Ethics Manual: (1) related to “the system” (here, AIoTES), and (2) related to the access to data.

The ACTIVAGE IoT Ecosystem Suite (AIoTES) will be continuously monitored and controlled to ensure smooth, reliable and efficient operation (system control). This will be made sure by the system security and privacy layer, developed in WP3.

The information provided and the services/ tools’ content will be accurate and appropriate for the target user groups (content control). These services/ tools aim to help and assist the end-users and not burden or frustrate them. Therefore, the content providers are responsible for creating and adjusting the content in order to be appropriate for the respective groups (e.g. content addressed to elderly users with cognitive impairments should be prepared based on cognitive accessibility guidelines<sup>3</sup>).

Ethically concerned, the Delegation of control will be ensured by the implementation of the Ethical design in the whole process, described in detail in Section 7.

---

<sup>3</sup> [https://www.w3.org/WAI/PF/cognitive-a11y tf/wiki/Main\\_Page](https://www.w3.org/WAI/PF/cognitive-a11y tf/wiki/Main_Page).

## 4 Legal aspects in ACTIVAGE

### 4.1 International and European instruments in the field of data protection

The “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data<sup>4</sup>” is the first European instrument in this field. It laid down the basic principles of a lawful data processing addressing the threats from the invasion of information systems, such as the data aggregation, at that time. In this respect, it concerns the automatic data processing, although the Member Countries could extend its applicability to non-automatic data processing. Art. 6 states that medical data may not be processed automatically unless domestic law provides appropriate safeguards. The Convention is of limited importance for EU countries after the enactment of the EC Directives on data protection.

The Charter of Fundamental Rights in the course independent authority of the respective legal trend dedicates a separate article to the protection of personal data. Article 8 sets out the right to the protection of personal data of an individual and thus the protection of personal data has now an own legal basis apart from the right to respect for an individual’s private life and the protection of the human dignity. Art. 8 of the Charter sets out the rules for the legitimate processing of personal data, notably that the processing shall be fair and for pre-specified purposes based on the consent of the data subject or other legitimate basis laid down by law. Reference is furthermore made to two rights of the data subject: the right of access to the data and the right to have it rectified. Finally, Article 8 sets out the need for guidelines which shall control the compliance with the data protection rules.

In 1999 the Council of Europe has adopted the Recommendation on the Guidelines for the protection of privacy in the information highways. These Guidelines may be incorporated in or annexed to codes of conduct of Internet service provider to obtain legal validity. The Recommendation is in line with the EC Data Protection Directives regarding the principles of the lawful data processing, the duties of the Internet service providers and the rights of the data subject. The Recommendation encompasses a series of detailed information what the users and service providers shall do to reduce the risks arising from the Internet. It is worth mentioned that the users are required to use digital signature and encryption techniques. On the other hand, the service providers are required to use certified privacy enhancing technologies, to ensure data confidentiality and integrity as well as logical and physical security of the network and the services provided over the network. The service providers shall also incorporate detailed privacy statements on the web-sites. Finally, the communication of sensitive data, for instance medical data, for marketing purposes requires the previous, informed and explicit consent of the data subject.

The OECD is actively participating in the issues regarding the data protection, the data protection on the Internet as well as the protection of consumer rights with regards to e-commerce. First, OECD issued Guidelines governing the protection of privacy stipulating the fundamental principles (OECD, 1980).

In 1998, OECD issued a Recommendation with regards to the implementation of the aforementioned Guidelines on global networks. The Recommendation addresses mainly commercial sites offering various goods and services, such as tourism, air travel ticket sales,

---

<sup>4</sup> Treaty No. 108 of the Council of Europe, available under [www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108).

finance, etc. It is not legally binding, unless the Internet service providers stipulate this explicitly. Although the Recommendation does not address healthcare applications, its provisions might apply as following:

The Recommendation imposes the obligation to the web-site provider to refer with a hyperlink to the national legislation on data protection and the national Data Protection Authority. Moreover, every Data Protection Authority should be present on the Internet through relevant, well-documented and interactive sites. The web-sites shall also maintain on-line private statements giving details on the kind of data collected, the purpose of, the use of the clickstream data and processing to which they are subject, as well as the opportunity to opt out. In case of on-line payments by cards they should configure their systems in such a way that they ask for the card details once, provided that they store this information in highly secure files on non-networked computers. Warning messages on the risks of the Internet shall be provided in case of processing of confidential data. For confidential data the highest degree of security shall be implemented. The implementation of privacy enhancing technologies is also required. Moreover, web-sites should formally state the acceptance of full responsibility for the security and confidentiality of the personal data collected and processed. With regards to data subjects rights the Recommendation highlights the right to access on-line the information collected and stored directly or indirectly, i.e. clickstreams or purchased profiles.

## 4.2 Relevant Legislation, Directives and Guidelines

According to Article 19: Ethical Principles the following encompasses the legal foundation for

*“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.”*

[http://ec.europa.eu/research/participants/data/ref/h2020/legal\\_basis/fp/h2020-eu-establact\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/fp/h2020-eu-establact_en.pdf)

Any arising ethics related issues are handled following the following principles:

- Helsinki Declaration of 1964 (revised version 2004)
- European Convention of Human Rights
- Rules of the Convention of the Council of Europe for the protection of individuals (automatic processing of personal data)
- European Directive 95/46/EC, for the protection of personal data
- Charter of fundamental human rights (Art. 8, 2000) about the personal right of each person to protect and access their personal data. Such data can be processed only after the person has given their consent and any related processes can be controlled by an independent authority.

Specific Laws and Directives to be considered per area are summarised in the Table below.

Table 10: Legislation, Directives and Guidelines considered by the ACTIVAGE PLG Board

Ethical & social issue	Ethical field	Law/directive
<b>Human Dignity and integrity of user</b>	<b>Human rights</b>	<ul style="list-style-type: none"> <li>– Universal Declaration of Human Rights (United Nations)</li> <li>– Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe)</li> </ul>

Ethical & social issue	Ethical field	Law/directive
		<ul style="list-style-type: none"> <li>– European Charter of Fundamental Rights</li> <li>– Draft recommendation of the Council of Europe on the promotion of the human rights of older persons</li> <li>– European Charter of the Rights of Older People in need of Long-term care and assistance</li> </ul>
Privacy	Data protection	<ul style="list-style-type: none"> <li>– Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)</li> <li>– Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA</li> <li>– Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the <b>retention of data generated or processed in connection with the provision of publicly available electronic communications services</b> or of public communications networks and amending Directive 2002/58/EC</li> <li>– Directive 2002/58/EC of the European Parliament and of the Council, concerning the <b>processing of personal data and the protection of privacy in the electronic communications sector</b></li> <li>– Take into account developments of <b>Reform of the legislative framework for personal data protection</b> (In January 2012, the European Commission proposed a reform of the Directive 95/46/CE, which constituted until now the basic instrument for personal data protection, in the form of a global Regulation on data protection 2012/001 (COD), supplemented by Directive 2012/0010 (COD) concerning the processing of personal in the area of police and judicial cooperation in criminal matters)</li> <li>– Art.29 <b>Data Protection Working party: Working Document on Privacy on the Internet</b></li> <li>– REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC</li> <li>– REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU</li> </ul>
Bioethics and clinical trials	Medical research	<ul style="list-style-type: none"> <li>– World Medical Association Declaration of Helsinki – <b>Ethical Principles for Medical Research</b> Involving Human Subjects</li> <li>– Opinion on the <b>processing of health data</b> by the Article 29 Data Protection Working Party</li> <li>– Universal Declaration on <b>Bioethics and Human Rights</b></li> </ul>

Ethical & social issue	Ethical field	Law/directive
		<ul style="list-style-type: none"> <li>– Directive 2001/20/EC on the approximation of the laws, regulations and administrative provisions of the Member States relating to the <b>implementation of good clinical practice in the conduct of clinical trials</b> on medicinal products for human use.</li> <li>– Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: <b>Convention on Human Rights and Biomedicine</b> (and Guide for Research Ethics Committee Members)</li> <li>– Charter for the <b>Rights of Older People in Clinical Trials</b> (<a href="http://www.predict.eu.org/PREDICT_Charter/predict_charter.html">http://www.predict.eu.org/PREDICT_Charter/predict_charter.html</a>)</li> <li>– Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to Active <b>Implantable Medical Devices</b> as amended by Directive 2007/47/EC of 5 September 2007</li> <li>– Council Directive 93/42/EEC of 14 June 1993 concerning Medical Devices as amended by Directive 2007/47/EC of 5 September 2007</li> <li>– Directive 98/79/EC on <b>In Vitro Diagnostic Medical Devices</b> as amended by Directive 2007/47/EC of 5 September 2007</li> <li>– Commission Regulation (EU) No 207/2012 of 9 March 2012 on <b>electronic instructions for use of medical devices</b></li> <li>– Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the <b>Community code relating to medicinal products for human use</b></li> </ul>
<b>Disability</b>	<b>Accessibility</b>	<ul style="list-style-type: none"> <li>– Disability Rights Commission: Guidelines for Ethical research (2004)</li> <li>– UN Convention on the Rights of Persons with Disabilities</li> <li>– Commission's proposal for a Directive on the accessibility of public sector bodies' websites</li> <li>– Accessibility Act</li> </ul>
<b>New Technologies</b>	<b>Liability and Safety</b>	<ul style="list-style-type: none"> <li>– Directive 85/374/EEC on <b>liability for defective products</b> as amended by Directive 1999/34/EC, hereinafter "the defective products Directive"</li> <li>– -Directive 2011/24/EU on the application of <b>patients' rights in cross-border healthcare</b></li> <li>– Directive 90/385/EEC on active implantable medical devices and Directive 93/42/EEC on medical devices and Directive 98/79/EC on in vitro diagnostic medical devices</li> <li>– -RoHS Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003, on the <b>restriction of the use of certain hazardous substances in electrical and electronic equipment</b></li> <li>– Directive 98/34/EC of the European Parliament and of the Council of 20 July 1998 amended by Directive 98/34/EC laying down a procedure for the <b>provision of information in the field of technical standards and regulations and of rules on information society services</b></li> </ul>

In addition to the aforementioned specific Laws and Directives, each DS should take also into account National legislation or local guidelines as these have been presented in Section 3.3.2.

## 4.3 GDPR legislation

According to the EU, “The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years”. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and its scope is to harmonize data privacy laws across Europe, to protect and empower all EU citizens’ data privacy and to reshape the way organizations across the region approach data privacy.

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. The European Parliament’s Civil Liberties committee and the Permanent Representatives Committee (Coreper) of the Council then approved the agreements with very large majorities. So, 4 years after debated and discussions, the GDPR was approved by the EU Parliament on 14 April 2016, as a major step forward in the implementation of the Digital Single Market Strategy. On the 4<sup>th</sup> of May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the Regulation will enter into force on 24 May 2016, 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.

GDPR Regulation aims to support the privacy rights, by arriving as a centrepiece of the EU Digital Single Market Directive, an initiative designed to boost digital innovation within the EU. By harmonizing privacy legislation across the EU member states and carving out exemptions for scientific, historical and health research, the GDPR seeks to reconcile the often competing values of privacy and innovation.

GDPR gives research many privileged, since organizations that process personal data for research purposes may avoid restrictions on secondary processing and on processing sensitive categories of data (Article 6(4); Recital 50). These organizations should implement appropriate safeguards, and they may override a data subject’s right to object to processing and to seek the erasure of personal data (Article 89). Additionally, the GDPR may permit organizations to process personal data for research purposes without the data subject’s consent (Article 6(1) (f); Recitals 47, 157). The GDPR clearly intends to relax restrictions on further processing personal data for research purposes. In isolated cases, research organizations may be able to transfer personal data to third countries for research purposes, without any other transfer mechanism in place (Article 49(h); Recital 113).

Additionally, GDPR treats public health research as a subset of scientific research (see Recital 159). GDPR also contains several provisions applicable exclusively to public health research. For example Article 49 permits the transfer of personal data to third countries that do not offer an adequate level of protection if “the transfer is necessary for important reasons of public interest,” which may include public health research. Recital 112 explains that this derogation applies especially “for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport”. Article 36 requires controllers to consult with a supervisory authority prior to processing that may result in a “high risk” to data subject rights. Even in the absence of a high risk, however, “Member State law may require controllers to consult with, and obtain prior authorization from, the supervisory authority.”

### 4.3.1 GDPR Strengths and Challenges

One of the core points of GDPR is its Enforcement process. There is more a debate rather than a consensus between experts about the enforcement process of the GDPR. So it may be characterised both as a lowlight and a highlight of the Regulation.

There appears to be a consensus on the fact that the use of personal data nowadays requires a higher level of diligence than it did in the past. When at the 1995 EU Data Protection Directive was created, each Member State was required to transpose that instrument into its own national law. What transpired were some fairly stark differences in the way each state regulates and enforces data protection. At one level this is a hugely confusing situation both for business and for consumers. Launching the GDPR, the European Commission intended to create a 'One Stop Shop' mechanism that would allow companies to 'simplify' their dealings with data protection regulators by only needing to interact with a single Data Protection Authority (DPA).

Widespread concern was expressed that this DPA arrangement would work against the interests of citizens and in favour of large entities. Thus, the GDPR now specifies a 'lead' Authority for investigations, but it also allows intervention by other 'concerned' regulators. This mechanism could potentially act as a brake on DPAs that are unwilling to take assertive action and it could also provide support for DPAs that are under-resourced. Importantly, these intervening DPAs can refer a decision by the lead Authority to the newly created European Data Protection Board (EDPB).

Even if each nation has its own DPA, there is little consistency in the powers, functions and limitations of each one, and what binds them is a set of principles (proportionality, fairness etc.). Additionally, the decades of legal evolution of each nation drives to the development of 28 national regulators with wildly different approaches to data protection enforcement. This divergence applies not just in law, but also to the operational issues of each DPA. For example, Germany and the Scandinavian and Nordic countries enjoy a wide degree of power and autonomy while Ireland has built a more relaxed business-facing culture. This flexibility for Member States to set their own rules is reflected throughout the entirety of the data protection spectrum. In each case, individual states may decide for themselves the rules that will apply to the processing and transfer of data (Covington & Burling, 2016). Additionally, the new regulation may have conflicts with other non-European laws and regulations and practices (e.g. surveillance by governments) and companies in such countries should no longer be considered acceptable for processing EU personal data (see EU-US Privacy Shield, [https://en.wikipedia.org/wiki/EU-US\\_Privacy\\_Shield](https://en.wikipedia.org/wiki/EU-US_Privacy_Shield)).

Thus, the implementation of the GDPR in practice will require comprehensive changes to business practices for companies that had not implemented a comparable level of privacy before the regulation entered into force. Additionally, since there is already a lack of privacy experts and knowledge as of today and new requirements might worsen the situation. Therefore education in data protection and privacy will be a critical factor for the success of the GDPR. Nonetheless, the European Commission and DPAs have to provide sufficient resources and power to enforce the implementation and a unique level of data protection has to be agreed upon by all European DPAs since a different interpretation of the regulation might still lead to different levels of privacy. Finally, consideration has to be given to the fact that Europe's international trade policy is not yet in line with the GDPR ([Irion et al., 2016](#))

Another important fact in GDPR is the principle of the Right to be forgotten. In practice, this means that data would have to be deleted entirely from the controller's system if the controller has made the information public and would have to ensure the erasure of links to this information too. This right can be applied when data are no longer necessary for the purpose for which they were collected or processed, if the individual withdraws consent to processing (and if there is no other justification for processing), when the data are otherwise

unlawfully processed or when the data have to be erased to comply with Union or Member State law which applies to the controller. The principle of “the right to be forgotten” has been enshrined, though there is still some argue from some that this right is poorly conceived in the GDPR.

The new GDPR recognised the importance of giving consent, which over the past several decades fell victim bad practice. The absence of definition and clarity has resulted in a regime of ‘implied’ consent that compromised the very basis of data protection. The Regulation establishes a more robust framework to better ensure that consent in most cases must be explicit. One risk, of course, is that the mechanism to ensure consent could end up similar to the much-lambasted EU cookie notice policy. As with the Directive, the GDPR stipulates that consent should be ‘freely given,’ and may not be coerced, for instance by making consent for non-essential processing a precondition to entering into an agreement, or where there is a clear imbalance between the controller and the data subject.

Finally, GDPR will bring more legal certainty and coherence than today, where 28 different legal systems as well as 28 different judicial and enforcement cultures define the regulatory environment. In times where merely no company can afford to not be present in the digital sphere and use services of Internet companies from all around the world this creates massive bureaucracy and legal uncertainty. The change to a single legal framework including a level playing field for all companies on the European market is extremely positive for both businesses and consumers.

Last but not least, GDPR makes it is possible, at least in theory, for regulators to penalise an organisation up to €20 million or 4% of its annual turnover, whichever is the greater in case of non-compliance. For a serial offender such as Google 3 this could mean risking a fine of up to €3 billion. It is, however, debatable whether some DPAs will ever impose such penalties. The UK Information Commissioner’s Office (ICO), for example, was given authority several years ago to impose fines of up to half a million pounds but it chose instead to pursue a ‘light regulatory touch’ with offenders.

# 5 ACTIVAGE Data privacy policy

## 5.1 Introduction

As it has been described in Section 2, privacy risks in the Internet is increasing and the respect of privacy which secures, inter alia, the personal private sphere against unjustified interventions is of critical concern in ACTIVAGE project. In the current Deliverable we will delineate the basic lines for the data privacy policy of ACTIVAGE. This policy will be then detailed in the context of D1.4 Data Management Plan (M6), where the Management of Data, Knowledge & IPR issues will be explained in detail, and a coherent strategy will be developed.

## 5.2 Confidentiality and data protection

Participants, and the data retrieved from them (e.g. performance or subjective responses) must be kept anonymous unless they give their full consent to do otherwise. However, the following guidelines should be followed by DS carrying tests with end-users:

1. Identifiable personal information should be encrypted (i.e. anonymization and coding). Otherwise ethical approval is necessary specifically for this.
2. Anonymization is preserved by consistently coding participants with unique identification codes. Only one person at each pilot site will have access to personal identifiers (if any).
3. A Participant ID will be issued for each of the participants, whereas the pilot site person that will collect and issue them will not have participated in the evaluation and will have not come into contact with the test participants and their performance in the tests.
4. Each individual entrusted with personal information is personally responsible for their decisions about disclosing it.
5. Pilot site managers must take personal responsibility for ensuring that training procedures, supervision, and data security arrangements are sufficient to prevent unauthorised breaches of confidentiality.

The participants should also be informed as quickly as possible when their data are accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons. The recent revision of the e-Privacy Directive introduced a mandatory personal data breach notification covering, only the telecommunications sector. Given that risks of data breaches also exist elsewhere (e.g. the healthcare sector), the obligation to notify personal data breaches should be extended to other sectors. A consistent and coherent approach on this matter will have to be ensured even when the organisation breaching the confidentiality is not based within the EU.

Finally, we need to keep in mind that any person should have a so-called 'right to be forgotten', which means that the data subject should have the right to ensure that their personal data will be deleted and no longer processed, where they have withdrawn their consent for processing or where they object to the processing of personal data concerning them. The European Commission has also proposed complementing the rights of participants by ensuring 'data portability', i.e. providing the explicit right for an individual to withdraw his/her own data (e.g. his/ her photos or a list of friends) from an application or service so that the withdrawn data can be transferred to another application or service, as far as technically feasible, without hindrance from the data controllers.

## 5.3 Coding anonymized data and storing

Information should be anonymised so that individual identities cannot be revealed. Anonymization provides a safeguard against accidental or mischievous release of confidential information. There are different ways in which personal data can be modified to conceal identities:

*Coded information* contains information which could readily identify people, but their identity is concealed by coding. The key to which is held by members of the research team using the information.

*Anonymised data* with links to personal information is anonymised to the research team that holds it, but contains coded information which could be used to identify people. The key to the code might be held by the custodians of a larger research database.

*Unlinked anonymised data* contains nothing that has reasonable potential to be used by anyone to identify individuals. Combinations of all demographic data that might lead to identification of individuals or small groups will be avoided (e.g. age, gender, nationality, occupational and Socio-Economic Status (SES), diagnosis, address, other contact details). In cases of in-depth qualitative data collection (e.g. ethnographic observations, interviews) with increased complexity of data collection, potential links in data identification will be judged on a case-by-case basis and it will be taken into serious consideration for ethics approval.

Any databases including participants' details will not be maintained after the end of the project, unless participants state so (i.e. in many occasions participants inform researchers that they would like to participate in other studies). In such cases, participants provide written consent of their willingness to share their personal details. The latter also depends heavily on national laws and guidelines.

For the statistical analysis, the answers provided by the participants will be associated with their user group membership (if any) or age, gender etc. However, each month, and during the project, the anonymised data will be re-sorted randomly, to mix participants' order. Data handling will be carried out only for anonymised datasets and will be aggregated and consolidated by the partner who shall consolidate and analyse data.

Different templates will be prepared for data gathering based on data type. Additional testing materials related to data gathering will be used such as meta-data template (i.e. a template describing briefly the data types collected at each site and any related data that describe and present the procedure). Meta-data templates facilitate analysts to understand the procedures and the nature of tests conducted at each site. This proves very helpful and efficient in cases the analyst is not the test responsible or is not a member of the test conduction team.

Separate common templates will be created for each instrument and technique applied. For example, interviews with open-ended questions will be transcribed under main themes topics for further content analysis and questionnaires could be available in electronic forms.

Participants will be informed about ACTIVAGE data privacy protection policy and relevant policies (Chapter 4: Legal aspects in ACTIVAGE). As databases are developed, confidentiality will become increasingly hard to maintain. Simple stripping of the participants name and its replacement with a code is no guarantee of complete confidentiality. The ACTIVAGE PLG Board will especially scrutinise the information pre-processing within databases. Within ACTIVAGE the participant will be informed about the sharing of their data, even, if only anonymised data is being shared. There are solutions to the challenge of maintaining confidentiality including substituting numerical identifiers for names, aggregating data so that the performance of individuals is not obtainable, encryption or layering data so

that researchers who need identifying information can obtain it only after signing a legal document that requires honouring the confidentiality of individuals.

## 5.4 Privacy of ACTIVAGE system

ACTIVAGE system provides services to elderly user with cognitive impairments in order to protect their health and personalise its services. However, it performs it with due respect, as:

- All required user profile data will be stored at his/ her profile and be securely protected by relevant WP3 mechanism. Relevant preferences relate to his/her physical activities, transportation modes, social networking, and, in general, simple everyday task preferences.
- When the system realises a potential deviation from user's planned actions (i.e. not following or not performing the proper exercises, deviating from his/her route), feedback will be strictly given to the user him/herself and not to the relatives or other persons (in a discrete mode). Only in case of medical emergency recognised or risk of getting lost (for people with significant cognitive problems; diagnosed condition) will the system inform his/ her carer.
- The user's location and route will be only temporarily stored (i.e. during a trip), in order to assist the user in case he/she is lost and train the system on his/her preferences and will be automatically deleted afterwards, unless the user wishes to store it.
- The user will have the capacity to view, change or delete, as he/she wishes, all stored data by the system (including his/her profile data), with the help of a very simple and multimodal interaction (touch, buttons and voice input supported).
- The user will be able him/herself to provide selected data access to third parties (i.e. his/ her children), so that they can monitor his/her health or diet, if in this way he/she feels safer (but will require the user to specifically configure the system to do so). Default is a closed system, unless otherwise by medical prescription.
- All ACTIVAGE use existing on the market sensors (no new sensors developed) and do not use any intuitive sensor (i.e. video camera) on the user but only for security functions.

# 6 Ethical Risk assessment and mitigation strategy in ACTIVAGE

## 6.1 Risk assessment strategy

It is a well-accepted paradigm that there is nothing in life without risk. Although, life or wellbeing risks are not anticipated during the evaluations within the ACTIVAGE project, any indirect effect should be considered mainly because testing involves patients and because carrying out tests for long periods of time increases the probability a person to encounter a risk regardless if it is related to the ACTIVAGE services or not. Two risk assessment and mitigation processes will be realised within the lifetime of the project. Firstly, the Ethics Board and the local ethics committees will closely evaluate any potential risks and ensure that no undue risk is present for the user. The second is a specific mitigation strategy set and presented in the ethics manual that is related to specific risks that might appear and how they should be handled. This process involves all evaluation involved personnel and not only the ethics committee members and responsible people. The nature of risk is very much related to how the risk is perceived by the user and which strategies can be employed to rectify or even avoid a negative outcome. Any risks are discussed and presented in the consent form and the prospective participant can ask any related questions. There are 4 primary risks:

- No **physical damage** is anticipated because of participation in ACTIVAGE pilots. However, the person may suffer any other type of physical damage during the pilots not related to testing (e.g. falls monitored by the Fall Detection module).
- No major **psychological stress** or anxiety is anticipated to be experienced because of participation to the pilots. Nonetheless, older people with cognitive impairment often feel anxious because they realise the limitations in their activities that were not present before. The investigators will work in close collaboration with the healthcare professionals on how to communicate with the participants.
- **Social inconveniences** and effects will be minimised (e.g. additional travelling costs are reimbursed for the participant and their carer).
- **Privacy** is secured under the anonymity and confidentiality principles and participants will be informed about this before they sign the consent form.

## 6.2 Ethical Risks in ACTIVAGE

Next table summarizes some initial ethical risks related to ACTIVAGE activities. Within WP1, such risks will be further elaborated prior the execution of the large-scale pilots and results will be included in the corresponding reports of WP1.

Table 11 : Considerations regarding ACTIVAGE Ethics Risk Management

Ethical and Social risks	Description	Ethics Risk Management in ACTIVAGE
Loss of Privacy Control	Storage and process of personal and individual sensitive data	For the data collection privacy-preserving sensors will be utilized (e.g. no cameras will

Ethical and Social risks	Description	Ethics Risk Management in ACTIVAGE
	<p>Confidentiality</p> <p>Measurements from various sensors will be transmitted wirelessly (e.g. based on the IoT ecosystem foreseen in ACTIVAGE)</p>	<p>be used at any stage of the demonstrations).</p> <p>Any original (raw) data will be destroyed after that, if this is not forbidden by law of the country in which the information was collected, stored and analysed. Special measures will be undertaken to ensure data anonymization and data access control (e.g. access only by authorized persons).</p> <p>Moreover, core partners involved in Pilots, have the expertise and the know-how from similar past and ongoing collaborative projects, towards providing the necessary ethical guidelines that should be adopted during the execution of the Pilots. Local ethical committee (and the National committee, if needed) will be informed towards getting an official permission for the execution of the selected Pilots.</p>
Data Security	<p>Difficulty in ensuring the security of shared personal health data.</p>	<p>Special attention will be given to ensure confidentiality and for incorporating Privacy Enhancing Technologies (PETs) to ensure protection from data breaches. Consortium partners involved in Demonstrations have the capacity and the experience to cope with the delivery of security mechanisms, based on highest possible data security standards.</p>
Accessibility	<p>Third parties interest in access to electronically recorded and stored personal health data.</p> <p>Participant/patient own access to his medical record.</p>	<p>Data protection measures will be taken for each Pilot, respecting both National and European legislation. Limited storage of medical records coupled with state-of-the-art encryption techniques will reduce risks related to accessibility of medical data by third parties.</p>
Transparency	<p>Possible lack of transparency:</p> <p>Analysis of health data and respective outcome.</p> <p>Work of healthcare professionals.</p>	<p>An current ethics manual (WP1) will be delivered for the pilots towards all activities performed to be in compliance with National and European legislation. Prior the execution of the pilots the local ethical committees will be informed for the data collection as part of the ACTIVAGE demonstrators and the necessary documents will be created by the consortium in order to get an ethical approval.</p> <p>Moreover, an informed consent will be provided to all participants (given in a clear and comprehensive language) and countermeasures will be taken for public trust in the new technologies to be introduced during the project lifetime (e.g. openness about uncertainties and knowledge gaps)</p>
Medical Data	<p>Physiological/ Behavioural measurements, respective profiles</p>	<p>As already mentioned above, PET technologies will be used in the pilots to ensure confidentiality and authorized access</p>

Ethical and Social risks	Description	Ethics Risk Management in ACTIVAGE
	<p>creation and pathological findings Need to notify proper trial authorities</p>	<p>to medical data. Moreover, all the pilots will be performed according to National &amp; European legislation and relevant data protection authorities will be informed on time.</p>
New technologies & IoT-related equipment	<p>Existing monitoring infrastructure in the foreseen DSs Additional sensor installations needed to validate the new business models of ACTIVAGE</p>	<p>The consortium partners have the expertise to make the appropriate installation for the purposes of the pilots, in which only common and certified technologies will be used. Moreover, most of the partners have participated in several National and European projects related to integration of sensors for demonstration purposes and their use in ethical compliance with National and European legislations.</p>
Safety	<p>Pilot testing should not entail any undue risk for participants</p>	<p>Guidelines for user involvement have been provided in the Ethics and Privacy Protection manual (WP1, D1.5, Section 3.4 ACTIVAGE Participants). Testing of technologies will be always supervised by the DS Responsible team.</p>
Users' engagement	<p>Demonstration actions have to be inclusive and representative of various user groups. The selection and recruitment of users is a crucial part of the user involvement process, as it will impact on the quality of the outcomes and the sustainability of the research or policymaking process. A satisfactory number and combination of user characteristics is sought; gender balance and equality should be addressed.</p>	<p>ACTIVAGE will target older adults in the large sense (more than 7000 users will participate in the demonstrations). The substantial number of users will ensure a wide pilot perspective, including: i) different countries, ii) different age groups, iii) various levels of cognitive decline, iv) various social backgrounds, v) different living arrangements (living alone, with spouses, with family, living at care homes etc.) and vi) gender balance. PLG Board will oversee the selection of users. The Ethics and Privacy Protection Manual (D1.5) has addressed the issue of user involvement in practice (Chapter 3.4 ACTIVAGE Participants), ranging from guiding principles to how to engage older adults (patients or not) in DSs. The annual project reporting will be the occasion to evaluate the user involvement process.</p>
Accountability	<p>The accountability of the IoT applications regarding users' privacy. (Who is going to be legally accountable for the user's data? Are PET producers responsible for privacy breaches or the application where the PET is applied? Or the users themselves?)</p>	<p>ACTIVAGE Data Management Plan (D1.4), as well as the Large Scale IoT Pilot plans described in D9.1 will identify who will be responsible for the accountability of the data in which AIoT layer.</p>
Digital divide	<p>Users have different set of capabilities in accessing the IoT devices and applications. Depending on their level of technical</p>	<p>Introducing the user centre design from the beginning of the development of AIoT, as well as having a security interoperability layer minimised as much as possible the digital</p>

Ethical and Social risks	Description	Ethics Risk Management in ACTIVAGE
	<p>proficiency, users have different levels of perceptions of the privacy risks or different understanding of the requests sent to them through the IoT.</p>	<p>divide that occurs from the usage of IoT.</p>
<p>Conformance to regulatory frameworks</p>	<p>The definition, implementation and conformance to regulations in the context of ACTIVAGE can be hampered by two factors:</p> <ol style="list-style-type: none"> <li>1. The speed of the evolution of the IoT can be faster than the regulatory process itself, so that regulations can be moderately effective when they are enforced;</li> <li>2. The regulatory framework to evolve may be extremely broad due to the participation of many different countries in the Large Scale IoT pilots.</li> </ol>	<p>All the possible Legislation, Directives and Guidelines that have to be considered by the ACTIVAGE PLG Board are presented in Table 10: Legislation, Directives and Guidelines considered by the ACTIVAGE PLG Board. Additionally all the local legislation available in each DS has been captured and depicted in the Tables of Section 3.3.2.</p>

# 7 ACTIVAGE Ethical Design Model

## 7.1 Security and identity management

The security IT system should ensure that all personal data against any potential threats of unauthorised access or disclosure risks as defined by the OEAD – Security Safeguard Principle (<http://oe.cd/2002sg>) (Section 4.1). Any security related threats or issues should be handled on a network area level and a cloud-based level. Security is an integral part of Information Technologies (IT) and especially in ACTIVAGE more advanced security measures and protocols should be applied as its system design is based on a cloud-based infrastructure with all services integrated as modules. Therefore, security of data transmission, transferring, and sharing – whilst protecting the identity of the person the data belongs to and simultaneously maintaining and managing a system of high **confidentiality, integrity, quality** and **efficiency** – is of core importance for safeguarding the security and identity protection principles. Limiting access to certain personnel enhances security and data integrity. Data should be accessed and modified only by authorised personnel (in most cases by the principal site investigator). Although, most information and data will be stored on cloud service(s), consideration should be made about the security and threats of pcs and applications used to access these data. Information flow should be monitored and controlled to be able to control for security bridges and rectify in case of security breach. In addition, data should be stored in a secure area with increased security protocols and firewall protection. Data should be regularly checked for quality (e.g. corruptions because system failures, crashes, malicious acts, accidental losses or alterations) either with automated tools or manually by the administrator. Data privacy, availability and auditing should be ensured in a way that will not affect the system's performance. In other words, any applied protocols should be flexible and viable for the system and its users. By system we mean the final cloud-based ACTIVAGE system with all integrated modules. Making the ACTIVAGE system secure entails the following technical security requirements.

- **Physical integrity:** the system is protected by physical failures (e.g. power).
- **Logical integrity:** robust databases where erroneous or required modifications do not alter the structure and connections of fields.
- **Element integrity:** accuracy of added data.
- **Control of access:** levels of authorised entry to the system based on access levels (e.g. the principal investigator may have access to personal data and a data analyst will have only access to the database with anonymised and not-identifiable-data).
- **User authentication:** Very related to the access control (just above) and access is given with registered credentials provided (and sometimes controlled) by the administrator. Permission is granted to certain registered users.
- **System availability:** uninterrupted data flow for authorised users whenever a request is send.
- **Auditability:** record activity and access details (who, when, which data, duration of session, and data transferring (if any)).
- **Application of security policies and standards:** setting the requirements for document encryption, use of digital signatures, setting security protocols (like SAP) to ensure secure communication channels, use personal anti-virus software and personal firewalls and encryption mechanisms for data storing and communicating (e.g. sending via email protocols).

## 7.2 Ethical design and SecKit

### 7.2.1 Introduction to SecKit

SecKit (Neisse et al, 2015) is a Model-based Security Toolkit for the Internet of Things which is integrated in a management framework for IoT devices, and supports specification and efficient evaluation of security policies to enable the protection of user data.

Policy Decision Point (PDP) and Policy Enforcement Point (PEP) are the main policy enforcement components of the toolkit. The toolkit principal workflow which is also depicted in Figure 8 below is the following: the PDP component receives event notifications from the PEP component and evaluates the security policies integrated within its sub-modules. In response to the fired events, the PDP replies to the PEP with a preventive enforcement message for tentative events or a reactive enforcement message to the Behaviour Executor for actual events. PEPs are embedded in the IoT system using standard techniques such as custom libraries or runtime instrumentation. It's worth mentioning that PDP can also use dynamic policy configuration templates by deciding to deploy additional security policy rules in response to changes in the context or system events.

The PDP and PEP components of the toolkit are deployed and activated in the IoT devices either as part of the IoT device platform design, as part of the IoT application design, or as an add-on embedded transparently in the application or platform at runtime.

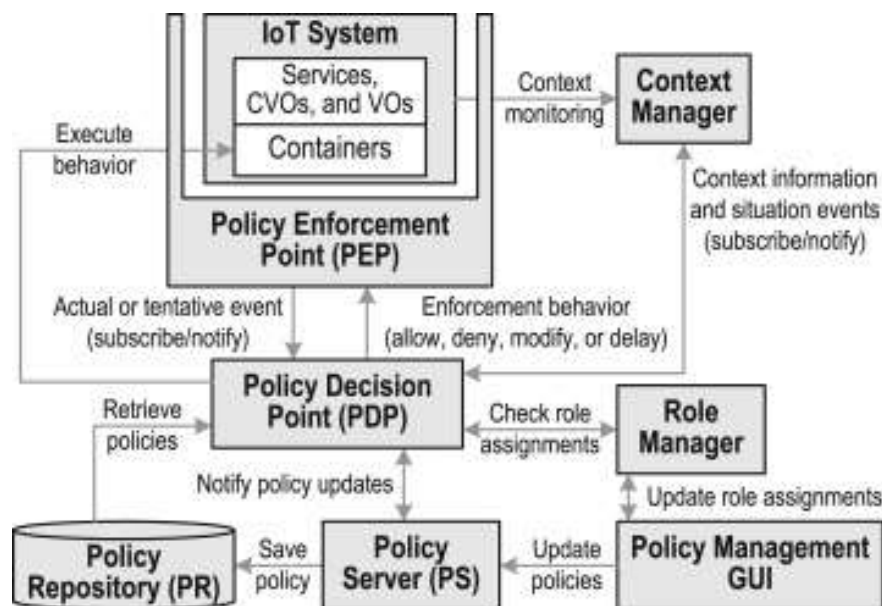


Figure 8: SecKit architecture depicting enforcement components

SecKit Toolkit has been designed to tackle with research challenges such as:

1. How to ensure that user needs for security and privacy are validated in the evolution of internet towards IoT, and
2. How trust relationships can be established and managed between the IoT technology and the individuals who use such technology.

### 7.2.2 Main usages and implementations

The toolkit has several usages and implementations; some of them are outlined below:

1. Dedicated Drupal module for improving the security of web applications powered by Drupal; some code snippets from the module are listed below.
2. Integration with the MQ Telemetry Transport (MQTT) Protocol layer so as to enforce security policy rules (Neisse, Steri & Baldini, 2014).
3. Distributed Internet-like Architecture for Things (DIAT) (Sarkar et al., 2015).
4. Agent-based design (Neisse, 2015) for Informed Consent in IoT, where access to personal data is regulated through usage control policies.

The code implementation as regards the SecKit dedicated Drupal module is available in <https://github.com/p0deje/seckit> and some example security functions in PHP can be found below:

#### a. Report of CSP violation to watchdog

```
function _seckit_csp_report() {
    // we should only allow POST data with application/json content type
    $method = $_SERVER['REQUEST_METHOD'];
    $json_type = strstr($_SERVER['CONTENT_TYPE'], 'application/json');
    $length = $_SERVER['CONTENT_LENGTH'];
    if (($method == 'POST') && ($json_type) && ($length > 0)) {
        // get and parse report
        $reports = file_get_contents('php://input');
        $reports = json_decode($reports);
        // log to watchdog
        foreach ($reports as $report) {
            $report = (array) $report; // convert object to array
            $omit = array('violated-directive', 'blocked-uri');
            $data = array_diff_key($report, array_flip($omit));
            $info = array(
                '@directive' => $report['violated-directive'],
                '@blocked_uri' => $report['blocked-uri'],
                '@data' => print_r($report, TRUE),
            );
            watchdog('seckit', 'CSP: Directive @directive violated. <br /> Blocked
            URI: @blocked_uri. <br /> Data: <pre>@data</pre>.', $info, WATCHDOG_WARNING);
        }
    }
}
```

#### b. X-XSS-Protection HTTP Header

```
function _seckit_x_xss($apply) {
    switch ($apply) {
        case SECKIT_X_XSS_0:
            drupal_add_http_header('X-XSS-Protection', '0'); // set X-XSS-Protection
            header to 0
            break;

        case SECKIT_X_XSS_1:
            drupal_add_http_header('X-XSS-Protection', '1; mode=block'); // set X-XSS-
            Protection header to 1; mode=block
            break;

        case SECKIT_X_XSS_DISABLE:
            default: //do nothing
            break;
    }
}
```

#### c. Strict-Transport-Security HTTP header

```
function _seckit_hsts($apply) {
    if ($apply) {
        // get default/set options
        $options = _seckit_get_options();
        // prepare HSTS header value
    }
}
```

```

$max_age = $options['seckit_ssl']['hsts_max_age'];
$subdomains = $options['seckit_ssl']['hsts_subdomains'];
$header[] = "max-age=$max_age";
if ($subdomains) {
    $header[] = 'includeSubDomains';
}
$header = implode('; ', $header);
// send HSTS header
drupal_add_http_header('Strict-Transport-Security', $header);
}
}

```

#### d. Default Security Options

```

function _seckit_get_options() {
    // set default options
    $default['seckit_xss']['csp'] = array(
        'report-only' => 0,
        'script-src' => '',
        'object-src' => '',
        'img-src' => '',
        'media-src' => '',
        'style-src' => '',
        'frame-src' => '',
        'font-src' => '',
        'connect-src' => '',
        'policy-uri' => '',
    );
    $default['seckit_csrf'] = array(
        'origin' => 1,
        'origin_whitelist' => '',
    );
    $default['seckit_clickjacking'] = array(
        'js_css_noscript' => 0,
        'x_frame_allow_from' => '',
    );
    $default['seckit_ssl'] = array(
        'hsts' => 0,
        'hsts_subdomains' => 0,
    );
    $default['seckit_various'] = array(
        'from_origin' => 0,
    );
    // get variables
    $result['seckit_xss'] = variable_get('seckit_xss', $default['seckit_xss']);
    $result['seckit_csrf'] = variable_get('seckit_csrf', $default['seckit_csrf']);
    $result['seckit_clickjacking'] = variable_get('seckit_clickjacking',
    $default['seckit_clickjacking']);
    $result['seckit_ssl'] = variable_get('seckit_ssl', $default['seckit_ssl']);
    $result['seckit_various'] = variable_get('seckit_various',
    $default['seckit_various']);
    // enable Content Security Policy (CSP)
    if (!isset($result['seckit_xss']['csp']['checkbox'])) {
        $result['seckit_xss']['csp']['checkbox'] = 0;
    }
    // set CSP default-src directive to self
    if (!isset($result['seckit_xss']['csp']['default-src']) ||
    !$result['seckit_xss']['csp']['default-src']) {
        $result['seckit_xss']['csp']['default-src'] = "'self'";
    }
    // set CSP report-uri directive to menu callback
    if (!isset($result['seckit_xss']['csp']['report-uri']) ||
    !$result['seckit_xss']['csp']['report-uri']) {
        $result['seckit_xss']['csp']['report-uri'] =
    'admin/config/system/seckit/csp-report';
    }
    // set X-XSS-Protection header to disabled (browser default).
}

```

```

if (!isset($result['seckit_xss']['x_xss']['select'])) {
    $result['seckit_xss']['x_xss']['select'] = SECKIT_X_XSS_DISABLE;
}
// enable X-Content-Type-Options
if (!isset($result['seckit_xss']['x_content_type']['checkbox'])) {
    $result['seckit_xss']['x_content_type']['checkbox'] = 1;
}
// enable Origin-based protection
if (!isset($result['seckit_csrf']['origin'])) {
    $result['seckit_csrf']['origin'] = 1;
}
// set X-Frame-Options header to SameOrigin
if (!isset($result['seckit_clickjacking']['x_frame'])) {
    $result['seckit_clickjacking']['x_frame'] = SECKIT_X_FRAME_SAMEORIGIN;
}
// set Custom text for disabled JavaScript message
if (!isset($result['seckit_clickjacking']['noscript_message'])) {
    $result['seckit_clickjacking']['noscript_message'] = t('Sorry, you need to
enable JavaScript to visit this website.');
```

## 7.2.3 Rule Model Specification

The Rule Model is controlled using the SecKit GUI through which some Trust management rule templates can be generated.

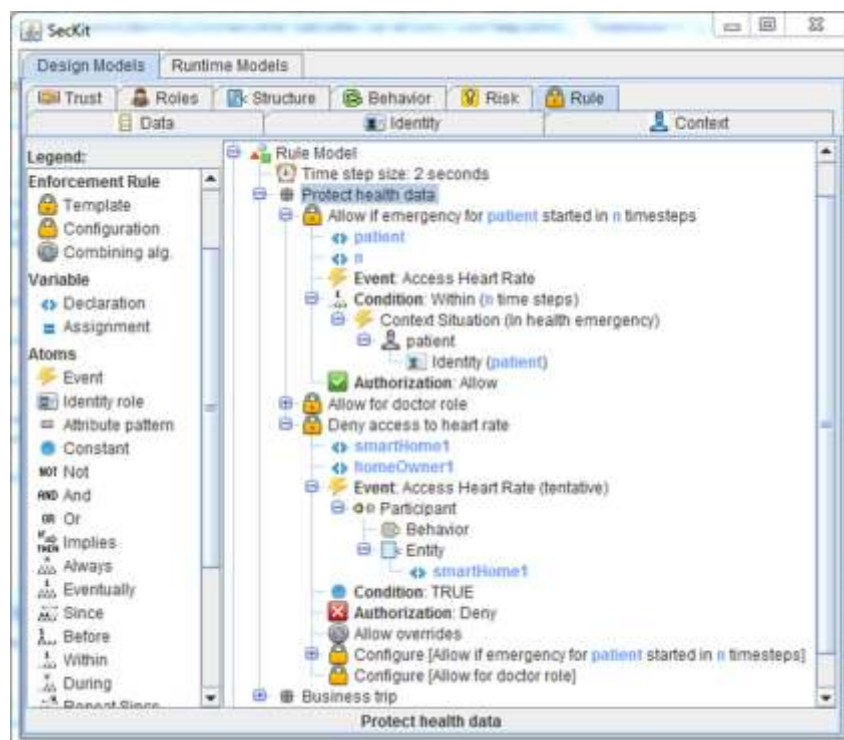


Figure 9: SecKit GUI that controls rule model specification

Two examples of role and context-based rule templates for tentative (left) and actual (left) events are depicted in the figure below.



Figure 10: Context-based rule templates

SecKit introduces abstract Event-Condition-Action (ECA) rule templates and configurations. The ECA rule policy language supports the specification of templates with complex conditions including context situation events, propositional, temporal, cardinality, role assignments, and trust assessment operators.

Rule templates are parameterized with variables and may be recursively nested using a flexible configuration rule that instantiates and disposes rule templates according to particular conditions. For example, a configuration rule may be specified to instantiate a set of enforcement templates when a particular context situation starts (e.g., moving from the house to a public environment) and to dispose the instantiated templates when the situation ends (e.g., exiting from the public environment). The change of the context can be simply triggered by a recording of location (i.e., provided by a GPS receiver or communication transmitter in the smartphone) or by other events like the authentication of the badge when an employee enters the office. This capability is important to support changes in the context and address the challenge related to the dynamic context. A change in the context could also change the levels of access to the IoT services and devices. The change of the levels of access is embedded in the policy template and the user has the power to accept, modify or reject it before the policies are deployed and activated in the IoT devices used by her or him.

Rules can be specified using context situation events, temporal operators, and trust bootstrapping using dispositional trust values by default. Furthermore, rules can be specified to decrease the trust degrees everyday by a specific amount assigning old experiences or recommendations a lower weight. An interesting application is also the implementation of alternative behaviours to require explicit consent to allow other people inside the house in addition to the trust-based decisions if home owner is on holidays.

Nested enforcement rule templates also specify a conflict resolution algorithm that should be used when two or more policy rules with conflicting results are triggered, such as first applicable in their specified order. This is important to address challenge about the influence of Psychological bias. While policies created by users could have embedded personal bias, the conflicts with more generic rules (e.g., privacy regulations) will be detected and can be automatically resolved by the toolkit using the selected conflict resolution algorithm.

## 7.2.4 Potential for Integrating SecKit with ACTIVAGE

SecKit, when implemented in the security and privacy protection module, could be a crucial component of the ACTIVAGE IoT Ecosystem Suite whose purpose is to guarantee both the protection of sensitive information of users and will also comply with ethical and legal requirements for privacy and confidentiality. More specifically, the capabilities of the SecKit PDP component (Role Manager, Policy Repository, etc) could be highly leveraged in all the layers of the ACTIVAGE security module. For instance, in:

1. Protection of Intellectual Property in the Service Layer (I8 in Figure 11),
2. ACTIVAGE Privacy and Confidentiality requirements (I9 in Figure 11)
3. Platform Specific Privacy and Data Protection applied approaches (I10 in Figure 11).

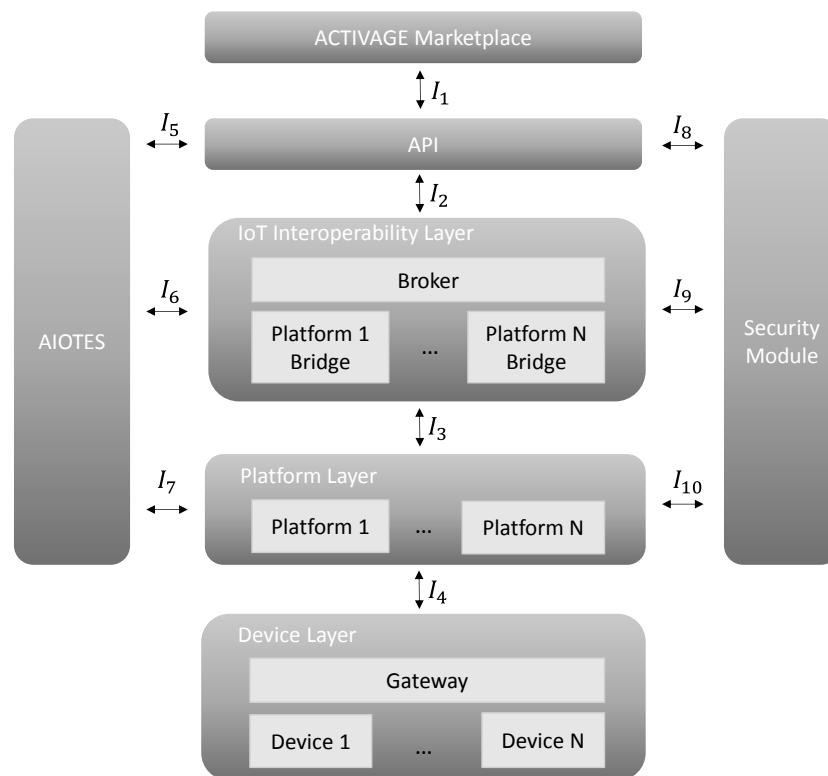


Figure 11: ACTIVAGE High-Level Architecture

Furthermore, the toolkit can be leveraged to ensure the appliance of ethics rules upon the different user roles of the project. Technically, the Role Manager PDP sub-component could be matched with the following roles of the ACTIVAGE architecture: (a) IoT system owner, (b) 1<sup>st</sup> degree relatives, (c) other family members / friends, and (d) carers.

Two examples/scenarios (as taken from Section 5.4 above) of how the ACTIVAGE roles outlined above, could participate in SecKit context-based rule templates based on events could be:

1. The owner (i.e. the patient) who will be able him/ herself to provide selected data access to third parties 1st degree relatives (e.g. his/ her children), so that they can monitor his/her health or diet, if in this way he/she feels safer.
2. When the system realises a potential deviation from owner's planned actions (i.e. not following or not performing the proper exercises, deviating from his/her route), feedback will be strictly given to the owner him/ herself and not to the 1st degree relatives or other persons (i.e. Other family members/ friends or carer). Only in case of medical emergency

recognised or risk of getting lost (for people with significant cognitive problems; diagnosed condition) will the system inform her/ his carer.

Another important capability, which can be provided by the toolkit is to separate the On-Line and Off-line identity because the policy can be designed in such a way as to expose only specific information of the user in the on-line world, which can be separated by its real off-line identity. In other words, policies can be used to implement anonymization through pseudonyms or obfuscation of personal data (e.g., location data) to address the on-line and off-line identity challenge of IoT. In other words, the toolkit can support the concept of “privacy by design”.

Finally, as described in Kounelis et al. (2014), the toolkit can be used to define threat scenarios that provide an indication of the level of risk and required trust in a specific IoT operation including the possible negative consequences. The risk assessment model uses policy profiles as reference countermeasures that could be adopted to mitigate specific threat scenarios.

Additional details on the structure and capabilities of the Model-based Security Toolkit are presented in (Neisse et al. 2015). The SecKit framework has been implemented and already validated by some of the authors in (Neisse et al. 2014) for feasibility and performance aspects in various IoT devices.

## 8 Conclusion/ Future Work

Besides scientific advance, the potential benefit of the elderly users from ACTIVAGE will be social, cultural, economic and individual. Looking at the project in terms of human dignity, ACTIVAGE supports elderly people have Healthy and Active Aging, and to live their life autonomously and independently as long as possible. Furthermore, access to information society and health care institution is facilitated. Therefore, having ACTIVAGE ethics policy as a reference document to govern all activities in the project is critical; from research and development activities to data analysis and reporting. This document is a “baseline” document to be provide the basis of the ACTIVAGE ethical policy and framework of each DS, with any arising issues or topics not originally anticipated during this early stages of the project.

Major ethics issues were addressed and listed in this document with consideration and reference to international and European legislation and guidelines. The ethics management team (i.e. the ACTIVAGE PLG Board in collaboration with the Coordinator and Technical Manager) will oversee and scrutinise the research protocols with regards to privacy, confidentiality, anonymity and ethical risk assessment and mitigation.

Obtaining consent is of core important in testing and ethics. The informed consent is a very important part of the research process; that is why a lot of space in the present manual is dedicated to this issue and the relevant facings of a valid informed consent for ACTIVAGE are thoroughly described. Since not all investigators might be familiar with compiling and documenting of informed consent, such information is added here in detail (Appendix B). No experiments are being performed with person unable to give a valid consent.

The goal of this manual is to compose a guide for all the researchers within ACTIVAGE and to set a framework that all ethics related activities could consult in order to get ethically proven guidelines. As the information flow among different systems is constant, multi-dynamic and layered, it is imperative to define early in the project the overarching ethical principles governing all activities within ACTIVAGE project including the Large Scale Pilots. Consideration should be taken for the participants in the Large Scale Pilots and the moral implications of the research with regards to its communication to other external parties through an internal/ external database (i.e. relevant to the Data Management Plan, D1.5). In other words, work completed in the project can carry on “living” through the work of other researchers. Therefore, the ACTIVAGE consortium is obliged not only respect and preserve the values and the dignity of each individual who will participate in the project but additionally to ensure that the ethics management team will supervise activities that may have ethical implications and, as such, safeguard the human privacy rights.

This Ethics and Privacy Protection Manual (D1.5) is only the begging in a structured procedure that will follow in ACTIVAGE in order to ensure ethical viability throughout and after the project. In the next related Deliverable, D1.6 “Ethical and legal report”, which will be submitted at the end of every reporting period (annually), the detailed actions taken towards ethical design from each WP will be reported. Additionally, at the first version of D1.6 “Ethical and legal report”, the requirements of the users will be taken into account and mapped with each WP, in order to guaranty ethical and user design processed throughout the project. Finally, mitigation measures and contingency plans should be developed to prevent or minimize harm to participants or violation of their fundamental rights due to data errors, datasets poor quality or reliability, or underestimated methodological limitations. Thus, in each D1.6 “Ethical and legal report” version, the potential future ethical risks for the next year will be defined from each WP, as well as possible mitigation strategies that need to be taken into account.

# References

- American Psychological Association. (2002). American Psychological Association ethical principles of psychologists and code of conduct (standard 3.10). Available from: <http://www.apa.org/ethics/code2002.html>
- Articles 10 and 11 of Directive 95/46/EC
- Baldini, G., Botterman, M., Neisse, R. et al. Sci Eng Ethics (2016). doi:10.1007/s11948-016-9754-5
- Carlo Petrini and Enrico Alleva (2013). Editorial Issues raised by “incidental findings” and their ethical implications. Ann Ist Super Sanità 2013 | Vol. 49, No. 2: 108-109.
- CASAGRAS Project “Final Report, RFID and the Inclusive Model for the Internet of Things,” Available from: [http://www.grifs-project.eu/data/File/CASAGRAS FinalReport \(2\).pdf](http://www.grifs-project.eu/data/File/CASAGRAS%20FinalReport%20(2).pdf)
- CCS Insight Augmented and Virtual Reality Devices to Become a \$4 Billion-Plus Business in Three Years. 2015. Available from: <http://www.ccsinsight.com/press/company-news/2251-augmented-and-virtual-reality-devices-to-become-a-4-billion-plus-business-in-three-years>, <https://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#aa4e9da3cb55>
- Charter of Fundamental Rights of the European Union. Official Journal C 34, 18/12/2000 P. 0001 – 0022. Available from: [http://www.europarl.europa.eu/charter/pdf/text\\_en.pdf](http://www.europarl.europa.eu/charter/pdf/text_en.pdf)
- Cisco. (2014). Fourth Annual Global Cloud Index Study: <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-indexgci/>
- Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on “A comprehensive approach on personal data protection in the European Union”.
- Council of Europe. Additional Protocol to the Convention on Human Rights and Biomedicine, Concerning Biomedical Research. Council of Europe Treaty Series - No. 195 25 January 2005. Available from: [www.conventions.coe.int/Treaty/EN/Treaties/Html/195.htm](http://www.conventions.coe.int/Treaty/EN/Treaties/Html/195.htm)
- Covington & Burling EU Poised to Formally Adopt New Data Protection Laws; Amended Texts Published. (2016, April 06). Available from: <https://www.insideprivacy.com/international/european-union/eu-poised-to-formally-adopt-gdpr-and-pcj-dpd/>
- Danova, T., (2013) Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020, <http://www.businessinsider.com/75-billion-devices-will-be-connected-to-theinternet-by-2020-2013-10#ixzz2jlo3UCkd>
- Dechesne, F., Hoven, J.V., Pereira, Â.G., & Weber, R. (2012). Fact Sheet-ethics Subgroup lot -version 4.0 1.
- Ebersold K., and Glass R. 2016, The Internet of Things: a cause for ethical concern, Issues in Information Systems. Vol. 17, Issue IV, 145-151.
- EGE (European Group on Ethics in Science and New Technologies to the European Commission) (2012) 'Ethics of Information and Communication Technologies', Publications Office of the European Union: Luxembourg, Opinion No. 26
- Electrochemical Society, available from: <http://www.electrochem.org/redcat-blog/iot-and-sensors-creating-a-multitrillion-dollar-market/>

Empirica and WRC, 'ICT & Ageing - European Study on Users, Markets and Technologies: Final Report' (European Commission, 2010). Available from:

[http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc\\_id=952](http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=952)

European Commission (2010) eInclusion: Ageing Well Action Plan. Available from:

[http://ec.europa.eu/information\\_society/activities/einclusion/policy/ageing/index\\_en.htm](http://ec.europa.eu/information_society/activities/einclusion/policy/ageing/index_en.htm)

European Commission: The 2015 ageing report, underlying assumptions and projection, methodologies. (2014).

European Convention on Human Rights. *World Encyclopedia*. 2005. Available

from: <http://www.encyclopedia.com/doc/1O142-EuropeanConventnnHmnRghts.html>

Freeman, L., and Peace A. (2005). Information Ethics: Privacy and Intellectual Property. *Information Management* 17 (31). ProQuest. Web. 22 Apr. 2014.

Froehlich, Thomas (December 2004). "A brief history of information ethics". bid.ub.edu. Kent State University. Available from: <http://bid.ub.edu/13froel2.htm>

Guillemin, P., & Friess, P. (2009) Internet of things strategic research roadmap. Technical report, The Cluster of European Research Projects, September 2009. Available from:

[http://www.internet-of-things-research.eu/pdf/loT\\_Cluster\\_Strategic\\_Research\\_Agenda\\_2009.pdf](http://www.internet-of-things-research.eu/pdf/loT_Cluster_Strategic_Research_Agenda_2009.pdf)

Haller, S. 2011. The Things in the Internet of Things. Poster paper presented at Internet of Things Conference 2010, Tokyo, Japan. Available from: <http://www.iot2010.org/>

Haller, S., Karnouskos, S., & Schroth, C. (2009). The internet of things in an enterprise context. Berlin

Harmo, P., Knuuttila, J., Taipalus, T., Vallet, J. and Halme, A. (2005) Automation and Telematics for Assisting People Living at Home, Helsinki (IFAC): Automation Technology Laboratory, Helsinki University of Technology.

Hoven, J.V., Dechesne, F., Pereira, Â.G., & Weber, R. (2012). Fact Sheet-ethics Subgroup lot -version 4.0 1.

Internet Live Stats. Elaboration of data by International Telecommunication Union (ITU), World Bank, and United Nations Population Division. Available from:

<http://www.internetlivestats.com/internet-users/>

Internet of Things The IoT opportunity – Are you ready to capture a once-in-a-lifetime value pool? Chris Ip (叶远扬) Hong Kong IoT Conference 21 June 2016. Available from: [http://hk-iot-conference.gs1hk.org/2016/pdf/\\_04\\_Mc%20Kinsey%20-%20\(Chris%20Ip%20\)%20ppt%20part%20%201%20\\_IoT%20-%20Capturing%20the%20Opportunity%20vF%20-%2021%20June%202016.1pptx.pdf](http://hk-iot-conference.gs1hk.org/2016/pdf/_04_Mc%20Kinsey%20-%20(Chris%20Ip%20)%20ppt%20part%20%201%20_IoT%20-%20Capturing%20the%20Opportunity%20vF%20-%2021%20June%202016.1pptx.pdf)

Internet of Things. Wikipedia. Available from: [http://en.wikipedia.org/wiki/Internet\\_of\\_things](http://en.wikipedia.org/wiki/Internet_of_things)

IoT platforms: enabling the Internet of Things, March 2016. Available from:

<https://www.ihs.com/Info/0416/internet-of-things.html>

Irion, K., S. Yakovleva, M. Bartl: Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements". Institute for Information Law (IViR), University of Amsterdam. 22 September 2016.

Joan, Reitz M. "Information Ethics." Online Dictionary For Library And Information Science. N.p., 2010. Web. Available from: [http://www.abc-clio.com/ODLIS/odlis\\_i.aspx](http://www.abc-clio.com/ODLIS/odlis_i.aspx)

Kounelis, I., Baldini, G., Nisse, R., Steri, G., Tallacchini, M., & Guimaraes Pereira, A. (2014). Building trust in the human–internet of things relationship. *IEEE Technology and Society Magazine*, 33(4), 73–80.

Miorandi D., Sicari, S., De Pellegrini, F. and Chlamta, I. 2012, Internet of things: Vision, applications and research challenges, Ad Hoc Netw. (2012). Available from:

<http://dx.doi.org/10.1016/j.adhoc.2012.02.016>

Neisse, R., Steri, G. & Baldini, G. (2014) Enforcement of security policy rules for the Internet of Things, in: 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Available from:

[https://www.researchgate.net/publication/267152429\\_Enforcement\\_of\\_Security\\_Policy\\_Rules\\_for\\_the\\_Internet\\_of\\_Things](https://www.researchgate.net/publication/267152429_Enforcement_of_Security_Policy_Rules_for_the_Internet_of_Things)

Neisse, R., Steri, G., Fovino, I. N., & Baldini, G. (2015). SecKit: A model-based security toolkit for the internet of things. Elsevier Computers & Security Journal.

doi:10.1016/j.cose.2015.06.002. Available from:

<http://www.sciencedirect.com/science/article/pii/S0167404815000887#fig8>

Organisation for Economic Co-operation and Development, 'The OECD Privacy Framework' (Organisation for Economic Co-operation and Development, 2013). Available from:

[http://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)

R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, and A. R. Biswas, 2015, "An agent-based framework for informed consent in the internet of things," in Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, pp. 789–794, IEEE. Available from:

[https://www.researchgate.net/publication/303471338\\_An\\_Agent-based\\_Framework\\_for\\_Informed\\_Consent\\_in\\_the\\_Internet\\_of\\_Things](https://www.researchgate.net/publication/303471338_An_Agent-based_Framework_for_Informed_Consent_in_the_Internet_of_Things)

Rechel B. et al. Ageing in the European Union (2013).

Roberts, and Peter Wright, eds. 2008. Performative social science. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research 9 (2).

Sarkar, Chayan, et al., 2015. "DIAT: A Scalable Distributed Architecture for IoT." Internet of Things Journal, IEEE 2. 230-239. Available from:

[https://www.researchgate.net/publication/270567077\\_DIAT\\_A\\_Scalable\\_Distributed\\_Architecture\\_for\\_IoT](https://www.researchgate.net/publication/270567077_DIAT_A_Scalable_Distributed_Architecture_for_IoT)

Schmidt, E. (2010). Available from: <http://techcrunch.com/2010/08/04/schmidt-data/>

Schmitt J. M. (2002) 'Innovative medical technologies help ensure improved patient care and cost-effectiveness', International Journal of Medical Marketing, 2(2):174-178

Stahl B. ETICA - Project Final Report. De Montfort University. 2011.

Stahl et. al. 2011, ETICA. Final report. Available from:

[http://cordis.europa.eu/publication/rcn/15318\\_en.html](http://cordis.europa.eu/publication/rcn/15318_en.html)

Tom L. Beauchamp and James F. Childress, Principles of Biomedical Ethics (New York: Oxford University Press, 2009).

United Nations: World population ageing 2013, Economic and Social Affairs (2013).

Usability Professionals Association, UPA. Available from:

<http://www.usabilityprofessionals.org>

Wachtel, T (2012). IoT Expert Group Final Meeting Report. European Commission. European Commission, 14 Nov.2012. Available from:

[http://ec.europa.eu/information\\_society/newsroom/cf/dae/document.cfm?action=display&doc\\_id=1747](http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=1747)

## Appendix A ACTIVAGE Ethics checklist

Ethics consideration were included in the following table during the proposal submission. The ACTIVAGE Large scale IoT pilots involve elderly users with cognitive impairment and other stakeholder groups (row 7), personal data will be gathered (e.g. age, gender, diagnosis) but will be kept separately from the rest of data, therefore no identification will be possible. Raw data will be accompanied by metadata files including categorisation for facilitating analysis (row 13). Processing of previous data will be performed locally and only in cases where it is feasible to use baseline data from similar or matched groups; however, no identification will be possible as data will be anonymised and coded (row 14).

Table 12: ACTIVAGE ethics checklist

	YES	Page
<b>1. HUMAN EMBRYOS/ FOETUSES i</b>		
• Does your research involve Human Embryonic Stem Cells (hESCs)?		
• Does your research involve the use of human embryos?		
• Does your research involve the use of human foetal tissues/cells?		
<b>2. HUMANS</b>		
• Does your research involve human participants?	X	DoA, Part A, pp 16-18
○ Are they volunteers for social or human sciences research?		
○ Are they persons unable to give informed consent?		
○ Are they vulnerable individuals or groups?		
○ Are they children/minors?		
○ Are they patients?	X	DoA, Part A, pp 12-16
○ Are they healthy volunteers for medical studies?	X	DoA, Part A, pp 12-16
• Does your research involve physical interventions on the study participants?		
<b>3. HUMAN CELLS / TISSUES</b>		
• Does your research involve human cells or tissues? If your research involved human embryos/foetuses, please also complete the section “Human Embryos/Foetuses” (Box 1).		
<b>4. PROTECTION OF PERSONAL DATA ii</b>		
• Does your research involve personal data collection and/or processing?	X	DoA, Part A, pp 16-18
○ Does it involve the collection and/or processing of sensitive personal data (e.g.: health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	X	DoA, Part A, pp 16-18

○ Does it involve processing of genetic information?		
○ Does it involve tracking or observation of participants?	<b>X</b>	DoA, Part A, pp 16-18
• Does your research involve further processing of previously collected personal data (secondary use)?		
<b>5. ANIMALS iii</b>		
• Does your research involve animals?		

## Appendix B ACTIVAGE Consent Form (templates)

This Appendix is divided in 5 sections:

- B1.** Includes a template for a consent form to be used with patients (clinical and qualitative research) based on the universally accepted consent form template of the world health organization (WHO) ([http://www.who.int/rpc/research\\_ethics/informed\\_consent/en/](http://www.who.int/rpc/research_ethics/informed_consent/en/))
- B2.** Contains simple consent forms to be used with any type of stakeholder group
- B3.** Contains the documentation of Consent with the research participant's identity and the identity and dated signatures of the participant affirming that consent was given
- B4.** Informed Consent Documentation for an Illiterate Participant
- B5.** This form will be used by all ACTIVAGE researchers who record private information in the course of any evaluation/pilots. It has to be **signed** by the investigator and by each participant.

## B.1 Informed Consent Form (based on a clinical study template)

The informed consent templates (including information sheet) are based on WHO templates ([http://www.who.int/rpc/research\\_ethics/informed\\_consent/en/](http://www.who.int/rpc/research_ethics/informed_consent/en/) last access: 02/07/15). This template can be adjusted for all user groups addressed within ACTIVAGE project.

(Language used throughout form should be at the level of a local student of class 6<sup>th</sup>/8<sup>th</sup>)

Notes to Researchers:

1. Please note that this is a template based in the one developed by WHO ERC to assist the Principal Investigator in the design of their informed consent forms (ICF). It has been adapted to the outline and requirements of their particular pilot site requirements.
2. The informed consent form consists of two parts: the information sheet and the consent form.
3. Do not be concerned by the length of this template. It is long only because it contains guidance and explanations which are for the researcher and which they will not be included in the informed consent forms that they will be developed and provided to participants at each pilot site.
4. This template includes examples of key questions that may be asked at the end of each section that could ensure the understanding of the information being provided, especially if the research study is complex and participants suffer from cognitive impairment. These are just examples, and suggestions, and the investigators will have to modify the questions depending upon the needs of each pilot site.

5. In this template:

square brackets indicate where specific information is to be inserted;

bold lettering indicates sections or wording which should be included;

standard lettering is used for explanations to researchers only and must not be included in your consent forms. The explanation is provided in black, and examples are provided in red in italics. Suggested questions to elucidate understanding are given in black in italics.

TEMPLATE ON FOLLOWING PAGE

**[Name of Principle Investigator]**

**Informed Consent form for \_\_\_\_\_**

*Name the group of individuals for whom this informed consent form is written. Because research for a single project is often carried out with a number of different groups of individuals - for example healthcare professionals, formal carers, patients, and parents of patients - it is important that you identify which group this particular consent is for.*

*(Example: This Informed Consent Form is for individuals suffering from cognitive impairment who will participate in ACTIVAGE project.)*

You may provide the following information either as a running paragraph or under headings as shown below.

**[Name of Principal Investigator]**

**[Name of Organization]**

**[Name of Position/Role]**

**[Name of Proposal and version]**

**This Informed Consent Form has two parts:**

- **Information Sheet (to share information about the research with you)**
- **Consent Form (for signatures if you agree to take part)**

**You will be given a copy of the full Informed Consent Form**

## PART I: Information Sheet

### Introduction

Briefly state who you are and explain that you are inviting them to participate in the research you are doing. Inform them that they may talk to anyone they feel comfortable talking with about the research and that they can take time to reflect on whether they want to participate or not. Assure the participant that if they do not understand some of the words or concepts, that you will take time to explain them as you go along and that they can ask questions now or later.

*(Example: I am X, working for the Y Research Institute. We are doing research on cognitive impairment, which is nowadays very common. I am going to give you information and invite you to be part of this research. You do not have to decide today whether or not you will participate in the research. Before you decide, you can talk to anyone you feel comfortable with about the research.)*

*There may be some words that you do not understand. Please ask me to stop as we go through the information and I will take time to explain. If you have questions later, you can ask them of me, the study doctor or the staff. For participants who are health care professionals and formal carers, may include information about the health related aspects of the project with language and content relevant to their profession and clarify their role in participant recruitment if they agree to participate).*

### Purpose of the research

Explain in lay terms why we are doing research within the framework of ACTIVAGE project. The language used should clarify rather than confuse. Specifically, for users who suffer from cognitive impairments and informal carers (who might be members of the family, not working in any related field). Use local and simplified terms for cognitive impairment, e.g. forgetting. Avoid using terms like pathogenesis, indicators, determinants, equitable etc. There are guides on the internet to help you find substitutes for words which are overly scientific or are professional jargon.

*(Example: Forgetting is the most common symptom for people over 60 years old and it sometimes it is encountered in older people. Recent studies show that supporting an individual during their everyday activities helps them stay alert and mentally focused. There are applications that can help a person who forgets that can be used with no or minimum training. The reason we are doing this research is to find out how these applications can help them when they use them in their everyday life.)*

### Type of Research Intervention

Briefly state the type of intervention that will be undertaken. This will be expanded upon in the procedures section but it may be helpful and less confusing to the participant if they know from the very beginning whether, for example, the research involves follow-ups, continuous involvement, types of data gathered, completing questionnaires, etc.

*(Example: This research will involve using X applications for X period of time with two follow-up visits to your doctor.)*

### Participant selection

State why this participant has been chosen for this research. People often wonder why they have been chosen to participate and may be fearful, confused or concerned.

*(Example: We are inviting people who forget and who attend clinic X to participate in the research on testing new technologies to help people who have memory difficulties.)*

**Example of question to elucidate understanding:** Do you know why we are asking you to take part in this study? Do you know what the study is about?

### **Voluntary Participation**

Indicate clearly that they can choose to participate or not. State, what the alternative - in terms of the treatment offered by the clinic - will be, if they decide not to participate. State, only if it is applicable, that they will still receive all the services they usually do whether they choose to participate or not. This can be repeated and expanded upon later in the form as well, but it is important to state clearly at the beginning of the form that participation is voluntary so that the other information can be heard in this context. Participants with cognitive impairment will be reminded about their participation being voluntary before moving to the consent form and signing it.

*(Example: Your participation in this research is entirely voluntary. It is your choice whether to participate or not. Whether you choose to participate or not, all the services you receive will continue and nothing will change. If you choose not to participate in this research project, you will offer the treatment that is routinely offered for your condition (in case the participant is recruited in a clinic (e.g. outpatient clinic), and we will tell you more about it later. You may change your mind later and stop participating even if you agreed earlier.)*

**Examples of question to elucidate understanding:** If you decide not to take part in this research study, do you know what your options are? Do you know that you do not have to take part in this research study, if you do not wish to? Do you have any questions?

### **Information on the ACTIVAGE applications and system to be tested:**

1. Give information about the applications and explain what it does/ means. Explain to the participant why you are comparing results from various phases, why testing is carried out for long period of time.
2. Provide as much information as is appropriate and understandable about the system and applications such as its manufacturer or location of manufacture and the reason for its development (including illustrations of the applications or real demos, depending on availability).
3. Explain the known experience with these applications/services (mainly for technological implementations already in the market)

*(Example: The system and applications we are testing in this research are called A, B, X. Many of them have been tested before but now they will be integrated and offered as one system. We now want to test the whole system in different phases as it is evolving to find out if the application (s) ABX is made by C, D, E. We know of no problem or risks related to its/their use. Some participants in the research will not be given this/these application(s) we are testing. Instead, they will be given another/other application(s) XYZ. There is no risk associated with the use of this/these application(s) and no known problems. The healthcare professionals will receive information about the applications the users will test and what they do. The participants with cognitive impairments will receive information with illustrations (i.e. pictures, examples of functionalities, in simple language with no jargon.)*

### **Procedures and Protocol**

Describe or explain the exact procedures that will be followed on a step-by-step basis, the tests that will be done, data that will be gathered. Explain from the outset what some of the more unfamiliar procedures involve (medical examination, ICT training, etc.) Indicate which procedure is routine and which is experimental or research. Participants should know what to expect and what is expected of them. Use active, rather than conditional, language. Write "we will ask you to...." instead of "we would like to ask you to....".

In this template, this section has been divided into two: firstly, an explanation of unfamiliar procedures and, secondly, a description of process.

### **A. Unfamiliar Procedures**

This section should be included if there may be procedures which are not familiar to the participant.

Involving randomization or blinding, the participants should be told what that means and what chance they have of getting into each group (in case, of course, randomisation is applied).

*(Example: To do this, we will put people taking part in this research into two groups. The groups are selected by chance, as if by tossing a coin. . This information will be in our files, but we will not look at these files until after the research is finished. This is the best way we have for testing without being influenced by what we think or hope might happen. We will then compare which of the two has the best results. The healthcare professionals will be looking after you and the other participants very carefully during the study. If there is anything you are concerned about or that is bothering you about the research please talk to me or one of the other researchers.)*

### **B. Description of the Process**

Describe to the participant what will happen on a step-by-step basis. It may be helpful to the participant if you use drawings or props to better illustrate the procedures. An illustration of the system and applications will help participants understand the process better. Participants should be re-assured that they will provide all relevant information and training before actually using the system and the integrated applications. Moreover, there are no safety related risks when using the system, as it will be verified within the framework of the INLIFE project.

*(Example: During the research you make X visits to the clinic/institute/ X premises.*

We will also ask you a few questions about your general health and take a few measurements.

At the next visit, you will again be asked some questions about your health and then you will complete some questionnaires.)

### **Duration**

Include a statement about the time commitments of the research for the participant including both the duration of the research and follow-up, if relevant.

*(Example: The research takes place over \_\_\_\_ (number of) months in total. During that time, it will be necessary for you to come to the clinic/hospital/health facility \_\_\_\_\_(number of) days , for \_\_\_\_ (number of) hours each day. We would like to meet with you X months after your last visit for a final follow-up. In total, you will be asked to come Xtimes to the clinic in X months. At the end of X months, the research will be finished.)*

**Examples of question to elucidate understanding:** Can you tell me if you remember the number of times that we are asking you to come to the hospital to complete the treatment? The research project? Over how many weeks? Etc. Do you have any other questions? Do you want me to go through the procedures again?

### **Risks**

Explain and describe any possible or anticipated risks. Describe the level of care that will be available in the event that harm does occur, who will provide it, and who will pay for it. A risk can be thought of as being the possibility that harm may occur. Provide enough information

about any risks (not anticipated any within ACTIVAGE) that the participant can make an informed decision.

*(Example: By participating in this research it is there will be no more possibility to be at greater risk than you would otherwise be. While the possibility of this happening is very low, you should still be aware of the possibility. We will try to decrease the chances of this event occurring, but if something unexpected happens, we will provide you with\_\_\_\_\_.)*

**Examples of question to elucidate understanding:** Do you understand which applications will be tested? Do you have any other questions?

**Benefits** *(if reimbursement is used; benefits might not be provided)*

Mention only those activities that will be actual benefits and not those to which they are entitled regardless of participation. Benefits may be divided into benefits to the individual, benefits to the community in which the individual resides, and benefits to society as a whole as a result of finding an answer to the research question.

*(Example: If you participate in this research, you will have the following benefits: the applications will help to organize your day, exercise your brain, etc.). There may be other benefits for you and your participation is likely to help us find the answer to the research question. There may be any benefit to the society at this stage of the research and future generations are likely to benefit.)*

### **Reimbursements**

State clearly what you will provide the participants with as a result of their participation. There is no encouragement for using incentives. However, it recommends that reimbursements for expenses incurred as a result of participation in the research be provided. These may include, for example, travel costs and money for wages lost due to visits to health facilities. The amount should be determined within the host country context.

*(Example: We will give you [amount of money] to pay for your travel to the place of study taken place/follow-ups/parking and we will give you [amount] for lost work time. You will not be given any other money or gifts to take part in this research.)*

**Examples of question to elucidate understanding:** Can you tell me if you have understood correctly the benefits that you will have if you take part in the study? Do you know if the study will pay for your travel costs and time lost, and do you know how much you will be reimbursed? Do you have any other questions?

### **Confidentiality**

Explain how the research team will maintain the confidentiality of data, especially with respect to the information about the participant which would otherwise be known only to the physician but would now be available to the entire research team. Note that because something out of the ordinary is being done through research, any individual taking part in the research is likely to be more easily identified by members of the community and is therefore more likely to be stigmatized.

*(Example: With this research, something out of the ordinary is being done in your community. It is possible that if others in the community are aware that you are participating, they may ask you questions. We will not be sharing the identity of those participating in the research.)*

*The information that we collect from this research project will be kept confidential. Information about you that will be collected during the research will be put away and no-one but the researchers will be able to see it. Any information about you will have a number on it instead of your name. Only the principal investigator will know what your number is and we will lock that information up with a lock and key. It will not be shared with or given to anyone*

*except [name who will have access to the information, such as research sponsors, Ethics board, your clinician, etc.]*

**Example of question to elucidate understanding:** Did you understand the procedures that we will be using to make sure that any information that we as researchers collect about you will remain confidential? Do you have any questions about them?

### Sharing the Results

Where it is relevant, your plan for sharing the information with the participants should be provided. If you have a plan and a timeline for the sharing of information, include the details. You should also inform the participant that the research findings will be shared more broadly, for example, through publications and conferences.

*(Example: Confidential information will not be shared. There will be small meetings with consortium and these will be announced. After these meetings, we will publish the results in order that other interested people may learn from our research.)*

### Right to Refuse or Withdraw

This is a reconfirmation that participation is voluntary and includes the right to withdraw. Tailor this section to ensure that it fits for the group for whom you are seeking consent. The example used here is for a patient at a clinic.

*(Example: You do not have to take part in this research if you do not wish to do so and refusing to participate will not affect your treatment (if recruitment at a clinic) in any way. You will still have all the benefits that you would otherwise have at this clinic. You may stop participating in the research at any time that you wish without losing any of your rights as a patient here. Your treatment at this clinic will not be affected in any way.)*

OR

*(Example: You do not have to take part in this research if you do not wish to do so. You may also stop participating in the research at any time you choose. It is your choice and all of your rights will still be respected.)*

### Alternatives to Participating

Include this section only if the study involves administration of health related procedures and relevant to communication between healthcare professional and participant. It is important to explain and describe the established standard treatment. The participant should feel no pressure to

*(Example: If you do not wish to take part in the research, you will be provided with the established standard treatment available at the centre/institute/hospital. People who have cognitive impairment are given....)*

### Who to Contact

Provide the name and contact information of someone who is involved, informed and accessible (a local person who can actually be contacted. State also that the proposal has been approved and how.

*(Example: If you have any questions you may ask them now or later, even after the study has started. If you wish to ask questions later, you may contact any of the following: [name, address/telephone number/ e-mail])*

This proposal has been reviewed and approved by [name of the local IRB], which is a committee whose task it is to make sure that research participants are protected from harm. If you wish to find about more about the IRB, contact [name, address, telephone number.]. It

has also been reviewed by the ACTIVAGE Ethics Committee which is supporting this pilot study.

**Example of question to elucidate understanding:** Do you know that you do not have to take part in this study if you do not wish to? You can say No if you wish to? Do you know that you can ask me questions later, if you wish to? Do you know that I have given the contact details of the person who can give you more information about the study? Etc.

## PART II: Certificate of Consent

This section should be written in the first person and have a statement similar to the one in bold below. If the participant is illiterate but gives oral consent, a witness must sign. A researcher or the person going over the informed consent must sign each consent. The certificate of consent should avoid statements that have "I understand...." phrases. The understanding should perhaps be better tested through targeted questions during the reading of the information sheet (some examples of questions are given above), or through the questions being asked at the end of the reading of the information sheet, if the potential participant is reading the information sheet him/herself.

**I have read the foregoing information, or it has been read to me. I have had the opportunity to ask questions about it and any questions that I have asked have been answered to my satisfaction. I consent voluntarily to participate as a participant in this research.**

**Print Name of Participant** \_\_\_\_\_

**Signature of Participant** \_\_\_\_\_

**Date** \_\_\_\_\_

**Day/month/year**

### **If illiterate**

*An illiterate witness must sign (if possible, this person should be selected by the participant and should have no connection to the research team). Participants who are illiterate can provide oral consent.*

**I have witnessed the accurate reading of the consent form to the potential participant, and the individual has had the opportunity to ask questions. I confirm that the individual has given consent freely.**

**Print name of witness** \_\_\_\_\_

**Signature of witness** \_\_\_\_\_

**Date** \_\_\_\_\_

**Day/month/year**

**Statement by the researcher/ person taking consent**

**I have accurately read out the information sheet to the potential participant, and to the best of my ability made sure that the participant understands that the following will be done:**

- 1.
- 2.
- 3.

**I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability. I confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.**

**A copy of this ICF has been provided to the participant.**

**Print Name of Researcher/person taking the consent** \_\_\_\_\_

**Signature of Researcher /person taking the consent** \_\_\_\_\_

**Date** \_\_\_\_\_

**Day/month/year**

## B.2 Informed Consent Form

[YOUR INSTITUTIONAL LETTER HEAD]

**[Informed Consent Form for \_\_\_\_\_]**

Name the group of individuals for whom this consent is written. Because research for a single project is often carried out with a number of different groups of individuals - for example counsellors, community members, clients of services - it is important that you identify which group this particular consent is for.

You may provide the following information either as a running paragraph or under headings as shown below.

**[Name of Principle Investigator]**

**[Name of Organization]**

**[Name of Sponsor]**

**[Name of Project and Version]**

**This Informed Consent Form has two parts:**

- **Information Sheet (to share information about the study with you)**
- **Certificate of Consent (for signatures if you choose to participate)**

**You will be given a copy of the full Informed Consent Form**

### Part I: Information Sheet

#### Introduction

Briefly state who you are and that you are inviting them to participate in research which you are doing. Inform them that they may talk to anyone they feel comfortable talking with about the research and that they can take time to reflect on whether they want to participate or not. Assure the participant that if they do not understand some of the words or concepts, that you will take time to explain them as you go along and that they can ask questions at any time.

#### Purpose of the research

Explain the research question in lay terms which will clarify rather than confuse. Use local and simplified words rather than scientific terms and professional jargon. In your explanation, consider local beliefs and knowledge when deciding how best to provide the information. Investigators however need to be careful not to mislead participants, by suggesting research interests that they do not have. For example, if the study wants to find out about treatments provided by local practitioners, wording should not suggest that they want to find out about how the practitioners are advertising themselves. Misleading participants may be essential and justified in certain circumstances, but that needs to be carefully argued, and approved by an ethics committee.

#### Type of Research Intervention

Briefly state the type of intervention that will be undertaken. This will be expanded upon in the procedures section but it may be helpful and less confusing to the participant if they know from the very beginning whether, for example, the research involves a vaccine, an interview, a questionnaire, or a series of finger pricks.

## Participant Selection

Indicate why you have chosen this person to participate in this research. People wonder why they have been chosen and may be fearful, confused or concerned.

**Example of question to elucidate understanding:** Do you know why we are asking you to take part in this study? Do you know what the study is about?

## Voluntary Participation

Indicate clearly that they can choose to participate or not. State, only if it is applicable, that they will still receive all the services they usually do if they choose not to participate. Explanation: It may be more applicable to assure them that their choosing to participate or not will not have any bearing on their job or job-related evaluations. This can be repeated and expanded upon later in the form as well. It is important to state clearly at the beginning of the form that participation is voluntary so that the other information can be heard in this context. Although, if the interview or group discussion has already taken place, the person cannot 'stop participation' but request that the information provided by them not be used in the research study.

**Examples of question to elucidate understanding:** If you decide not to take part in this research study, do you know what your options are? Do you know that you do not have to take part in this research study, if you do not wish to? Do you have any questions?

## Procedures

- A. Provide a brief introduction to the format of the research study.
- B. Explain the type of questions that the participants are likely to be asked in the focus group, the interviews, or the survey. If the research involves questions or discussion which may be sensitive or potentially cause embarrassment, inform the participant of this.

## Duration

Include a statement about the time commitments of the research for the participant including both the duration of the research and follow-up, if relevant.

**Examples of question to elucidate understanding:** If you decide to take part in the study, do you know how much time will the interview take? Where will it take place? Do you know that we will be sending you transport to pick you up from your home? Do you know how much time will the discussion with other people take? If you agree to take part, do you know if you can stop participating? Do you know that you may not respond to the questions that you do not wish to respond to? Etc. Do you have any more questions?

## Risks

Explain and describe any risks that you anticipate or that are possible. The risks depend upon the nature and type of qualitative intervention, and should be, as usual, tailored to the specific issue and situation.

## Benefits

Benefits may be divided into benefits to the individual, benefits to the community in which the individual resides, and benefits to society as a whole as a result of finding an answer to the research question. Mention only those activities that will be actual benefits and not those to which they are entitled regardless of participation.

## Reimbursements

State clearly what you will provide the participants with as a result of their participation. WHO does not encourage incentives beyond reimbursements for expenses incurred as a result of participation in the research. These may include, for example, travel costs and reimbursement for time lost. The amount should be determined within the host country context.

**Examples of question to elucidate understanding:** Can you tell me if you have understood correctly the benefits that you will have if you take part in the study? Do you know if the study will pay for your travel costs and time lost, and do you know how much you will be re-imbursed? Do you have any other questions?

### Confidentiality

Explain how the research team will maintain the confidentiality of data with respect to both information about the participant and information that the participant shares. Outline any limits to confidentiality. Inform the participant that because something out of the ordinary is being done through research, any individual taking part in the research is likely to be more easily identified by members of the community and therefore more likely to be stigmatized. If the research is sensitive and/or involves participants who are highly vulnerable - research concerning violence against women for example - explain to the participant any extra precautions you will take to ensure safety and anonymity.

The following applies to focus groups: Focus groups provide a particular challenge to confidentiality because once something is said in the group it becomes common knowledge. Explain to the participant that you will encourage group participants to respect confidentiality, but that you cannot guarantee it.

**Example of question to elucidate understanding:** Did you understand the procedures that we will be using to make sure that any information that we as researchers collect about you will remain confidential? Do you understand that we cannot guarantee complete confidentiality of information that you share with us in a group discussion Do you have any more questions?

### Sharing the Results

Your plan for sharing the findings with the participants should be provided. If you have a plan and a timeline for the sharing of information, include the details. You may also inform the participant that the research findings will be shared more broadly, for example, through publications and conferences.

### Right to Refuse or Withdraw

This is a reconfirmation that participation is voluntary and includes the right to withdraw. Tailor this section to ensure that it fits for the group for whom you are seeking consent. The example used here is for a community social worker. Participants should have an opportunity to review their remarks in individual interviews and erase part or all of the recording or note.

### Who to Contact

Provide the name and contact information of someone who is involved, informed and accessible - a local person who can actually be contacted. State also the name (and contact details) of the local IRB that has approved the proposal. State also that the proposal has also been approved by the WHO ERC.

**This proposal has been reviewed and approved by [name of the local IRB], which is a committee whose task it is to make sure that research participants are protected from harm. If you wish to find out more about the IRB, contact [name, address, telephone number.]). It has also been reviewed by the Ethics Review Committee of the World Health Organization (WHO), which is funding/sponsoring/supporting the study.**

**Example of question to elucidate understanding:** Do you know that you do not have to take part in this study if you do not wish to? You can say No if you wish to? Do you know that you can ask me questions later, if you wish to? Do you know that I have given the contact details of the person who can give you more information about the study? Etc.

You can ask me any more questions about any part of the research study, if you wish to. Do you have any questions?

## Part II: Certificate of Consent

This section must be written in the first person. It should include a few brief statements about the research and be followed by a statement similar the one in bold below. If the participant is illiterate but gives oral consent, a witness must sign. A researcher or the person going over the informed consent must sign each consent. Because the certificate is an integral part of the informed consent and not a stand-alone document, the layout or design of the form should reflect this. The certificate of consent should avoid statements that have "I understand...." phrases. The understanding should perhaps be better tested through targeted questions during the reading of the information sheet (some examples of questions are given above), or through the questions being asked at the end of the reading of the information sheet, if the potential participant is reading the information sheet him/herself.

(This section is mandatory)

I have read the foregoing information, or it has been read to me. I have had the opportunity to ask questions about it and any questions I have been asked have been answered to my satisfaction. I consent voluntarily to be a participant in this study

**Print Name of Participant** \_\_\_\_\_

**Signature of Participant** \_\_\_\_\_

**Date** \_\_\_\_\_

**Day/month/year**

*If illiterate*<sup>5</sup>

**I have witnessed the accurate reading of the consent form to the potential participant, and the individual has had the opportunity to ask questions. I confirm that the individual has given consent freely.**

**Print name of witness** \_\_\_\_\_

**Thumb print of participant**

**Signature of witness** \_\_\_\_\_

**Date** \_\_\_\_\_

**Day/month/year**

**Statement by the researcher/person taking consent**

\_\_\_\_\_

<sup>5</sup> A literate witness must sign (if possible, this person should be selected by the participant and should have no connection to the research team). Participants who are illiterate should include their thumb print as well.

**I have accurately read out the information sheet to the potential participant, and to the best of my ability made sure that the participant understands that the following will be done:**

- 1.**
- 2.**
- 3.**

**I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability. I confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.**

**A copy of this ICF has been provided to the participant.**

**Print Name of Researcher/person taking the consent** \_\_\_\_\_

**Signature of Researcher /person taking the consent** \_\_\_\_\_

**Date** \_\_\_\_\_

Day/month/year

## B.3 Documentation of Consent

**Research participant's identity and the identity and dated signatures of the participant affirming that consent was given**

The information shown below identifying the participant should be entered in the designated spaces at the time of filling in the consent document together with the participant.

Participant's Name: \_\_\_\_\_

Participant's Birth Date: \_\_\_\_\_

Participant's Unique Reference Number: \_\_\_\_\_

### 3.2 Participant Consent Form

**Title of the experiment:**

\_\_\_\_\_

**Place of the experiment:**

\_\_\_\_\_

*This part will be filled in by the participant.*

*The original will be kept by the investigator; a copy will be given to the participant.*

	Please circle as appropriate	
I was informed about the effect to be expected, about possible disadvantages and about possible risks verbally and in writing by the test leader of the experiment.	Yes	No
I was informed about the purpose of research, the expected duration and the procedures verbally and in writing by the test leader of the experiment.	Yes	No
I was informed about any benefits to me or to others which may reasonably be expected from the research.	Yes	No
I was informed about the explanations on confidentiality (and limits) of	Yes	No

the data.		
I was informed about the right to decline to participate and to withdraw from the research once participation has begun and the foreseeable consequences of declining or withdrawing.	<b>Yes</b>	<b>No</b>
I was informed about whom to contact for questions about the research and research participants rights.	<b>Yes</b>	<b>No</b>
I have read and understood the written information handed out for the experiment mentioned above. My questions in connection with the experiment have been answered satisfactorily. I can keep the written information and receive a copy of my written declaration of consent.	<b>Yes</b>	<b>No</b>
I had sufficient time to take my decision.	<b>Yes</b>	<b>No</b>
In case an incident arises contrary to expectation, an insurance consists for me in the legally specified scale. The insurance was constructed by ..... for this experiment.	<b>Yes</b>	<b>No</b>
I have spoken to: Dr./Mr./Ms. ....		
I understand that I am free to withdraw from the experiment <ul style="list-style-type: none"> <li>◆ at any time</li> <li>◆ without having to give a reason for withdrawing</li> <li>◆ and without affecting my future medical care</li> </ul>	<b>Yes</b>	<b>No</b>
I agree to take part in the experiment.	<b>Yes</b>	<b>No</b>
The confidentiality of my personal data was assured to me. Personal data will be used anonymised at the publication of the experiment results. I approve of the fact however under a strict compliance with the confidentiality that the responsible experts of the authorities and the ethics commission may take a look for examining and control purposes of my original data.	<b>Yes</b>	<b>No</b>
If aftereffects appear, I will contact Dr./Mr./Ms.		

Signature .....

Date.....

Name (in capitals).....

## B.4 Informed Consent Documentation for an Illiterate Participant

I confirm that I was present when the trial was conducted with the participant ..... The participant has given oral informed consent to the following points:

- The purpose of the research, expected duration, and procedures;
- the possible risks, discomfort, adverse effects, and side effects (if any)
- a description of any benefits to the subject or to others which may reasonably be expected from the research
- confidentiality (and limits) of the data;
- Their right to decline to participate and to withdraw from the research once participation has begun and the foreseeable consequences of declining or withdrawing.
- Contact for questions about the research and research participants rights.

I think it is appropriate to conduct the trial with the participant .....

Witness's Name (in capitals): \_\_\_\_\_

Witness's Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## B.5 Informed Consent Concerning Private Information

This form will be used by all ACTIVAGE researchers who record private information in the course of any evaluation/pilots. It has to be **signed** by the investigator and by each participant. **One copy of the signed form has to be given to the participant.**

**Please clearly explain** to the participant how the following issues regarding privacy are handled related to the experiment at hand:

- What kind of data will be recorded, stored and why?
- Will the data be transferred?
- Data ownership?
- Is the data connected to other information?
- Will the data possibly be commercially exploited?
- Length of storage?
- Where will the data be stored, - according to which national legislation?
- Who will access the data?
- Who will supervise the data protection?

### **Investigator**

**Date** .....

**Name** (in capitals) .....

**Signature**.....

### **Participant**

**Date** .....

**Name** (in capitals) .....

All information mentioned in the shadowed box above has been given to me. I was able to fully understand all topics, ask questions and demand further clarifications. For the moment I have no additional questions; I fully understood that I may ask for additional information anytime in the course of the experiment.

**Signature**.....

# Appendix C Official Definitions / Principles applied

## From the Directive 95 / 46 / EC

### Article 2

#### Definitions

For the purposes of this Directive:

1. 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
2. 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
3. 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
4. '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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
5. 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
6. 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
7. 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
8. 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

### OECD privacy principles

We abide to the principles mention below:

#### Collection Limitation Principle

"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject".

The limits of the data collection – distinction between necessary and unnecessary data that will not be stored.

### **Data Quality Principle**

"Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date".

### **Purpose Specification Principle**

"The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose".

The purposes will be clearly explained to the participant; never later than during the informed consent process.

### **Use Limitation Principle**

"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance [Purpose Specification Principle] of the OECD Privacy Guidelines except:

- a. with the consent of the data subject; or
- b. by the authority of law".

Within ACTIVAGE personal data will solely be disclosed to other parties with the consent of the participant.

### **Security Safeguards Principle**

"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data".

We will meticulously protect the infrastructure, where personal data is being stored. The next chapter about Security issues within ACTIVAGE covers this topic.

### **Openness Principle**

"There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the Data Controller".

A task force related to privacy has been established. It will monitor current developments in this field. The nature of the personal data will constantly be scanned, also relating to the planned use. A list of data controllers will be posted.

### **Individual Participation Principle**

"An individual should have the right:

- a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

- b. to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- c. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".

Upon request one of the publicly posted data controllers will deliver the information recorded, if such information exists.

### Accountability Principle

"A Data Controller should be accountable for complying with measures which give effect to the principles stated above".

The data controllers will be accountable according to national law of the member states.

### Information about your Organisation and your Web Site

Providing visitors to your Web site with information about your organisation, and in particular about the legal entity which controls the processing of personal data, is consistent with the [Openness Principle](#) in the OECD Privacy Guidelines. Therefore, the information that you provide in this section will be disclosed in your privacy statement so that visitors to your Web sites will know who you are.

### Name of the Data Controller

An indication of the name of the data controller is required by the OECD Privacy Guidelines. According to the OECD Privacy Guidelines, " the Data Controller means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf". Therefore the "data controller" may be a legal or natural person, for example, a public authority, an organisation, a department within an organisation, a board of directors, or an individual.

### OECD - definitions

#### Specific Data

According to the OECD [Data Quality Principle](#), personal data should be relevant to the purposes for which they are to be used. In many countries, the personal data listed below are regarded as sensitive and their use restricted. If you collect and use personal data which fall into this category, you should consult the [Privacy Resource](#) (for example, the following instruments: Convention 108 of the Council of Europe, European Directive 95/46/EC and the UN Guidelines for the Regulation of Computerised Personal Data Files): Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Health/Medical data, Sex life, Police/Justice data such as civil/criminal actions brought by or against the visitor.

#### Consent

Seeking consent from visitors for disclosure of their personal data for new purposes accords with both the [Purpose Specification Principle](#) and the [Use Limitation Principle](#). The Purpose Specification Principle provides that the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. The Use Limitation

Principle develops this further by stating that personal data should not be disclosed, made available or otherwise used for purposes other than those specified. However, if you wish to use or disclose your visitors' personal data for an incompatible and unspecified purpose, you may do so provided that you have obtained consent of your visitors' before proceeding with the new use or disclosure.

### **Confidentiality/Security**

Establishing a security policy that protects personal data under your control is consistent with the [Security Safeguards Principle](#) of the OECD Privacy Guidelines.

The [Security Safeguards Principle](#) implies that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. The [2002 OECD Security Guidelines](#) also recommend that "security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency" under the Democracy Principle.

Security safeguards are intended to reinforce limitations on data use and disclosure. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasised that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality.

### **Secure Transmission Method**

For example, if you use an industry standard encryption technology for transferring and receiving personal data on your Web site(s).

### **Unauthorised Access**

For example, steps should be taken to ensure that only authorised staff have access to the data.

### **Improper Use or Disclosure**

For example, steps should be taken to ensure that the data are only used or disclosed for those purposes which were indicated to the visitor at or before the time of collection. Steps may also be taken to confirm the identity of individuals before providing a copy of their personal data to avoid the improper disclosure of one individual's personal data to another individual.

### **Unauthorised Modification or Alteration**

"Modified" should be construed to cover unauthorised input of data. Steps should be taken to ensure that the data are only altered/modified by authorised staff, and are not altered in such a way as would make the data inaccurate.

### **Unlawful Destruction or Accidental Loss**

"Loss" of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage medium. Steps should be taken to ensure that adequate security procedures are in place to prevent any person from either unlawfully (i.e. not in accordance with the data controller's instructions) or accidentally destroying and losing the data.

### **Data Processors**

Data Processors are third parties that process data on behalf of a [Data Controller](#) only for the completion of stated purposes, and who do nothing further with the data

### **Proof of Identity**

If you require proof of identity before providing an individual with information about the personal data you hold, or providing a copy of the personal data held, you may wish to indicate the proof you require in your privacy policy statement - for example, a password, confirmation of date of birth etc.

# Appendix D Template on Ethical and Legal issues per DS

## Questionnaire on Ethical and Legal issues

This is a template on ethical and legal issues that has to be completed by all partners who conduct pilots.

Questionnaire on ethical and legal issues: This questionnaire on ethical and legal issues has to be filled in by the responsible investigator conducting the trials involving human participants. It is a sort of a checklist reminding the researcher to take into account all relevant ethical aspects before planning and later on conducting any experiment within ACTIVAGE. The questionnaire itself divided into different subsections (e.g. informed consent, ethical control instruments, privacy, safety, risk assessment, etc.).

Please complete the questionnaire based on how you are planning to handle ethics related issues within ACTIVAGE project. Your answers will help shape the ACTIVAGE Ethics policies and your feedback will be used for the preparation of the ACTIVAGE Ethics Manual (D1.5).

## Data privacy and ethical issues

**1) Should all testing related activities be approved by an ethics controlling body in your country?**

- Yes  
 No

**2) Which is the ethics controlling body in your country?**

**3) Which is the procedure that should be followed?**

Provide the link or describe the procedure here.

**4) Is there any national legislation in application of AHA IoT practices in your country?**

- Yes
- No

If Yes, please describe:

**5) Are there any guidelines or legislation for the training of doctors who apply IoT in AHA practices?**

- Yes
- No

If Yes, please give details:

**6) In you country the doctors who apply IoT in AHA practices should be authorized by a legal authority?**

- Yes
- No

If Yes, please provide a brief outline of it:

**7) Is there any national legislation or law direction for the applying of medical devices to the patients?**

- Yes
- No

If Yes, please describe:

**8) Is there an ethics controlling committee for the organizations and hospitals who apply IoT practices?**

- Yes
- No

If Yes, please describe the procedure:

**9) Is there an established Data Protection Authority which should be followed?**

- Yes
- No

If Yes, please describe:

**10) Do you follow or are aware of any official national or international guidelines on protecting data privacy?**

- Yes
- No

If Yes, please provide a brief outline and references:

**11) Are there any national laws or legislation for protecting patient's information?**

- Yes
- No

If Yes, please give a brief outline of it:

**12) Access to health records and databases should be authorized by a legal authority?**

- Yes  
 No

If Yes, please give details about the procedure:

**13) Are patient data allowed abroad – country wise –?**

- Yes  
 No

**14) What is the patient data collecting system that is used in your country?  
(i.e. “elektronischer gesundheitskarte” in German, Kanta in Finland)**

## Participants and informed consent

**1) Do you intend to involve participants who might not understand the informed consent form?**

- Yes  
 No

If Yes, briefly explain the procedures you follow in order to obtain informed consent:

If No, please continue with the next question.

**2) Is there any doubt about the individual’s cognitive capacity to consent?**

Yes No

If Yes, briefly explain the procedures you follow in order to obtain informed consent:

If No, please continue with the next question.

**3) a) Is the informed consent provided in common language to be understood by “the man/woman in the street”?**

 Yes No

If No, why not? Please provide an example of any technical term that used within the description.

**3) b) Will the participant be given sufficient time to reflect their decision of giving or withholding consent?**

 Yes No

If No, why not? Please indicate the time given to the participant.

**4) Is the participant unable to consent for any reason not specifically listed in questions 1 to 3?**

 Yes No

If Yes, no experiment will be performed since these participants are excluded from ACTIVAGE trials.

If No, please continue with the next question.

**5) Does the participant included in research object in either words or body language or any physical action that can be interpreted to that end?**

Yes

No

If yes (he/she does object) no experiment will be performed since these participants are excluded from ACTIVAGE trials.

If No, please continue with the next question.

**6) a. Is the participant for any reason unable to read the form by themselves?**

Yes

No

If Yes, please continue with b). If No, please continue with the next question.

**b) There are a range of people who are unable to read the consent form; these include those who have severe visual impairments (e.g. cataract, glaucoma).**

**7) Is an oral consent of an illiterate participant that is witnessed in accordance with your national legislation?**

**8) Is there an international or national legislation, which you must follow when performing tests within the ACTIVAGE project?**

**a) Involving healthy human participants?**

- Yes
- No

If Yes, please give details (reference number and short description of procedure):

**b) Involving participants with cognitive impairments / learning difficulties?**

- Yes
- No

If Yes, please give details (reference number and short description of procedure):

**9) Involving illiterate or with co-morbid conditions participants?**

- Yes
- No

If Yes, please give details (reference number and short description of procedure):

## DS details

Country	Site partner	Ethics responsible	DS profile (all types of services in all sites)	DS participants (main targeted user groups)
			-	-
			-	-
			-	-
			-	-
			-	-
			-	-
			-	-
			-	-
			-	-
			-	-