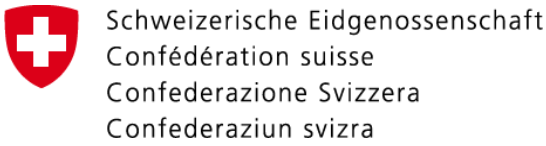
Deliverable 2.2 Ethical Methodologies

This project has been funded under the 2014 AAL call, AAL-2014-153



Document information

Document Properties	
Contract number	AAL-2014-153
Deliverable name	Ethical Methodologies
Deliverable number	D2.2
Status	Final
Version	1.0
Document responsible	EURAG Austria
Author(s)	Eva Reithner (EURAG), Stefan Kroll (TERZ)
Reviewer(s)	Eva Reithner (EURAG), Stefan Kroll (TERZ), Walter Colitti (MODO), Alberto Olliaro (UNIGE)
Dissemination level	Public
Contractual delivery date	Feb 2016
Delivery date	Feb 2016
Keywords	Ethics, Issues, Methodologies, Data protection, Consent

Contents

1. Introduction

Within the SmartHeat project there are many ethical, privacy, and usage issues related to the end user that may occur. All involved partners are responsible to identify and integrate ethical standards from the very beginning. These issues have to be addressed in a professional manner throughout all work.

This deliverable should provide the necessary guidelines in approaching the user studies for the execution of the SmartHeat project. User studies and the technical components designed/developed during the project will adhere to these guidelines to ensure that the necessary ethical considerations are met. There are three main objectives to be met through this deliverable. The first is to respect the privacy and intimacy of end users who are involved in the SmartHeat project. The second objective is to ensure the confidentiality of personal data that will be transmitted to external services; while the third is to achieve a high level of security regarding the potential risks and critical situations at home.

This document is the Ethical Guideline for the SmartHeat project. Based on international and national standards, it categorises three areas of ethical concerns within the execution of the project: privacy of end users, confidentiality of personal data, and security of usage in the home. These ethical issues are addressed and methods of prevention are provided.

1.1. Legal Responsibilities

The SmartHeat project will take into account all relevant ethical issues and will be compliant with the fundamental ethical principles in the use of personal data and in the involvement of human subjects in research activities. These principles take into account widely accepted national and international policies and regulations. The overwhelming themes to these policies are that participation must be voluntary and conducted in the safest possible way. Voluntary participation implies that the person(s) must not be coerced and shall enter into the project on their own accord. Once this takes place, it is upon the researchers to ensure that studies are conducted in a way as to not cause harm to the person(s) physically or mentally. Within social research, this risk is reduced greatly. However, each study should be fully evaluated beforehand to ensure that there is no risk of harm.

If at any point an ethical concern arises that is not mentioned in this document, it is the responsibility of the project partner to bring the issue to the attention of the project coordinator for an ethical review. The ethical situation in question will be

considered, keeping the fundamental rights in mind, and restructured where necessary to avoid any conflict.

1.1.1. International Policies and European Union Regulations

The aspect of ethics in research has come to light in the past 100 years. Many important historical events have lead to the need to protect the users throughout research endeavors. Such events resulted in many reports and guidelines, identifying issues to be considered when preparing for research with humans. One such document that greatly contributed to ethics in research involving humans is the Nuremberg Code of 1949. Within this document, 10 essential principles should be considered when conducting research with human participants.

1. Voluntary consent is essential.
2. Results of the research should be used to better society.
3. The study should be designed that the anticipated results justify the means.
4. Avoidance of all unnecessary physical and mental suffering and injury is essential.
5. No experiment should be conducted where there is a risk of death or disabling injury.
6. The degree of risk should never exceed that of the importance of the problem to be studied.
7. Facilities where the studies take place should be prepared in a way to eliminate even remote possibilities of injury, disability, or death.
8. Studies should only be carried out by responsible, qualified persons.
9. Participants must have the right to leave the experiment at any time.
10. Those conducting the study must be prepared to end the experiment at any time if there is reason to believe the continuation is likely to result in injury, disability, or death to the subjects participating in the study.

The Nuremberg code set the precedent for future research involving human participants. Ethical guidelines by many international institutions and organisations expand upon these 10 principles. The Declaration of Helsinki (1964); Food, Drug, & Cosmetics Act (1962); and many others have contributed to basic ethical guidelines in research with human subjects. The Belmont Report (1979) contributed to the standard of well-controlled studies, including respect for persons through the requirement for informed consent.

These reports, and many more, influenced the creation of general ethical principles. These are considered as fundamental rights in Europe and worldwide, such as protection of human dignity and human life, protection of personal data and privacy as well as the environment. SmartHeat partners will closely observe the Universal Declaration of Human Rights by the general Assembly of the United Nations (1948) Charter of Fundamental Rights of The European Union, published in the Official

Journal of the European Communities (2000/C 364/01), the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), the Handbook on European Data Protection Law (2013) and all legislative documents associated with the ongoing process of the EU data protection reform[1]. The values presented in these documents include, but are not limited to:

- Respect of Human Rights
- Freedom of research
- Physical and moral integrity of individuals involved
- Right for Private and Family Life
- Informed consent of participants
- Protection of personal data
- Freedom of thought, expression and information

1.1.2. National Laws and Regulation

In addition to the international standards, partners will act in accordance with community law as well as national conventions. The user studies will take place in Austria and Switzerland; those national laws apply. All partners will strictly adhere to the legal regulations and guidelines presented by the European Union and all participating countries. Below we identify national codes of conduct and laws for the protection of data, including all subsequent and future amendments that may apply. These also follow the European Data Protection Law (2013).[2]

The Data Protection Acts in each respective country, may differ slightly in their terminology, however they all provide the same fundamental rights to those participating in the SmartHeat project. These fundamental rights provide individuals with secrecy of the data concerning the individual and the right to rectification of incorrect data, so long as there are no issues overriding the interests of others. This follows the European Data Protection Law (2013).

Main ethical committees and regulatory organisations

1.1.2.1. Austria:

Authorities:

- Bundeskanzleramt: Österreichische Datenschutzkommission

Main regulations:

[1] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[2] http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

- Bundesgesetz über den Schutz personenbezogener Daten. Datenschutzgesetz 2000. BGBI. Inr. 165 del 17/8/1999 (Federal Law Gazette I No. 165/1999)[3]
- Datenschutzverordnung des. BPräs[4]: This legal ordinance controls basic principles on data investiga-tion and processing, data usage, its transmission and deletion.
- Informationssicherheitsgesetz[5]: This act regulates basic rights of data privacy and the duty to give information
- Wiener Antidiskriminierungsgesetz (LBI 35/2004)[6]: This act regulates the abatement of discrimination referring to the access to social, health and education as well as public services. It focuses on the non-discrimination and equal treatment regarding sex, age, disability, ethnic group, religion, ideology and sexual orientation

1.1.2.2. Switzerland:

Authorities:

- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (responsible for all issues regarding data security)
- Kantonale or eidgenössische Ethikkommission (competence depending on regional scope; must be informed and / or asked to state their opinion in cases in which sensitive medical data of identifiable testing persons shall be handed over to third persons)

Main regulations:

- Bundesverfassung, Art. 13 (Protection of privacy, including the protection of private and family life, home, mail and telecommunication, financial secrecy)
- Bundesgesetz über den Datenschutz (revised January 1, 2014)
- Verordnung zum Bundesgesetz über den Datenschutz (revised December 1, 2010)
- Schweizerisches Zivilgesetzbuch, Art. 28-28l
- Bundesgesetz über die Forschung am Menschen (Humanforschungsgesetz, HFG, revised January 1, 2014)

[3] Datenschutzgesetz 2000: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597

[4] Datenschutzverordnung des Bundespräsidenten: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000688

[5] Informationssicherheitsgesetz: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001740

[6] Wiener Antidiskriminierungsgesetz: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=LrW&Dokumentnummer=LWI40003262

2. Ethical Issues

2.1. Involvement of Human Participants

Human participants are integrated into the SmartHeat work to support the development of a successful SmartHeat system. This project follows a user-centered design approach and will focus on iterative involvement. Three specific areas of application that involve human participants are identified below.

User and Business Requirements

- User and Business requirements will be explored and evaluated qualitatively by running, e.g., workshops, interviews and surveys with human volunteers. Each method used will focus on a specific requirement aspect and/or need, identifying different areas of importance to potential users. Questionnaires will also be delivered to the potential end users, collecting additional quantitative data.

Intermediate User Evaluations

- User evaluations will be performed in, for example, workshops to discuss initial design sketches and identified services to be implemented. User studies will be conducted with the mobile lab equipment in the partner countries Austria and Switzerland. These evaluations will be used to assess all aspects relevant to the usability, e.g. handling, comprehensibility or accessibility of the initial SmartHeat system and gain first insights on user experience.

Closing Field Trials (Pilot Study)

- Completed in the homes of potential end-users, these field trials will be conducted in Austria and Switzerland with the objective to evaluate the user experience and acceptance of the developed SmartHeat system and related services (but also collect usability and accessibility issues). Secondary users can be involved as far as features of control by third persons are implemented and concerned. This may concern both the access of family members or any other close person caring for the end-users informally and professional service providers (e.g. mobile nurse services, personnel in sheltered housing) caring for the end-users at hand.

Applying a user-centered design approach means that the users' roles will be clearly defined at the beginning of the project. For example, users will provide information

on needs, interests, and preferences regarding heating, as well as opinions on and suggestions for the developed technical solutions within the design phase, and feedback on implementation functionality, usability, user experience and user acceptance, and proposed services of the SmartHeat system within the evaluation activities. The balancing act between the promotion of independence and the hazard of reducing personal freedom or self-control by use of technological innovation will be considered through intense consultation of the target groups. The meaning of autonomy and room for personal decisions on the part of the end-users will therefore extensively be considered.

The developed system will be mainly self-explanatory. In the situation when support is needed, SmartHeat partners involved in conducting the studies will explain a solution to the users. Considering that the target groups may be unfamiliar with the types of technology applied in the SmartHeat system and that the complexity of the design may go against full transparency from the users' perspective, extensive effort will be invested to make the technology as understandable as possible in order to create trust, accessibility and acceptability among all groups of users. This concerns both their direct involvement in the design process as well as ex ante instructions, explanations and continuous accessibility of support by the consortium.

There are three ethical objectives to meet throughout the project duration. These include privacy issues regarding those users involved in the execution of SmartHeat, data privacy with external services, and maintaining a high-level of security for use of SmartHeat in the home. These objectives will ensure that all areas where potential concerns may occur are covered and addressed for the protection of all end-users.

2.2. Privacy of End Users

Before each user study or inquiry, an informed consent will be presented to the participant which describes the objectives of the study or the inquiry, the ways of handling private information, and the associated risks, if any. The participants might also be asked for permission to record data on video/audio tapes or take photos. If the participant agrees with the terms of the informed consent, s/he will be asked to sign the form and are provided with a copy. The original informed consent form was written in German as the studies and inquiries are conducted within countries where German is the mother tongue (Austria, and Switzerland). A copy of the informed consent can be found in the Annex of this deliverable.

Participation in the user studies must be on a voluntary basis. Those individuals who volunteer to participate in these studies are told s/he is not obligated to answer the questions or do the tasks within the study and that s/he can withdraw at any point of

the study (i.e., exit rights and self-determination). The participants are also made aware of the information that is collected, stored, and processed during the user studies and the platform design. They will have the right to refuse the use of any information, which they may judge private or sensitive. At any point throughout the workshops, interviews, and evaluation methods, a participant has the right to stop the study and end their involvement.

Participants will not be put in prejudicial situations during observations, group discussions, or any user study. Researchers in the project will be very careful to explain the objectives of the study to the participants, to clarify what is expected from them, and what the future technology will be used for. After this explanation, a verbal response is requested from the participants and recorded during the interaction with the researchers. All study results, such as verbal protocols, videos, pictures, or statistical results will be anonymised (i.e., they will not contain personal information, only the age in years, if necessary). Researchers participating in the project will take into consideration any concerns about privacy and user acceptability of privacy violations, if any, that may arise into the design of the studies.

Within the project, we strive to work closely together with potential future user groups. To ensure this is done in an ethically adequate way, effort will be put into continuously and clearly inform users about the objective of the work, as well as their rights in the user studies (incl. the field trials). Participants will also be explained that they may or may not personally benefit from the future technology. This is to reduce too high of expectations study participants may have.

The pilot study will be limited to 2 month for the first iteration and 4 month for the second iteration in order to avoid dependency that may generate by use of the SmartHeat system by older adults. Additionally, special attention will be put on informing the older adults involved in the evaluation activities that they are testing a prototype and not a market-ready product.

Regular communication with participants of their rights in their participation will not only serve as a reminder and method of monitoring ethical considerations, but may also help to maintain the dignity of those involved. Preserving the dignity of participants strengthens the integrity of the study and ensures that those individuals remain as voluntary participants and are afforded all ethical considerations that have been set in both international and national communities.

2.3. Confidentiality of Personal Data and Protection

The following section defines the guidelines for the protection of personal and private information of study participants that will be followed in the SmartHeat project.

2.3.1. Use of Personal Data for Research

The next section specifies the guidelines for the collection, storage and erasement of private and personal data of study participants in the SmartHeat project.

2.3.1.1. Quality of Data

Data Collection: Personal data may be collected for processing, and undergoes such processing, only if the data is adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which the data is obtained.

Data Deletion: Personal data shall be erased when it has ceased to be necessary or relevant for its purpose for which it was obtained or recorded.

Research Subject Identification: Data shall not be kept in a form which permits identification of the data subject for longer than necessary for the purposes for which it was obtained or recorded.

Data Storage: Personal data shall be stored in a way which permits the right of access to be exercised, unless lawfully erased.

2.3.1.2. Right of Information about Personal Data Collection

Human individuals from whom personal data is requested must previously be informed explicitly, precisely and unequivocally about the following issues:

Existence of Data: The existence of a file for personal data processing, the purpose for collecting the data, and the recipients of the information.

Nature of Data: The obligatory or voluntary nature of the reply to any given question

Consequences of Data: The consequences for obtaining the data or for refusing to provide them.

Access to Data: The possibility of having the right to access, rectification, erasure and objection of personal data.

Transparency: The identity and address of the controller of the study or of his representative.

This information will be included in the SmartHeat Informed Consent that is attached in the annex section at the end of this deliverable.

2.3.1.3. Data Security

Within this study only employees of the respective organization that conducts the study will have access to the raw data.The person who processes personal data of study participants shall adopt the technical and organisational measures necessary to ensure the security of the gathered personal data and prevent their alteration, loss, unauthorised processing or access, having regard to the state of the art, the nature of the data stored and the risks to which they are exposed by virtue of human action or the physical or natural environment.
It is stated explicitly that data will be transferred from one to another within the consortium only after it was made anonymous.
No personal data of study participants shall be recorded in files which do not meet the conditions laid down by rules regarding their integrity and security, as well as the rules governing the processing centers, premises, equipment, systems and programs.

2.3.1.4. Duty of Security

The person who controls and any other person involved in any stage of processing personal data from study participants shall be subject to professional secrecy as regards such data and to the duty to keep them. These obligations shall continue even after the end of the relations with the owner of the file, or, where applicable, the person who is responsible for it.

2.3.1.5. Right of Access

Human individuals that participate in any study shall have the right to request and obtain free of charge information on his/her personal data subjected to processing, on the origin of such data and on their communication or intended communication.
The information may be obtained by simply displaying the data for consultation or by indicating the data subjected to processing in writing, or in a copy, fax or photocopy, whether certified a true copy or not, in legible and intelligible form, and without using keys or codes which require the use of specific devices.

2.3.1.6. Right of Rectification or Cancellation

The person who controls shall be obliged to implement the right of rectification or cancellation of the data subject within a period of ten days.

2.3.2. Data Storage and Handling

Research in SmartHeat revolves around information about persons – their age, lifestyle, health status, behaviors and other personal data – drawn from records,

scientific studies, surveys and interviews. In some cases, the information also reveals facts about relatives and relationships. These types of information are private and sensitive, although attitudes and expectations vary widely.
The protection of the privacy of participants is a responsibility of all persons involved in research with human participants. Privacy means, that the participant can control the access to personal information and s/he is able to decide who has access to the collected data in the future.
Due to the principle of autonomy the participants have to be asked for their agreement before private and personal information is collected (see Annex Informed Consent). It shall be ensured that all persons involved in research studies understand and respect the requirement for confidentiality. The participants should be informed about the confidentiality policy that is used in this research project.
Privacy plays a major role in the SmartHeat project and will be addressed as follows:

Publications: Hints to or specific personal information of any participant in (scientific) publications. It should be prevented to reveal the identity of participants in research deliberately or inadvertently, without the expressed permission of the participants.

Dissemination: Dissemination of data among partners. This relates to access to data, data formats, methods of archiving (electronic and paper), including data handling, data analyses, and research communications. Restricted access to private and sensitive information within the partner organisation must be guaranteed.

Protection: The organisation is responsible for the protection of the participants' privacy within the organisation (e.g. employers, etc.) throughout the whole SmartHeat project process like communications, data exchange, presentation of findings, etc.

Control: Furthermore, the participants have to be able to control the dissemination of the collected data. The investigator is not allowed to circulate information without anonymisation. This means that only relevant attributes, i.e. gender, age, etc. are retained. Another possibility is to keep the identity of the participants, but only with their prior consent.

Information: As already mentioned above, the protection of the confidentiality implies informing the participants about how their data may be dealt with (i.e. data sharing). 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.

2.3.3. Security Measures for Storage and Handling

Personal information storage, delivery and access procedure will be selected to be secure and the users' rights will be managed with the greatest care. In this way, there is complete guarantee that the accessed, delivered, stored and transmitted content will be managed by the entitled persons at the right time.

State of the art firewalls, network security, encryption and authentication processes will be used to protect collected data. Firewalls prevent the connection to open network ports, and exchange of data will only be done through consortium known ports. Where possible (depending on the facilities of each partner) the data will be stored in a locked server. All sensible data will be encrypted and protected during storage and process so that the user's identity and privacy will not be compromised as a result of the introduced technology. Context awareness technologies will also contribute to determine which content should be registered and which should not be annotated.

Data recorded on the gateway (temperature, humidity and presence) are.stored in pure text files. The gateway is protected from external access, it can be added only with credentials and the API is accessible via the HTTPS protocol which is the secure version of HTTP.

2.3.4. Enforcement within the Project

Data will be collected in research sites: at different locations, times and with different scopes; within surveys, interviews, experiments, test pilots, workshops, technical lab tests and evaluation studies. The collected data will be stored in a secure server, only visible to the research site network. Anonymous and identity data will be stored separately, and only the project leader will have access to the securely locked users' identities.

Anonymity will be guaranteed by separating identifiable data from anonymous data. Each user will get a unique identifier that will link one to the other, but only anonymous data will be available to researchers. If any identifiable data is required, access to it will be permitted only after explicit user permission and after agreement of the responsible data protection authority. The data will be saved for one year after the end of the project. After this time, each SmartHeat partner will be responsible for destroying the recorded personal data.

Authentication will be required to access stored data on the research site. Authorised researchers will have access to the recorded anonymous data after authentication. Researchers conducting studies will have access rights to add data to the identity database, synchronised with the writing of the anonymous data. No editing or reading rights will be granted to them to prevent alteration/disclosure of private user data. Collected data in the SmartHeat project will only be used for the purpose of the

project or study. A use of private user data outside of the project scope is not allowed.

2.4. Potential Risks and Critical Situations at Home

The project will specifically address ethical, privacy, and usage related issues related to the use of the SmartHeat system by the end user. Below are the planned approaches to reduce the risk of potential ethical violations after the completion of the project:

Modern Ambient Assisted Living (AAL) technologies, such as the solution developed in the SmartHeat project, offer a broad range of possibilities and opportunities for various markets and stakeholders.
The characteristics that are inherent to ambient technologies are specified by Aarts and Marzano[7] as following:

Embedded: Devices are networked and integrated into the environment
Context Aware: Devices are able to recognise people and their situational context
Personalised: Devices have the possibility to be tailored to individual personal needs. The service or technology can be adapted on the basis of this profile in such a manner that the service will be completely matched to the needs and preferences of a dedicated person.
Adaptive: Devices are able to adapt their behavior in reaction to changes in a person's behavior over time.
Anticipatory: Devices have the ability to anticipate the wishes of persons.

The following lines describe 13 risks of ambient technologies identified by Wright et al.[8] focusing on social, economic, legal, technological and ethical issues related to identity, privacy and security in Ambient Intelligence (AmI) environments. Find below a summary and short outline of the identified risks and how Smartheat will deal with the possible risks.

1. Privacy: It is important to be aware of the implications of AmI for private life and personal data and to take adequate social, technical, economic and legal measures to protect privacy.
Privacy in SmartHeat: Privacy in SmartHeat will be a concern since personal data of human subjects will be recorded during various evaluation studies and for the

[7] Aarts, E. and Marzano, S. (2003). The new everyday: views on ambient intelligence. 010 Publishers, Rotterdam,Netherlands, 2003

[8] Wright, David, Gutwirth, S.; Friedewald, M.; Vildjiounaite, E.; Punie, Y. (Eds.), Safeguards in a World of Ambient Intelligence, Springer, Dordrecht, 2010.

personalisation of the future SmartHeat system and services. Diverse coding and encryption strategies will be applied to safeguard and protect personal data of the involved human beings.

2. Security: Is another key challenge for a successful AmI implementation. Security issues can be depicted in the following contexts: security imposed for telework, biometrics used for authentication or identification, human factors and security, malicious attacks, security audits, back-up security measures, security risks, access control, the illusion of security and viruses.
Security in SmartHeat: Also security will be a concern in SmartHeat with a major focus on the co-text “access control of personal data”. SmartHeat will strive for password strategies and personalised access control mechanisms where users decide themselves who will have access to their personal data.

3. Identity: Different components of identity (i.e. information related to legal identity, identification, authentication, preferences, economic and financial information) play important roles in determining the feasibility of the AmI environment.
Identity in SmartHeat: The SmartHeat project will options so that individual preferences and other identity aspects can be integrated to form a general personal identity within the system and services.

4. Trust: The notion of trust has technical aspects as well as social, cultural and legal aspects. Trust can be raised in different contexts: Trust and confidence, lack of trust (from loss of control, unwillingness to provide some data, contextual misunderstandings) and honesty.
Trust in SmartHeat: Trust will be covered from different perspectives. During studies with active user involvement legal regulations from the involved partner countries will be followed next to general ethical key principles that define the protection of personal data. In addition written documents (Informed Consent) are applied that include basic information about the user rights and scope of the project and study. From a technical point of view encryption and password strategies will be applied to raise the trust in the security of the system.

5. Loss of Control: This risk of AmI stems from different factors, for instance, when there is a lack of trust on the part of the citizen/consumer in the AmI infrastructure and its components or a lack of skills on how to handle different devices (i.e. older persons). It can also emerge when the complexity level of AmI devices or services is too high and consequently does not enable users to get what they want.
Loss of control in SmartHeat: Several usability and user experience studies are planned to cover the possibilities of the elderly in handling the device and services in use.

6. Dependency: This risk emerges directly from the usage of a technology by the user and the prospects (benefits and alternative solutions) for the technology. Risky situations can be seen in dependence on personalised filtering, on seamless and ubiquitous communications, on AmI systems (e.g. health monitoring and traffic management systems) and users' feeling of dependence and frustration when the technology does not work as expected.
Dependency in SmartHeat: The system will always provide manual override, therefore preventing users' sense of abandonment in situation where the system is not working as desired.

7. Exclusion: Exclusion may be voluntary, for instance, when a user switches off, but usually it is outside people's own will. Equal rights and opportunities for all need to be built into the design of technologies since they are not achieved automatically. Exclusion can also be the result of lack of interoperability, denial of services, inadequate profiling, data mismatches or lack of data.
Exclusion in SmartHeat: Since the core of the project is on developing a solution that can be independently used with different devices (e.g., PC, mobile device) the project itself covers the aspect of interoperability and denial of services when using different devices.

8. Victimisation: Citizens have a democratic right not to be treated as criminals (unless they are criminals). Victimisation as an AmI impact describes a disproportionate reaction based on unfounded suspicions and emphasises the difficulty in being able to act anonymously.
Victimisation in SmartHeat: Victimisation will not play a role of concern since the system provided will not enable the user to start criminal actions.

9. Surveillance: Every citizen/consumer leaves electronic traces as the price of participation in the AmI society. These traces will make it possible to construct very sophisticated personal profiles and activity patterns. Although the justification for installing surveillance systems has a strong public interest, surveillance raises ethical, privacy and data protection issues. There is a clear need to delineate and define the boundaries between the private and public spheres.
Surveillance in SmartHeat: A surveillance/alarm system will be integrated. This function will only be available for private use and the connection with relevant others (secondary users) in cases of emergency. No public spheres will be integrated so boundaries will not have to be defined.

10. Identity Theft: Without appropriate security, the AmI environment may provide malicious persons many opportunities to steal identity information and to use it for criminal purposes. A new kind of crime is data laundering.

Identity Theft in SmartHeat: Advanced data protection strategies (encryption algorithms, passwords, firewalls, spam filters, etc.) will be applied to avoid unwanted access of (criminal) persons to personal data.

11. Malicious Attacks: Every new technology is plagued by known and/or unknown weaknesses, which threaten to serve as the backdoor for the risk of malicious attackers.
Malicious Attacks in SmartHeat: next to the data protection strategies mentioned above, the services will be installed on a controlled system to guarantee that no external access to personal user data will be possible for malicious attacks.

12. Digital Divide: AmI technology has the potential (because of its foreseen user friendliness and intuitive aspects) to bridge some aspects of the current digital divide, but this same tech-nology could also widen other aspects with regard to the risk of unequal access and use.
Digital divide in SmartHeat: The project strives for a reduction of the digital divide by making existing technologies available for senior citizens

13. Spamming: Spamming encompasses several risks such as profiling, disclosure of personal data and malicious attacks.
Spamming in SmartHeat: advanced spam filters data encryption and password strategies will be applied to guarantee that spamming and danger of malicious attacks will be reduced to a minimum.

In addition to issues and counters found in literature, there are some specific to the SmartHeat for which we need tailored solutions. Therefore not only all the building blocks will be designed taking into consideration the ethical issues mentioned in this document but also special attention will be given to those parts of the system that directly impact user's privacy and security on these matters:

- A secure login system will be included so that the user can interact with the system by providing his/her credentials. The authentication system will also allow the user to grant permissions to third party users. This permission rests on personal trust and can be revoked at any time by the primary user.
- The communication protocol will be selected with a security by design principle. Only protocols which have guaranteed encryption mechanisms will be taken into account.
- The system will include a gateway for the access to the Internet. The gateway introduces an extra layer of security. In addition, in case the user is not confident with the data storage on cloud based systems, the gateway can act as a local storage system and would exclude the need for a cloud based database.

3. Conclusion

This deliverable discusses ethical issues concerned with the execution of the SmartHeat project and will be updated as necessary. Issues primarily relate to the inclusion of humans during various studies and methods of evaluation of the system and aspects of data and privacy protection and will be addressed within the consortium. Three main topics were identified as respect the privacy and intimacy of end users involved, confidentiality of personal data transmitted to external services, and security regarding the potential risks and critical situations at home. To address these concerns, SmartHeat partners will ensure that all participation is voluntary and informed of the rights available when participating, including informed consent. In addition, safety measures will be taken in the design and function of the platform to protect the data of users with external services and potential risks of unconscious incurred costs.

4. Annex

- IC from Austria
- IC from Switzerland

5. References

Aarts, E. and Marzano, S. (2003). The new everyday: views on ambient intelligence. 010 Publishers, Rotterdam,Netherlands, 2003

Wright, David, Gutwirth, S.; Friedewald, M.; Vildjiounaite, E.; Punie, Y. (Eds.), Safeguards in a World of Ambient Intelligence, Springer, Dordrecht, 2010.

Reformed EU data protection rules, http://ec.europa.eu/justice/data-protection/reform/index_en.htm, 2012

European Union Agency for Fundamental Rights, Council of Europe – European Court of Human Rights, Handbook on European data protection law, 2014, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzgesetz 2000, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597, (last visit 2016)

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzverordnung des Bundespräsidenten, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000688, (last visit 2016)

Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Informationssicherheitsgesetz, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001740, (last visit 2016)

Bundesverfassung, Art. 13 (Protection of privacy, including the protection of private and family life, home, mail and telecommunication, financial secrecy)

Bundesgesetz über den Datenschutz (revised January 1, 2014)

Verordnung zum Bundesgesetz über den Datenschutz (revised December 1, 2010)
Schweizerisches Zivilgesetzbuch, Art. 28-28l

Bundesgesetz über die Forschung am Menschen (Humanforschungsgesetz, HFG, revised January 1, 2014)