Ambient Assisted Living Joint Programme

AAL JP project number: AAL-2011-4-099

Project acronym: ALICE

Project full title: Assistance for Better Mobility and Improved Cognition of Elderly Blind and Visually Impaired

D.1.4 Ethical and privacy guide

Deliverable Id :	D.1.4
Deliverable Name :	Ethical and privacy guide
Status :	Final
Dissemination Level :	Public
Due date of deliverable :	M9
Actual submission date :	M12
Work Package :	WP 1
Organisation name of lead contractor for this deliverable :	I&IMS
Author(s):	M. Cunill, A.Menéndez, Davorka Šel, Polona Car, Roger Wilson
Partner(s) contributing :	Consortium

Project funded by the AAL JP and the following national authorities:

REPUBLIKA SLOVENIJA MINISTRY OF EDUCATION, SCIENCE, CULTURE AND SPORT

ANR

GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Technology Strategy Board Driving Innovation

HISTORY

Version	*Date*	*Modification reason*	*Modified by*
0.1	15.11.12	TOC	Asier Menéndez
0.2	29.04.13	Contributions to TOC	Mònica Cunill
0.3	10.05.13	Contributions to TOC	Davorka Šel, Polona Car
0.4	10.05.13	Contributions to TOC	Roger Wilson
0.5	13.05.13	Final Document	Mònica Cunill
0.6	16.07.2013	Contributions to Final Doc	Andrei Bursuc
0.7	25.07.2013	FINAL DOCUMENT	Mònica Cunill

1 TABLE OF CONTENTS

2 EXECUTIVE SUMMARY

This document provides an Ethical Guideline and Data Protection Plan for the ALICE project. Relevant ethical aspects are highlighted in order to ensure that all the consortium partners will respect them.

In chapter 4, a brief summary about the ethical issues in the countries involved in the project is developed. Chapter 5 provides the official documents related to the project regarding ethical issues. Furthermore, a Data Protection Plan, which covers general issues about the anonymity procedure, data storage and handling process and procedures of data destruction, appears in Chapter 6. Finally, some conclusions are drawn in Chapter 7.

3 AIMS

The core of D1.4 is to create an Ethical and Data Protection Plan which compiles all the factors and considerations that should be taken into account, before starting and while different activities (especially those where humans are involved), are being carried out.

Personal data are those which enable to identify a person. With this plan, all issues regarding the treatment of personal data and public freedoms will be granted and guaranteed. Furthermore, it will ensure compliance with the ethical issues in relation to users' privacy, confidentiality, consent and respects the common values of autonomy, beneficence, non-malfeasance and justice during the whole project.

4 ETHICAL ISSUES MANAGEMENT IN EACH COUNTRY INVOLVED

4.1 GENERAL ETHICAL FRAMEWORK

Ethical aspects will not only affect the end-users participating in the project, but will also be considered relevant for the people and organisations participating in the project, and in general terms, will cover the limitations and regulations that must be applied to every project activity: research, development, testing, evaluation and dissemination.

People and organisations participating in the project will guide their activities by means of the following four principles:

1. Non malfeasance. The study and general operation of the device should not harm the participant or put him/her under unacceptable risk (this includes risks to privacy).

2. Beneficence. The study and general operation of the device should benefit the participant according to his/her own conception of the good.

3. Justice. The study and general operation of the device should take into account the legitimate interests of third parties and should not incorporate or promote any bias based on gender, culture, nationality, or other sources of social prejudice (this includes fair selection of the subjects for the user trials). Benefits of the study will be shared with the involved communities (this includes publication of the results of the study).

4. Respect for autonomy. With the general aim of promoting the participants' cognitive and functional abilities, participation in the study and in the general operation of the device should be based upon, a process of informed consent and right to control his/her personal information will be respected at all times (this includes issues of confidentiality and data security).

Data privacy refers to the evolving relationship between technology and public expectation and legal right of privacy in the collection and sharing of data. Privacy problems exist wherever uniquely identifiable data related to a person or group are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data that are affected by data privacy issues are:

- Health information.
- Criminal justice.
- Financial information.
- Genetic information.

- Location information.
- Cultural information.

The challenge to be faced according to data privacy is to share data while protecting the personal identity from the information [1].

Directive 95/46/EC defines personal data as “all information on an identified or identifiable person”, considering an identifiable person as anyone whose identity might be determined, directly or indirectly, in particular by means of an identification number or one or several specific elements, characteristics of his physical, physiological, mental, economic, cultural or social identity or other attributes with special protection to health data [2].

Privacy is important to participants since they expect to have the right to control and to inspect personal information, and they expect that their personal information maintained by colleges and centres will be accurate.

The European Charter of Fundamental Rights [3] states:

Art 3: Right to the integrity of the person

1. Everyone has the right to be respected for his/her physical and mental integrity.
2. In the fields of medicine and biology, the following issues must be respected particularly:
    - The free and informed consent of the person concerned, according to the procedures stated by law.
    - The prohibition of eugenic practices, in particular those related to the selection of persons.
    - The prohibition of making the human body and its parts as such a source of financial gain.
    - The prohibition of the reproductive cloning of human beings.

Art. 8: Protection of personal data

1. Everyone has the right of the protection of personal data concerning him/ her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him/her, and the right to rectify them.
3. Compliance with these rules shall be subject to control by an independent authority.

Art. 13: Freedom of the arts and sciences

The arts and scientific research shall be free of constraint. Academic freedom shall be respected.

The European Directive on the protection of personal data contains a number of key principles which must be complied with. Anyone processing personal data must comply with the eight enforceable principles of good practice, which are:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to countries without adequate protection.

4.2 NATIONAL LAWS

Research and development in the ALICE project will be conducted in Spain, Slovenia, France and UK. In addition, field testing and evaluation will be performed in UK and in Slovenia and further on, the data treatment will be done in Spain.

The European constitution recognises the fundamental right about the data protection and establishes that all the European countries will have an independent Authority which will guarantee this right. In the following sections, the laws concerning these issues from each testing and evaluating participant country will be exposed.

4.2.1 SPANISH LAWS

I&IMS will fulfil all the requirements stated by the *Spanish Organic Law 15/1999 of the 13th of December on the Protection of Personal Data (LOPD 15/1999)* [4] that intends to guarantee and protect the public liberties and fundamental rights of natural persons, and in particular their personal and family privacy, with regard to the processing of personal data.

The Organic Law shall apply to personal data recorded on a physical support which makes them capable of processing and to any type of subsequent use of such data by the public and private sectors.

With personal data, the Organic Law means "any information concerning identified or identifiable natural persons". Some important information regarding the LOPD 15/1999 that applies to ALICE project is summarized in several articles as follows:

Art. 4: Quality of the data

1. Personal data may be collected for processing and undergo such processing, only if they are adequate, relevant and not excessive in relation to the scope.
2. Personal data shall be erased when they have ceased to be necessary or relevant for the purpose for which they were obtained or recorded.
3. They shall not be kept in a form which permits identification of the data subject for longer than necessary for the purposes for which they were obtained or recorded.
4. Personal data shall be stored in a way which permits the right of access to be exercised, unless lawfully erased.

Art. 5: Right of information in the collection of data

1. Data subjects from who personal data are requested, must previously be informed explicitly, precisely and unequivocally of the following:
    - The existence of a file of personal data processing operation, the purpose of collecting the data, and the recipients of the information.
    - The obligatory or voluntary nature of the reply to the questions put to them.
    - The consequences of obtaining the data or of refusing to provide them.
    - The possibility of exercising rights of access, rectification, erasure and objection.
    - The need of the identity and address of the controller or of his/her representative, if any.

Art. 9: Data security

1. The controller or, where applicable, the processor shall adopt the technical and organizational measures necessary to ensure the security of the 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.

2. No personal data 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 centres, premises, equipment, systems and programs.

Art 10: Duty of secrecy

1. The controller and any persons involved in any stage of processing personal data 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 responsible for it.

Art. 15: Right of access

1. The data subject shall have the right to request and obtain free of charge information on his personal data.

2. 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.

Art. 16: Right of rectification or cancellation

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

4.2.2 SLOVENIAN LAWS

Protection of personal data in Slovenia is guaranteed by the Constitution of the Republic of Slovenia, Art. 38. This article defines the use of personal data contrary to the purpose for which it was collected. The collection, processing, purpose of use, supervision and protection of the secrecy of personal data shall be provided by statute. Everyone has the right of access to the collected personal data related to him/her and the right to judicial protection in the event of abuse of such data. Detailed provisions of data protection are given in the Personal Data Protection Act.

Thus Slovenian partners (ALP, Comland and UBPS) will comply with the provisions of the Personal Data Protection Act of the Republic of Slovenia (Official Gazette of the Republic of Slovenia, 94/2007, 26. October 2007, PDPA).

Personal data defined by the PDPA is any data relating to an individual, irrespective of the form in which it is expressed, where individual is defined as an identified or identifiable natural person to whom personal data relates; an identifiable natural 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/her physical, physiological, mental, economic, cultural or social identity, where the method of identification does not incur large costs or disproportionate effort or require a large amount of time.

The institution responsible for supervision over the implementation of the provisions of PDPA is the Information Commissioner; whose task it to handle cases of complaints, appeals, notifications and other applications, explaining possible breach of law. It also issues supervision measures based on Art. 54 of PDPA - prohibition to process personal data, anonymity, blocking, erasing or destroying personal data, when established that the data is not processed according to the law.

Most important Articles from PDPA related to the ALICE project are listed below:

Article 8: Legal grounds and purposes

1. Personal data may only be processed if the processing of personal data and the personal data being processed are provided by statute, or if the personal consent of the individual has been given for the processing of certain personal data.

2. The purpose of processing personal data must be provided by statute, and in cases of processing on the basis of personal consent of the individual, the individual must be informed in advance in writing or in another appropriate manner of the purpose of processing of personal data.

Article 16: Purpose of collection, and further processing

Personal data may only be collected for specific and lawful[1] purposes.

Article 17: Processing for historical, statistical and scientific-research purposes

1. Irrespective of the initial purpose of collection, personal data may be further processed for historical, statistical and scientific-research purposes.

2. Personal data shall be supplied to the data recipient for the purpose of processing from the previous paragraph in an anonymized form, unless the individual, to whom the personal data is related to, gives prior written consent for the data to be processed without anonymized.

3. Personal data supplied to data recipient in accordance with the previous paragraph shall on completion of processing be destroyed, unless otherwise provided by statute. The data recipient shall be obliged without delay after destruction of the data to inform the data controller who supplied him the personal data in writing when and how he destroyed them.

4. Results of processing from the first paragraph of this Article shall be published in anonymized form, unless otherwise provided by statute or unless the individual to whom the personal data relate gave written consent for publication in a non-anonymized form or unless written consent for such publication has been given by the heirs to the deceased person under this Act.

[1] Provided for by statute (a general act of Parliament).

Article 19: Informing the individual of the processing of personal data

1. If personal data are collected directly from the individual to whom they relate, the data controller or his representative must communicate to the individual the following information, if the individual is not yet acquainted with them:

    - Data on the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively).

    - The purpose of the processing of personal data.

2. If in view of the special circumstances of collecting personal data from the previous paragraph there is a need to ensure lawful [2] and fair processing of personal data of the individual, the person from the previous paragraph must also communicate to the individual the additional information, if the individual is not yet acquainted with them, and in particular:

    - A declaration as to the data recipient or the type of data recipients of his personal data,

    - a declaration of whether the collection of personal data is compulsory or voluntary, and the possible consequences if the individual will not provide data voluntarily,

    - information on the right to consult, transcribe, copy, supplement, correct, block and erase personal data that relate to him.

Article 21: Duration of storage of personal data

1. Personal data may only be stored for as long as necessary to achieve the purpose for which they were collected or further processed.

2. On completion of the purpose of processing, personal data shall be erased, destroyed, blocked or anonymized, unless pursuant to the statute governing archive materials and archives they are defined as archive material, or unless a statute otherwise provides for an individual type of personal data.

Article 24: Security of Personal Data

1. Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data by:

    - Protecting premises, equipment and systems software, including input-output units;

[2] Verbatim: statutory (in accordance with a statute, meaning mostly in accordance with this Act).

- Protecting software applications used to process personal data;
- Preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
- Ensuring effective methods of blocking, destruction, deletion or anonymization of personal data;
- Enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

Article 30: Right of the individual to information

1. Data controller shall on request of the individual be obliged to:

   - Enable consultation of the filing system catalogue;
   - Certify whether data relating to him are being processed or not, and to enable him to consult personal data contained in filing system that relate to him, and to transcribe or copy them;
   - Supply him an extract of personal data contained in filing system that relate to him;
   - Provide a list of data recipients to whom personal data were supplied, when, on what basis and for what purpose;
   - Provide information on the sources on which records contained about the individual in a filing system are based, and on the method of processing.
   - Provide information on the purpose of processing and the type of personal data being processed, and all necessary explanations in this connection;
   - Explain technical and logical-technical procedures of decision-making, if the controller is performing automated decision-making through the processing of personal data of an individual.

Article 32: Right to supplement, correct, block, erase and to object

1. On the request of an individual to whom personal data relate, the data controller must supplement, correct, block or erase personal data which the individual proves as being incomplete, inaccurate or not up to date, or that they were collected or processed contrary to statute.

2. On the request of the individual the data controller must inform all data recipients and data processors to which the controller has supplied the personal data of the individual, before the measures from the previous paragraph have been carried out, of their supplementation, correction, blocking or erasure pursuant to the previous paragraph. Exceptionally the data

controller shall not need to do this if it would incur large costs, disproportionate efforts or would require a large amount of time.

In addition, the Slovenian partners will take into account some of the basic principles of the Ethical Code, applicable for Social protection field.

Ethics – the basis of the conduct

The partners adhere to the principles of ethics in order to protect end-users with whom they work and themselves against misuse of professional and social power. Their work should be distinguished from political, religious, ideological, personal and institutional influences and interests that might interfere with their human and professional judgment.

Respect human rights and freedoms

Partners comply with all the laws and Constitution of the Republic of Slovenia and the rights guaranteed by the all international documents on human rights, which Slovenia has adopted or ratified.

Respect for human dignity and uniqueness

In the process of working with end-users, partners, protect the dignity, privacy, autonomy and individuality of each person; they take into account the culture and social background and adjust the language and the level of communication to each individual. Partners obtain very confidential information about the participants, thus they are obliged to protect any confidential information as a professional secret.

Criteria of public communication

Partners should protect individuals from improper handling and possible misuses of the media and the public. Information must protect the privacy and the benefits of the end-users.

Prevention of personal harassment and violence

In all processes partners protect sexual, physical, mental, and spiritual integrity of individuals.

Data protection

End-users information must be protected as a professional secret.

4.2.3 UK LAWS

Concerning personal data,UK laws are based on the Protection Act of 1998 (DPA) which is the main piece of legislation that governs the protection of personal data in the UK. With accordance to this law, UK partners within Alice project will fulfil the following conditions:

1.

2. Partners will be in regular contact with the survey participants for the duration of the Alice project.

3. The personal information of the participants will not be released outside the project partnership.

4. In addition, the names and addresses of participants will not be disclosed to partners, who will only receive a code relating to each participant.

Furthermore, there are some guidelines laid down by the UK government and the Information Commissioner's Office (ICO) who states that those businesses who hold some personal data (for example about customers or employees) are referred to as 'data controllers'. According to the data controller obligations, the Protection Act states that:

1. Personal information must be processed fairly and lawfully. In order to comply, the entity must provide individuals with the name of the business and with other details of the purpose for which their information will be used. You should make clear that the individual can access and correct the information. Crucially, the entity must also expose them if the information will be used in any way that is not immediately obvious. For example, the entity must tell the individual if their details will be passed on to credit reference agencies or be processed for specified lawful purposes. Furthermore, the entity must have a specified, lawful reason for collecting data. Furthermore, the entity cannot use the data collected for another, "incompatible" or unlawful purpose. The data must be adequate, relevant and not excessive and it should only collect the bare minimum; the entity may not collect information that is not immediately relevant to the specified purpose, and it may not collect more information than needed. Any information must be factually accurate, and updated where necessary. Depending on the nature of the business, the entity may need to develop mechanisms that allow individuals to update their details quickly, not be kept for any longer than is necessary.

2. If the purpose for which the entity collects the data is time-limited, it must ensure that it is not retained once it is no longer needed. Where applicable, the entity should tell individuals how long the data is likely to be retained for.

3. The Act sets out the rights of individuals, as well as the responsibilities of data controllers. The entity should make sure that it understand these rights, and act in accordance with them.

4. The entity must take adequate steps to ensure the security of the data. This means that it should be safe from tampering, loss, or unlawful processing. It may need to develop both technical and organisational processes. Data must not be transferred outside the European Economic Area without adequate protection and may only be transferred out of the EEA if the country to which it is being transferred has adequate legal protection for individuals and their details.

The Act works on the basis that all data controllers are required to notify the ICO of its' activities, but some exemptions are available. If the entity is not exempt but it fails to notify the ICO, it risk prosecution. The may be exempt from the notification requirement if it only process data for the purposes of: staff administration; payroll; advertising, marketing and PR that are directly related to its' own business activities.

4.2.3 FRENCH LAWS

The principal law regulating data protection in France is Law No. 78-17 of 6 January 1978 on data processing, data files and individual liberties, as amended (DP Law). Directive 95/46/EC on data protection (Data Protection Directive) was implemented through Law No. 2004-801 of 6 August 2004, which amended the DP Law Decree No. 2005-1309 of 20 October 2005 implements certain sections of the DP Law.Violations of the DP Law can be prosecuted under, among others, Articles 226-16 to 226-24 of the Criminal Code.

The confidentiality obligations that regulate personal data processing and concern the ALICE project partners, include the:

- Public Health Code, for example, Articles L. 1110-4, L. 1111-8, L. 1112-3, L. 1121-3, L. 1142-24-4, L. 1343-3, and L. 2132-1.
- Laws that do not directly relate to data privacy that can impact personal data processing in some circumstances, such as Article 9 of the Civil Code that is the basis for the right to privacy of all natural persons (including employees).

The DP Act applies to data controllers and data processors (*Articles 3 and 35, DP Act*).

A data controller is a person, public authority, department or any other organisation who determines the purposes and means of the data processing, unless expressly designated by legislative or regulatory provisions relating to the data processing in question (*Article 3, DP Act*). A data processor is any person who processes personal data on behalf of the data controller (*Article 35, DP A*ct).

The DP Act regulates personal data. Personal data is any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him (*Article 2, DP Act*). To determine whether a person is identifiable, all means that the data controller, or any other person, uses or may have access to should be taken into consideration.

The DP Law applies to:

- Automatic processing of personal data.
- Non-automatic processing of personal data that is or may be contained in a personal data filing system, except for processing carried out to exercise exclusively private activities.
- The processing of personal data by a data controller that is established in France or carries out its activity in France in an establishment, whatever its legal form.
- A data controller that, although not established in France or in any other EU member state, uses means of processing located in France, except for processing only for the purposes of transit through France or any other EU member state.

4.2.3.1 MAIN DATA PROTECTION RULES AND PRINCIPLES

MAIN OBLIGATIONS AND PROCESSING REQUIREMENTS

All personal data must be (*Article 6, DP Act*):

- Processed fairly and lawfully.

- Collected for specific, explicit and legitimate purposes, and subsequently processed in accordance with these purposes.
- Collected in an adequate, relevant, and non-excessive way, in view of the purposes for which it is collected.
- Accurate, comprehensive and, when necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected, or for which it is further processed. Personal data can only be stored beyond this necessary period for processing for historical, statistical or scientific purposes.

In addition, data subjects must be given specific information about the processing of their personal data at the time such data is collected or, if data is disclosed to a third party, at the time the data is disclosed to that third party. As a general rule, all such information must be in French (*Law No. 94-665 of 4 August 1994*).

Consent may also be required. The consent of data subjects is required before processing personal data, unless an exception applies (*DP Law*). Online consent will suffice.

Implied consent of the data subject is sufficient for processing personal data, unless special rules apply. Under the DP Law, express consent of data subjects is required for:

- Any processing of sensitive data, unless an exception applies.
- Medical research requiring the collection of biological sample identifiers.

Express consent may be required under other legislation (for example, for other types of medical research under the Public Health Code).

SPECIAL RULES

Certain processing can only be carried out after prior authorisation has been granted by the National Data Processing and Liberties Commission - *Commission Nationale de l'Informatique et des Libertes (*CNIL). This includes:

- Processing genetic data.
- Processing, whether automatic or not, data relating to offences, convictions or measures restricting personal liberty.
- Processing that may, due to its nature, importance or purposes, exclude persons from the benefit of a right, service or contract, in the absence of any legislative or regulatory provision.

Sensitive data is defined as data that reveals, directly or indirectly, the data subject's (*Article 8, DP Act*):

- Racial or ethnic origins.
- Political, philosophical or religious opinions.
- Trade union affiliation.
- Health or sex life.

The collection and processing of sensitive data are prohibited unless one of the following applies (*Article 8, DP Act*):

- The data subject has given express consent.
- The processing is necessary to protect human life and the data subject is unable to give his consent.
- The processing relates to personal data made public by the data subject.
- The processing is necessary to establish, exercise or defend a legal claim.

In addition, if sensitive data is, within a short period of time, to be made anonymous using a procedure approved in advance by the CNIL, the CNIL can authorise certain categories of processing, by taking into account its purpose.

Further, sensitive data processing is not prohibited if it is both:

- Justified by the public interest.
- Authorised by the CNIL or by a decree of the Supreme Administrative Court after a published opinion of the CNIL.

RIGHTS OF INDIVIDUALS

The data controller must provide, at the time data is collected, information regarding (*Article 32, DP Act*):

- The identity of the data controller and its representative, if any.
- The purposes of the data processing.
- Whether providing each type of data is compulsory or optional.
- The possible consequences of failing to provide data.
- The recipients or categories of recipients of the data.
- The rights of individuals to access, correct or delete data and to oppose data processing.
- Whether data is to be transferred outside the EU, and in that case, specific details regarding the conditions of transfer.

Data subjects are entitled to obtain from the data controller (*Article 39, DP Act*):

- Confirmation as to whether their data is being processed.
- Information relating to the purposes of the processing, the categories of processed personal data and the recipients or categories of recipients to whom the data are disclosed.
- If applicable, information relating to transfer of the personal data outside the EU.
- A copy, in an accessible form, of their personal data, as well as any available information on the origin of the data.
- Information allowing data subjects to know and object to the reasoning involved in the processing, where a decision taken based on automatic processing produces legal effects in relation to the data subject.

Data subjects can ask the data controller to, as the case may be, rectify, complete, update, block or delete their personal data that is:

- Inaccurate.
- Incomplete.
- Equivocal.
- Expired.
- Prohibited from being collected, used, disclosed or stored.

SECURITY REQUIREMENTS

The data controller must take all useful precautions, in relation to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent its alteration or damage, or access by unauthorised third parties (*Article 34, DP Act*).

The CNIL has issued recommendations on how to maintain a proper level of security, in particular:

- Adopt a strong password management policy.
- Set up a process for the creation and deletion of user accounts.
- Secure workstations.
- Identify exhaustively who may have access to the data.
- Ensure confidentiality of data in relation to suppliers.
- Secure the local network.
- Secure the physical access to the premises.
- Anticipate the risks of loss or disclosure of data.
- Adopt an information systems (IS) security policy.
- Train users on information technology (IT) risks.

4.2.3.2 INTERNATIONAL TRANSFER OF DATA

TRANSFER DATA OUTSIDE THE JURISDICTION

Data controllers cannot transfer personal data outside the EU unless the country where the recipient is located provides an adequate level of protection of the individual's privacy, liberties and fundamental rights, relating to the actual or possible processing of his personal data, as determined by the European Commission (Commission).

If the transfer does not provide this adequate level of protection, it requires prior authorisation from the CNIL, based on:

- A data transfer agreement between the data exporter and data importer, identical to the EU model clauses.
- Binding corporate rules.
- An ad hoc data transfer agreement.

In addition, data controllers can transfer personal data to a country not providing an adequate level of protection if the data subject has expressly consented to their transfer, or if the transfer is necessary to do any of the following:

- Protect the data subject's life.
- Protect the public interest.
- Satisfy obligations ensuring the establishment, exercise or defense of legal claims.
- Perform a contract between the data controller and the data subject, or to take pre-contractual measures in response to the data subject's request.
- Conclude or perform a contract, in the interests of the data subject, between the data controller and a third party.

However, the CNIL strongly discourages reliance on data subject consent, or one of the exceptions listed above, to legitimise a transfer of data outside the EU.

5 ETHICAL DOCUMENTS

A consent letter which contains full information about the research in which the participant is going to participate and that will compile all the acceptance of participants will be developed. This document originates from the legal and ethical right that exposes that the participant has to know directly what will happen to his / her personal data.

Once the participant has been provided of the letter and has signed it (by him/her or by its' legal representative), he/she will send it to the researcher. The ALICE participants have the cognitive capabilities preserved, so they will sign the consent by themselves.

The information given to the participant or the representative will be in understandable language to the participant or the representative person. No informed consent, whether oral or written, may include any exculpatory language through which the participant or the representative is made to waive or appear to waive any of the participant's legal rights, or releases or appears to release the researcher, the sponsor, the institution or its agents from liability for negligence.

Also, appropriate and adequate information (e.g. the nature, duration, and purpose of the experiment; the method and means by which it will be conducted; any inconveniences and hazards reasonably to be expected; the effects upon his/her health, and that he/she may quit the testing at any point) shall be given in order to ensure informed consent.

The aim of this document is to provide the necessary information about the study in order to guarantee that the participant has enough information about the study and she/he can take the adequate decision about her/his participation on it. The document summarizes the main information with regard to the project: objectives, methods, participants, etc.

A sample of this letter can be found in Annex I.

6 DATA PROTECTION PLAN

For ALICE purposes, the way of collecting data to be carried out will be the collection of personal data. We have therefore analysed these aspects of data collection, studying the legislation in Europe as well as specifically in each involved country, and proposing a data protection plan that aims to cover all the cited aspects. This plan is presented below.

6.1 GENERAL ISSUES CONCERNING DATA PROTECTION PLAN

The data protection plan becomes part of the signed agreement between ALICE consortium and the investigator(s) participants in the project. If the agreement is executed, all members of the research team with access to the data are contractually obligated to follow all aspects of the data protection plan. The fundamental goal of the protections outlined in this plan is to prevent persons who are not signatories to the restricted data use agreement or the supplemental agreement with research staff from gaining access to the data.

The data protection plan applies to both, the raw data file received from ALICE consortium as well as any copies made by the research team, and any new data derived solely or in part from the raw data file. The plan should also address on how computer output derived from the data will be kept secure. This applies to all computer output, not only direct data listings of the file.

6.2 LETTER OF CONSENT

Explained in Section 5.

6.3 DATA STORAGE AND HANDLING PROCESSES

The protection of the privacy of participants is a responsibility of all people involved in research with human participants. Privacy means that the participant can control the access to personal information; he/she decides 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 (informed consent) before private information can be collected. It should be also ensured that all the persons involved in research work, understand and respect the requirement for confidentiality. The participants should be informed about the confidentiality policy that is used in the research.

The privacy plays a role at different levels:

- Hints to or specific personal information of any participant in publications.
- It should be prevented to reveal the identity of participants in research deliberately or inadvertently, without the expressed permission of the participants.
- Dissemination of data among partners.

- Access to data method of access, data formats, method of archiving (electronic and paper), including data handling, data analyses, and research communications. Offer restricted access to privacy sensitive information within the organization of the partner.
- Protection of the privacy within the organization of volunteers (employers, etc.) throughout the whole process like, communications, data exchange, presentation of findings, etc.
- Destruction of data once the purposes for which the data were obtained is over.

Furthermore, the participants have to be able to control the dissemination of the collected data. The investigator is not allowed to circulate information without anonymity. 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 prior consent of those.

As already mentioned, protection of confidentiality implies informing the participants about what may be done with their data (i.e. data sharing). As databases are developed, confidentiality will become increasingly hard to maintain.

6.4 PROCESS OF DATA DESTRUCTION

During the data collection, it needs to be clear that any personal data gathered from the persons participating in the project are relevant and as less as necessary for the successful development of the relevant purposes of the project. However, in this process of data collection, special needs may rise up that require collection of sensitive information when it comes to train or improve a technological device relevant for the project.

Specific measures will be developed and are recommended for all the partners:

- Dissociation of personal identifiable data as it was specified in section.
- Destruction of paper/documents with a paper destroyer after 5 years the project ends.
- Erasing of electronic documents containing personal data after 5 years the project ends.

7 CONCLUSIONS

The importance of protecting private data is an important issue to take into consideration while the development of the ALICE proposal in order to enforce the law. For achieving this purpose, an Ethical Guideline and Data Protection Plan has been developed in order to ensure that all consortium partners have respected and will respect ethical aspects throughout the project and that they will guide their activities by means of four main principles which are: Non malfeasance, beneficence, justice and respect of autonomy.

However, ethical aspects will not only affect the end-users who will participate in the project, but will also be considered relevant for the people and organisations participating in the project, and in general terms, will cover the limitations and regulations that must be applied to every project activity: research, development, testing, evaluation and dissemination.

The data protection plan applies to the raw data file received from ALICE consortium as well as any copies made by the research team, and any new data derived solely or in part from the raw data file. The plan also addresses on how computer output derived from the data will be kept secure. This applies to all computer output, not only direct data listings of the file.

This ethical guide has taken into consideration not just European laws, but also national laws and decrees. An exhaustive analysis of then has been carried out and integrated in a single document (the present), which is a living document which will be constantly consulted and taken into consideration throughout the whole document in order to achieve compliance with the ethical issues in relation to users' privacy, confidentiality, consent and respect of all the participants of the project.

8 REFERENCES

[1] European Commission: Ethics for researchers, Facilitating research excellence in FP7.

[2] Directive 95/46/EC. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[3] Charter of Fundamental Rights of The European Union. 2000/C364/01. Official Journal of the European Communities 18 December 2000.

[4] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de CarácterPersonal (BOE núm. 298, 14-12-1999, pp. 43088-43099) [Organic Law, 15/1999, for Protection of Data of Personal Nature, Text in Spanish].

[5] Constitution of the Republic of Slovenia. 33/1991. Official Gazette of the Republic of Slovenia 28 December 1991.

[6] Data Protection Act. 94/2007, 26. Official Gazette of the Republic of Slovenia 16 October 2007, PDPA).

[7] Ethical code. 59/2002. Official Gazette of the Republic of Slovenia 5 July 2002.

[8] Great Britain *Data Protection Act 1998. Part II*. London: HMSO.

A. ANNEX

ANNEX I.CONSENT LETTER

LETTER OF CONSENT

- SAMPLE

Dear participant,

You are being invited to participate in a project called ALICE. ALICE is an international project with different partners from France, United Kingdom, Spain and Slovenia. The project's purpose is to improve the quality of life of ageing people with impaired vision by providing an intelligent navigational assistant.

The navigational assistant will be able to offer visually impaired users an understanding of what is around them based on information from several sensors within the device. The ALICE project is combining research developments in cognitive sciences, psychology, computer vision, artificial intelligence and robot navigation.

ALICE will consist of a smartphone wirelessly connected to remote processing unit. As well as the camera, ALICE will utilise sensors for position detection, orientation, movement and distance from obstacles. The position and distance mapping will be cross-referenced and processed in combination with the visual information, so as to avoid confusion and misunderstanding. ALICE will use artificial intelligence to plan and anticipate based on bringing together all the information from sensors and combining it with previous knowledge. The system will deliver the information from the sensors as sounds and words via a synthetic voice. You will be able to communicate with the system via voice input, by talking to ALICE.

The project itself will last for 30 months. During this time, you will be interviewed about your requirements to inform the development of the project. The interview will be conducted wherever you prefer (e.g. in your home).

In the next phase, you will be requested to participate in testing of the device. Because of safety concerns, the testing of the system will be divided into three consecutive phases:

1. **Phase 1:** Requirements collection. The first step for the user requirement data collection is to develop a questionnaire in order to obtain users preferences to guide the developers to design and adapt the ALICE platform
2. **Phase 2:** Initial trial and iterations. The system will first be tested as a virtual model where possible collision situations can be simulated thus checking for flaws in the interpretation of the environment. You will not participate in testing scenarios at this stage as the tester should be able to correct decisions of the system.
3. **Phase 3: Final trial.** A 'Man behind the curtain' testing methodology will be utilized in the later stages of testing, when you will be participating in the device evaluation.

The researchers and developers of the ALICE project will not put you at risk at any stage of the project and will respect the fundamental ethical principles included in the Charter for Fundamental Rights of the European Union.

Several steps will be taken to protect your anonymity and identity. The typed interviews or any other document will NOT contain any mention of your name, and any identifying information will be removed. A unique numbered code will be used rather than names or other personal details. All the research material will be stored in a secured location within the participant organisations and the procedures for sharing information subject to a confidentiality and data security policy. Data will not be available on the Internet and staff involved in the project will need a password to access a data base.

Your participation in this research is completely voluntary and your expenses will be covered. However, you may withdraw from the study at any time for any reason.

The results from this project will be presented to the world in different ways, in the form of newspaper and scientific articles, photographs, videos or on different web pages including our project web page. We will present our work to conferences and seminars.

However, at no time will your name be used or any identifying information revealed. Any photograph or video will only be used, if you provide permission.

Should you require any further information about this project, please do not hesitate to contact us: (e.g.: UBPS in Slovenia or COMBD in the UK).

I have read the above information regarding the ALICE project and consent to participate in this project.

Printed Name:_____

Signature:_____

Date and place: _____

Notes:

The Informed Consent Discussion with Legally Blind Subjects

If you are enrolling subjects who cannot read the consent materials due to blindness, or the subject's legally authorized representative is legally blind:

- It is recommended that an impartial witness observe the consent process.
- Sufficient time should be allowed for questions to be asked and answered, both by the subject, and by the person obtaining consent to ensure the subject comprehends the consent information.

- Consider using an audio recording of the consent discussion as part of the documentation of informed consent.

Guidance set forth by the International Conference on Harmonisation (ICH E-6 4.8.9): If the subject (or subject's legally authorized representative) verbally agrees to participate in the study:

- If capable of doing so, the subject signs and personally dates the consent form.
- The witness signs and personally dates the consent form. By doing so the witness attests that the consent information was accurately explained and that the subject apparently understood the information and informed consent was given freely.
- The person obtaining consent signs and dates the consent form.
- Signed copies are given to the subject.

International Conference on Harmonisation (ICH E-6 4.8.9)