
HERMES - Cognitive Care and Guidance for Active Aging
FP7-ICT 216709
Specific Targeted Research or Innovation Project

Start date of project: January 1, 2008
Duration: 36 months



D.8.1 DATA PROTECTION AND DISCLOSURE PLAN

Elena Urdaneta (Fundación INGEMA)

Cristina Buiza (Fundación INGEMA)

M^a Feli González (Fundación INGEMA)

Aitziber Etxaniz (Fundación INGEMA)

Version: 1.0
Date: 29/04/2008
Dissemination level : PU

Project Co-Funded by the European Commission within the 7th Framework Programme

Abstract

In this deliverable, the privacy implications of the recording and processing of key moments in the life of the user and conversations are addressed. In this project it's necessary to safeguard the elderly privacy, especially in user evaluations. It's important to take also into account the privacy of the other persons that will be involved in the conversations and interactions with the elderly (i.e. the doctor, friends, and relatives). Privacy management is addressed centrally in this deliverable.

Table of Contents

1. INTRODUCTION	4
1.1 BACKGROUND	4
1.2 SCOPE OF THIS DELIVERABLE	4
2. DATA STORING LEGISLATION	6
3. COLLECTION OF PERSONAL, AUDIO AND VIDEO DATA	8
3.1 SPANISH LEGISLATION	8
3.2 GREEK LEGISLATION.....	10
3.3 AUSTRIAN LEGISLATION	12
3.4 ISRAELI LEGISLATION	13
4. DATA PROTECTION PLAN AT HERMES	13
4.1 GENERAL ISSUES CONCERNING DATA PROTECTION PLAN	13
4.1.1 <i>Informed Consent</i>	14
4.1.2 <i>Data storage and handling processes</i>	14
4.1.3 <i>Process of encoding or anonymization</i>	16
4.1.4 <i>Security measures for storage and handling</i>	18
4.1.5 <i>Security enforcement within the project</i>	20
5. HERMES AT RUNTIME	22
REFERENCES.....	23
6. ANNEX I	25
7. ANNEX II.....	27

1. Introduction

1.1 Background

Data privacy refers to the evolving relationship between technology and the legal right to, and public expectation of privacy in the collection and sharing of data. Privacy problems exist wherever uniquely identifiable data relating to a person or persons 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 in data privacy is to share data while protecting the personal identity from the information [1].

1.2 Scope of this Deliverable

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 and attributes special protection to health data [2].

Privacy is a major problem, particularly for some spoken-word collections when individuals do not have an expectation that their statements will be archived, although they have spoken in a public forum such as a company board meeting or a political rally. It may not be possible to offer a comprehensive solution to the privacy problem, particularly for materials where contact with the original collector or subject has long since been lost, but research in this area can accomplish some practical goals. Future collectors must be armed with reasonable policies to obtain clearances and document applicable rights.

Also this document covers the latter concerns to the development of the e-Forum on Privacy in information Society (www.eprivacy.jrc.it), with its experience on best practice on the development of privacy enhancing technologies.

Privacy is important to participants. Participants expect the right to control and inspect personal information, and they expect that their personal information maintained by colleges and centres will be accurate. Today's participants also expect information about their personal activities to be kept private.

The European Charter of Fundamental Rights [3] states:

Art 3: Right to the integrity of the person

1. Everyone has the right to respect for his or her physical and mental integrity.
2. In the fields of medicine and biology, the following must be respected in particular:
 1. The free and informed consent of the person concerned, according to the persons.
 2. The prohibition of eugenic practices, in particular those aiming at the selection of persons.
 3. The prohibition on making the human body and its parts as such a source of financial gain.
 4. The prohibition of the reproductive cloning of human beings.

Art. 8: Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Art. 13: Freedom of the arts and sciences.

1. 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. They say that data must be:

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

Among the main objectives of the HERMES project is to build a pervasive human centric system that could essentially alleviate the cognitive decline for senior citizens through memory aids, conversation support and other user-centric services. The system will heavily rely on audio and video analysis for acquiring end-user's context, which will accordingly be stored to the HERMES databases and knowledge bases. As a result, the above principles are of particular relevance to HERMES, since the project will extensively deal with collection and storage of data that pertain to elderly human users. In particular:

- The HERMES partners will collect audio and video data from senior citizens, with a view to building video and audio analysis components (in the scope of WP4 of the project).

- The HERMES system will (during its actual operation) store and manage data (derived from the end-users' daily living). Furthermore, it is likely that the system will post-process these data (in the scope of WP5) in order to understand patterns of their daily behaviour, as well as important moments where memory aids and reminder should be automatically provided.

The HERMES project will fully comply with the above EU directive. Furthermore, individual partners will be aligned to their national regulation and directives about protection of personal data associated with elderly users of the HERMES system.

As stated in the previously mentioned European Charter of Fundamental Rights, this deliverable aims at providing concrete details on data protection and storage policy.

The HERMES consortium has through their profile great experience and relevant procedures for protecting and storing data of any kind. Four of the partners are conducting research involving the testing with real persons and procedures for the protection and storage of data. The consortium as a whole will align to these procedures.

It has been clearly assumed within project partners, that personal data may only be collected, processed, or used insofar as this is necessary for pre-determined, clear, and legitimate purposes. High standards must and will be ensured with regard to data quality and in technical protection against unauthorized access. The use of the data must be transparent for those concerned; and the rights of the latter must be safeguarded with regards to information and correction and, if applicable, to objection, blocking, and deletion.

The rest of this deliverable presents data storing legislation, along with national laws about data collection processes and related privacy issues. Specifically:

- Chapter 2 reports on European data storing legislation and the main objective is to forge agreement on spoken-word collections and video-records of HERMES project.
- Chapter 3 emphasized on collections of personal, audio and video data.
- Chapter 4 describes the Hermes consortium data protection plan.

2. Data storing legislation

An expectation of privacy

Some issues surrounding audio and video capture in public are not dissimilar to those debated when face-recognition technology began to be used to scan for potential criminals in crowds at airports and other public places [4]. Here, the expectation of privacy is one of anonymity, but this expectation is not always codified in law. Several United States of America state courts have resisted attempts to curtail video and audio recording in public, finding that no reasonable expectation of privacy can exist in a public place [5]. Use of recording technologies for public surveillance in the United Kingdom has been common for some years, though the government in 2000 signaled its intention to regulate such surveillance in accordance with its 1998 Data Protection Act, passed to harmonize U.K. laws with the 1995 European Union Data Protection Directive [6]. Other E.U. nations, including Greece and Sweden, also interpret the E.U.

Directive (revised in 1998 and 2000) to specifically pertain to public video surveillance and closely regulate its use [4].

Use of wiretapping and other communications surveillance technology is, in general, well regulated, requiring that law enforcement obtain court or judicial orders to make use of such know-how. In reality, permission to wiretap is easily obtained. In the United States no state or federal law enforcement agency requests for wiretaps were denied in 2001, and a total of 1,491 were authorized [7]. The French government approved 4,175 wiretaps in 2000 and the German government 12,651 in the same year [4: pages 178, 185, 388]. Open monitoring and recording of telephone transactions and monitoring of employees' electronic communications for business purposes is also widespread [8]. The right of employees to opt out of such data-gathering has been weak or non-existent. The E.U. is leading the push to expand data privacy regulations to include employee-monitoring activities, which may have the effect of discouraging such monitoring beyond the E.U.[9]. Most European Union nations have appointed a central data protection agency, charged with oversight of all personal data collection and processing, and grant individual citizens a mechanism for review, change or removal of their own information.

Given the need for oversight and the ease of access to such information once stored in digital form, some difficult choices face the custodian. What balance should be struck between protection of the individual and benefits of large spoken word collections for worthy public purposes (e.g., scholarly inquiry, political discourse, law enforcement, artistic expression)? A good place to turn for examples and guidance may be the regulations governing research on human subjects [8]. These regulations clearly advocate informed consent and limited gathering and use of personal data [10].

Collecting agencies should determine whether individuals have granted permission for a recording to be made, implicitly or explicitly. A signed consent or permission form is the best safeguard, but is unlikely to be available, particularly for older recordings. Presenters and announcers, interviewers and interviewees, audience members and call-in guests, parties in a conversation: all such participants must be considered when determining whether privacy rights are an issue. A public figure, such as a politician or a known lecturer, is unlikely to substantiate an invasion of privacy claim were his speech to be recorded. The more public the citizen, the less likely he or she is to be able to make a claim.

Extent of copyright protections for spoken word materials

As signatories to the Berne convention [11], the United States and the European Union member nations have reciprocity in copyright protection so that materials created or published in one nation will, for the most part, enjoy the same protections in other nations. Copyright statutes generally reserve for the copyright holder the exclusive right to reproduce, display, distribute copies of, and perform or broadcast the work. The European Union issued a copyright directive [12] in 2001 that matches many of the provisions in the United States Digital Millennium Copyright Act (DMCA) of 1998. Both extend encryption protections with harsh anti-circumvention language. Principles in the EU Copyright Directive will be implemented through the laws of member nations. The results of this implementation do not yet offer clarity or guidance.

In general, sound recordings have historically been accorded fewer protections than other types of works, though some recent initiatives have the effect of increasing their protection [13]. In the United States, sound recordings were not protected by federal copyright law until 1972, and

recordings made before that date are still not federally protected (though they may be under state copyright laws). Works fixed after 1977 receive at least 70 years of protection. (In the United States, in order for works to qualify for protection, they must be fixed in some physical medium. This requirement has been clarified to encompass digital publication, as well.) In the United Kingdom, copyright for sound recordings was established in the 1911 law [14] and lasts for 50 years, 20 fewer years than granted to creators of print works. The 1979 revision of the Berne convention likewise established a 50-year duration of copyright, a term also endorsed by the European Union in 1993 [15].

Main objective

The aim of this part of the document is to forge agreement on spoken-word collections and video-records of HERMES project. We also need to focus research support on areas of access and preservation that we believe will yield the greatest security measures of the elderly personal recordings.

Spoken-word collections cover many different domains of daily living. These include information about diet, medical diagnosis, weight control, medication, administrative proceedings, oral narratives, meetings and telephone conversations. Needs vary in collecting, accessing and preserving such data.

Within the scope of HERMES we have identified several needs regarding privacy of data: acquisition, preservation, search and access of lectures; use of digital audio and video resources as primary sources for inquiry and explication.

For HERMES purposes, three main ways of collecting data will be carried out:

- Collection of personal data (socioeconomical, medical diagnoses, cognitive status)
- Collection of audio data
- Collection of video data

We have therefore analyzed these three main aspects of data collection, studying the legislation in Europe as well as specifically in each involved country (mainly Spain, Austria, Greece and Israel), and proposing a data protection plan that aims to cover all the cited aspects. This plan is presented in Chapter 3 below.

3. Collection of personal, audio and video data

In this Project, different partners from different European countries will develop research involving humans. Therefore, all the national legislations of the countries involved will be considered.

3.1 Spanish legislation

INGEMA will fulfil all the requirements stated by the *Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data (LOPD 15/1999)* [16] 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. This 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 HERMES:

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 and the specified, explicit and legitimate purposes for which they were obtained.
- 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 identity and address of the controller or of his representative, if any.

Art. 9: Data security

- 1) The controller or, where applicable, the processor shall adopt the technical and organisational 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 subjected to processing, on the origin of such data and on their communication or intended communication.
- 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

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

INGEMA as a part of the MATIA group has, according to the Spanish law [223/2004], a Research Ethics Committee that has to approve all research projects involving human participants. This Ethic Committee was accredited by Resolution of the Basque Health Department (BOVP 18th July 1997). This Committee guarantees the best quality of social, psychological and public health attention to elderly people and the fundamental ethical principles that a Clinical Research on human beings has to have. This Committee respects the criteria of Good Clinical Practice in Investigation and Helsinki and Oviedo Agreements. Also the studies involving humans are supervised by Ethics Committee of Donostia Hospital.

INGEMA will use the INFOR10.doc (see attachment) when working and collecting data within research projects involving humans, covering the Organic Law on Protection of Personal Data (LOPD 15/1999). This means, among other, that data collected in the project, due to security issues, will not be accessible from the Internet and the people working with the data will have to have a unique password to access the database. The database will of course be sealed from people not involved in the project but working at INGEMA. Before testing occurs the participants are clearly informed in that, they either are allowed in keeping the equipment or not and has to sign an Informed Consent. MATIA group and INGEMA have been involved in projects with humans from 10 years ago.

INGEMA will register the HERMES database on the Spanish Data Protection Agency (Agencia Española de Protección de Datos), fulfilling the requirement to notify this Agency of transfers of personal data between EU member states.

3.2 Greek legislation

In order to guide the handling of personal data, AIT will follow the “2472/1997 Greek law” namely “Individual protection for personal data processing” written in 1997 [17], but also the directive about Closed Television Circuits (CCTV) held out in 26-09-2000 by ‘Hellenic Data Protection Authority’.

Sensors used in the HERMES project will record and store information about users continuously. In order to protect users’ privacy, several security measures and protocols will be implemented in the platform.

AIT will be legitimate to the “Hellenic Data Protection Authority” during the project, and all sensible data will be encrypted and protected during storage and process so that user’s identity

and privacy will not be compromised as a result of the introduced sensors. Context awareness technologies will also contribute to determine which content should be registered and which should not be annotated.

The Law of “Individual Protection from Processing Data of Personal Character” 2472/1997 of Greece: The law of 2472/1997 dedicates several articles to the protection of personal data. The parameters that make processing of personal data legal are defined at its second chapter (4th article), which is entitled “Processing Data of Personal Character”. More specific:

In order to perform legal processing on personal data:

- Data should be collected with acceptable and legal methods for predefined, clear and legal purposes.
- Data should be coherent, convenient and no more than that the application demands.
- Data should be stored in a way that the definition of the subjects’ identity should be possible, only during the period that this is necessary for the completion the scope that they have been collected. After the termination of this period only the Hellenic Data Protection Authority could allow further preservation of personal data for historical, scientific or statistical purposes given that no right of the subjects is offended.

The observance of the above devolves the responsible of the data processing. All data collected contrary to what has been mentioned above should be destroyed by the responsible of data collection and processing.

The 5th article, mentions that the process of personal data is only allowed provided the subject’s assent. The responsible for data collection and processing is indebted to inform the Authority for the existence and operation of the database or the processing of its data.

According to 2472/1997/GR (article 7) processing of personal data is illegal unless:

- The subject has already given a written assent (provided that it has been legally constructed).
- The process of data concerns issues of personal health and it is carried out by someone that his profession is related to health services and he is subject to confidence obligation and relevant deontology code.
- The process is held for research and scientific purposes under the condition that anonymity is observed and all necessary measures for protecting individual’s rights are obtained.

The 10th article describes the Confidentiality and Security of Processing Personal Data. More precisely:

- The procedure of processing personal data should be confidential. This means that processing can only be conducted by those that are controlled by the responsible of process.
- The responsible of processing the data has to obtain all appropriate organising and technical measures for data security and their protection from incident or unwanted corruption, loss, or illegal distribution. The measures have to provide a level of protection proportional to the risks that emerge from illegal processing.

Articles 11 and 12 cover the rights of the subject person to be informed and to access his personal data. More specifically:

- The responsible for data collection and processing has to inform the subjects about his identity, the scope of the process, the recipients of the data.
- The subject of personal data has the right to receive information about all his personal data and their source.
- The reasoning behind the process.
- Subject has the right to correct, delete, or block his data.

Directive of Closed Television Circuits (CCTV) 26-09-2000: Regarding the directive of Closed Television Circuits (CCTV) held out by Hellenic Data Protection Authority

- Audio and Video data acquisition that reflect individuals are Data of Personal Character.
- Even storing such data incorporates process of personal data.
- Data collected through CCTV has to be related to the scope of the process and no more than needed to accomplish that specific task. Thereby the places that the cameras are installed and the way of capturing have to be defined so that only essential data is collected.
- Storage of such data shouldn't be retained more that necessary and much less than 15 days. Retaining such data bases requires special permission by the Authority.
- Special security measures have to be considered for as long data is stored. The responsible of processing has to mind for the security aspects.
- Before a subject enters the area where the cameras or microphones are placed he should be forewarned (signs, labels, doorplates).
- Capturing videos from communal places, given the Authority's permission, should be unvoiced. Data from communal places can only be retained for up to 48 hours unless a special license has been provided to the responsible of processing data.

3.3 *Austrian legislation*

In Austria, the main legislation regarding privacy issues can be found in two laws, the *Privacy law - Datenschutzgesetz 2000* or in short *DSG 2000* (long name: *Bundesgesetz über den Schutz personenbezogener Daten*) [18] as well as in the *Data security law for medical information - Gesundheitstelematikgesetz* or in short *GTelG* (long name: *Bundesgesetz betreffend Datensicherheitsmaßnahmen beim elektronischen Verkehr mit Gesundheitsdaten und Einrichtung eines Informationsmanagement, Stammfassung BGBl. I Nr. 179/2004* [19]):

- This law describes that Data should be protected against access from unauthorized persons, as well as protected against accidental and unlawful destruction and loss, according to paragraph 14, article 1.
- This also implies the declaration of those people that are allowed to access, update, analyse the data, the organisation of access control, the organisation of backups, the identification of users, etc.
- If explicit medical data is obtained and stored in a database, this has to be reported to the Privacy protection-register if the data, except if it is stored anonymised. Of course, the participant will have to sign the consent for this.

- The consent form has to be approved by the ethical committee.
- Anonymisation should be performed wherever possible and a relation to persons should only be available when it is absolutely necessary to a specific person. An ID is ok, as long as it cannot be indirectly connected to the specific person (e.g. through a combination of date-of-birth, city, employment).
- Distribution of data to other partners should be communicated to the Ethical committee with reason. Guidelines should be followed regarding encryption.

3.4 Israeli legislation

In Israel, personal data protection is governed by a set of laws including:

- The Protection of Privacy Law 5741-1981, 1011 Laws of the State of Israel 128, amended by the Protection of Privacy Law (Amendment) 5745-1985 [20]
- The Computer Law of 1995
- The Genetic Information Law of 200.

The Protection of privacy law regulates the processing of personal information in computer data banks. The law sets out 11 categories of prohibited activities and provides for civil and criminal penalties for violating individual privacy.

In June 2007, the Privacy Law was amended to include an obligation of person's conscious consent for invasion of privacy and punishment for violation of this obligation.

Unauthorized access to computers is punishable by the Computer Law.

The Genetic Information Law protects the rights of individuals with respect to their DNA samples and their genetic information. The Genetic Information Law and existing ethical guidelines cover most issues of informed consent, confidentiality, and rules of access for both identified and non-identified DNA samples or genetic information in the individual or family-based, small-scale collections.

4. Data protection plan at HERMES

4.1 General issues concerning data protection plan

Purpose of the Data Protection Plan: The Data Protection Plan becomes part of the signed agreement between HERMES 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.

What should be covered by the plan: The Data Protection Plan applies to both the raw data file received from HERMES 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 should address 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.

Components of the plan: HERMES Data Protection Plan should contain the following components:

4.1.1 Informed Consent

Informed consent is the process by which a participant will be fully informed about the research in which he/she is going to participate. It originates from the legal and ethical right the participant has to direct what happens to his / her personal data and from the ethical duty of the investigator to involve the participant in research.

Respect for persons requires that participants, to the degree they are capable, be given the opportunity to choose what shall or shall not happen to them. This opportunity is provided, when adequate standards for informed consent are satisfied.

In order to involve a human being as a participant in research, the investigator will obtain the legally effective informed consent of the participant or the participant's legally authorized representative.

All investigators within HERMES will seek such consent only under circumstances that provide the prospective participant or the representative sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence.

The information given to the participant or the representative will be in language understandable to the participant or the representative. 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 investigator, the sponsor, the institution or its agents from liability for negligence.

4.1.2 Data storage and handling processes

Much research revolves around information about people –their age, lifestyle, health– drawn from records, scientific tests, surveys and interviews. Sometimes, the information also reveals facts about relatives and relationships. These types of information are sensitive and private for many people, although attitudes and expectations vary widely.

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.

Furthermore the participants have to be able to control the dissemination of the collected data. The investigator is not allowed to circulate information without anonymization. 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. Simple stripping of the participants name and its replacement with a code is no guarantee of complete confidentiality.

At HERMES:

Original data will be kept at:

- At INGEMA: INGEMA Txiki, Area Neuro, Camino de los Pinos 27 San Sebastian (SPAIN);
- At CURE: CURE – Center for Usability Research and Engineering, Hauffgasse 3-5, A-1110, Vienna (AUSTRIA)

Copies of anonymous data will be kept at:

- At IBM: IBM Haifa Labs, Haifa University Campus, Mount Carmel, Haifa 31905, Israel.
- At AIT: 0,8 Km Markopoulo Ave. GR - 19002 Peania, Athens, (Greece);
- At TXT: TXT LABS, Via Capelli, 12 20126 Milano (Italy)
- At UniBrad (if applicable)

HERMES Research Project and Principal Investigators at these sites are:

- At INGEMA, C. Buiza/E. Urdaneta;
- At Cure, Arjan Geven/Norman Höller
- At AIT, John Soldatos
- At IBM, A. Sorin/H. Aronowitz/J. Mamou
- At TXT S. Gusmeroli/Fabio Cattaneo/A. Conconi
- At UniBrad, Jianmin Jiang.

4.1.3 Process of encoding or anonymization

Information should be anonymized 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.
- Anonymized data with links to personal information is anonymized 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 anonymized data contains nothing that has reasonable potential to be used by anyone to identify individuals.

As a minimum anonymized data must not contain any of the following, or codes for the following:

- Name, address, phone/fax. Number, e-mail address, full postcode.
- Any identifying reference numbers.
- Photograph or names of relatives.

Researcher and database developer should always consider – when designing studies, before passing information to others, and before publishing information- whether data contain combinations of such information that might lead to identification of individuals or very small groups. Within HERMES we will follow the unlinked anonymized data policy, excluding users having rare diseases and any other identifiers, except age, gender and nationality. Once anonymized, the data will not allow tracing back the participant in any way.

Data will be encoded, and anonymized using numerical codes. During the experiments and the development stages, the correspondence with the users list will be saved into a local database, which will be encrypted.

At HERMES the computing environment in which the data will be used at each of the sites, is explained above:

- At IBM:
 - Computing platform (PC, workstation, mainframe platform) PC
 - Number of computers on which data will be stored or analyzed – Multi-node infrastructure
 - Whether personal computers used in the research project will be attached to a network or will operate independently (stand-alone) - computers connected to a LAN
 - Physical environment in which computer is kept (e.g., in room with public access, in room locked when not in use by research staff) - Entrance to IBM Haifa Research

Lab premises is possible only to IBM employees who have a valid ID badge. Other invited visitors after authentication at the reception are escorted by an IBM employee. All the rooms are normally locked when not in used by research staff.

- At INGEMA:
 - Computing platform (PC, workstation, mainframe platform): PC
 - Number of computers on which data will be stored or analyzed: 2
 - Whether personal computers used in the research project will be attached to a network or will operate independently (stand-alone) -Stand-alone computers for the data collection, computers connected to a LAN for analysis
 - Physical environment in which computer is kept (e.g., in room with public access, in room locked when not in use by research staff): In Room locked when not in use by research staff.

- At TXT:
 - Computing platform (PC, workstation, mainframe platform): PCs and mobile devices (PDA)
 - Number of computers on which data will be stored or analyzed: 2 for storing, multi-node infrastructure for analysing, potentially available.
 - Whether personal computers used in the research project will be attached to a network or will operate independently (stand-alone): Network computers connected to the enterprise LAN.
 - Physical environment in which computer is kept (e.g., in room with public access, in room locked when not in use by research staff): Room locked when not in use by public staff.

- At Bradford:
 - Computing platform (PC, workstation, mainframe platform): PC;
 - Number of computers on which data will be stored or analyzed - Multi-node infrastructure
 - We will have 5 computers to store the data relevant to HERMES, which are networked but security protection is in place.
 - Whether personal computers used in the research project will be attached to a network or will operate independently (stand-alone) : The computers used in the project are networked, but their file access can only be made via manual transfer through flash disks.
 - Physical environment in which computer is kept (e.g., in room with public access, in room locked when not in use by research staff): all computers are kept in a laboratory, which is locked when not in use.

- At CURE:
 - Computing platform (PC, workstation, mainframe platform): PCs
 - Number of computers on which data will be stored or analyzed : 2
 - Whether personal computers used in the research project will be attached to a network or will operate independently (stand-alone) : Stand-alone computers for the data collection, computers connected to a LAN for analysis
 - Physical environment in which computer is kept (e.g., in room with public access, in room locked when not in use by research staff): Room locked when not in use by research staff.

- At AIT:
 - Computing platform (PC, workstation, mainframe platform): PC
 - Number of computers on which data will be stored or analyzed: Multi-node infrastructure
 - Whether personal computers used in the research project will be attached to a network or will operate independently (stand-alone): Stand-alone computers for the data collection or computers connected to a LAN
 - Physical environment in which computer is kept (e.g., in room with public access, in room locked when not in use by research staff): Room locked when not in use by public staff.

4.1.4 Security measures for storage and handling

AIT and IBM use state of the art technologies for secure storage, delivery and access of personal information as well as managing the rights of the users. In this way, there is complete guarantee that the accessed, delivered, stored and transmitted content will be managed by the right persons, with well-defined rights, at the right time.

State of the art firewalls, network security, encryption and authentication will be used to protect collected data. Firewalls prevents the connection to open network ports, and exchange of data will be through consortium known ports, protected via IP filtering and password. Where possible (depending on the facilities of each partner) the data will be stored in a locked server, and all identification data will be stored separately.

A metadata framework will be used to identify the data types, owners and allowable use. This will be combined with a controlled access mechanism and in the case of wireless data transmission with efficient encoding and encryption mechanisms.

At HERMES:

- At INGEMA on removable storage media such Zip(R) drive, with password access.
- At Cure, 1) identifiable information will be stored in a Truecrypt encrypted volume on removable media, with password access for the principal investigators only. 2) Other anonymised data will be stored in a separate truecrypt encrypted volume,

stored on CURE's intranet with password access to those CURE researchers directly involved in HERMES.

- At AIT, AIT won't use real identification data. Each subject will be tagged with a code-number (unrelated to real identification data), through which personal information retrieval will be impossible. Access to anonymous data will be permitted only to those that are directly involved in the project. The access will be password protected.
- At IBM: 1) Identification data will not be stored. 2) Anonymous audio recordings will be stored on IBM's intranet protected with the standard access control mechanism. The access will be provided only to the staff directly involved in HERMES project.
- At TXT, on local servers located in protected hosting rooms, inside the company's facilities for development, production and backup environments
- At UniBrad, on a secured and backed-up server managed by the technical supporting team within the School of Informatics, access to the data will strictly limited to researchers directly working on HERMES project only with password-based protection.

All sensible data will be encrypted and protected during storage and process so that user's identity and privacy will not be compromised as a result of the introduced sensors. Context awareness technologies will also contribute to determine which content should be registered and which should not be annotated.

Methods of data storage when data are not being used.

The data, not being used, will be stored in a locked server, and all identification data will be stored separately. A metadata framework will be used to identify the data types, owners and allowable use.

In this way, there is complete guarantee that the stored content will be managed by the right persons, with well-defined rights, at the right time.

Methods of transmitting the data between research team members

Researcher and database developer should always consider – when designing studies, before passing information to others, and before publishing information- whether data contain combinations of such information that might lead to identification of individuals or very small groups. Within HERMES we will follow the unlinked anonymized data policy, excluding users having rare diseases and any other identifiers, except age, gender and nationality. Once anonymized, the data will not allow tracing back the participant in any way.

Data will be encoded, and anonymized using numerical codes. During the experiments and the development stages, the correspondence with the users list will be saved into a local database, which will be encrypted.

Methods of storage of computer output (in electronic form as well as on paper).

- At INGEMA, the papers about evaluation of the participants will be kept with a code in a room locked and only the Principal Investigators would have access to the personal information and the information related with HERMES Project.
- At Cure, no paper based output will be kept or archived with respect to unanonymized data. The questionnaires that are filled out by the users will be only identifiable by a code. The relation between code and other data is kept only in computerized form stored in the Truecrypt volume described above. If paper output is used during the analysis phase, it is destroyed directly after usage whenever it relates back to individual participants. All computer outputs (such as statistical analyses, will be kept within the encrypted volume.
- At AIT, computer output will be stored in the same way audiovisual data will be stored in a dedicated server with the same measures of security. All outputs will arise from processing the anonymous data and no hard copies will be used.
- At IBM, computer output derived from the anonymous audio data will be stored in exactly the same manner as the source audio data. No hardcopies will be produced.
- At TXT, all the documents are secured inside our facilities in a locked room protected by electronic badge. Only R&D business unit employees have access to this area.
- At UniBrad digital storage as well as printed paper files will be stored in a dedicated project space, including server as well as archiving room for research within the School of Informatics, where access to the room is limited to managers at the School level.

4.1.5 Security enforcement within the project

Data will be collected at different research sites with surveys and experiments. The collected data will be stored in a secure server, only visible to the research site network, in a locked room at each of the research locations. Anonymous and identity data will be stored separately, and only the project leader will have access to all the users' identities. Anonymity will be granted by separating identifiable data from anonymous data. Each user will be granted 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 granted only after explicit user permission and after agreement of the responsible Data Protection Agency/Authority (Ethical Committee of Matia/Hurkoa/Gerozerlan).

Authentication will be required to access stored data on the research site. Authorized researchers will have access to the recorded anonymous data after authentication with a centralized server and on a need-to-know basis. Researchers performing the survey will have access rights to add data to the identity database, synchronized with the writing of the anonymous data. No editing or reading rights will be granted to them to prevent alteration/disclosure of private data.

Access to the different databases will be granted with an authentication server that will restrict access depending on the user identity, profile and the device he is currently using (identified through its IP address). If the device he is using is not from the local research site network, access will be banned. Access to each of the tables of the database will be also filtered on a user-based policy. A periodic change of password and minimum password quality policy will be enforced to grant the security of the system. Username, password and IP address will be checked before granting access to restricted data.

As stated previously, those researchers working on HERMES abide by the contractual obligations of the consortium. If not included in this obligation, they will sign a statement that commits them to make sure project data are not provided to persons outside HERMES.

User profile and habits will be stored in an anonymous way, and used for psychological research and user profiling. No financial data will be used in the project, so it is a non-issue. Medical data will be used in the research and will only be distributed anonymized and on a need-to-know basis. No medical data will be stored centrally in the final application.

Logs of all transactions in the databases will be kept continuously and backups of the logs will be done periodically, so that actions performed upon the data can be monitored and responsibilities attributed. The server should be stored in a locked room with restricted access. Integrity of data will be granted with periodical backups and redundant images of the database, in case that a roll-back is needed. Only the automatic logger user will have rights to modify those logs, to prevent modification of the recorded data.

If an exchange of data among the different research sites is required, for example, due to the need of some researchers of data collected in another country, the data will be encrypted, prior to the transmission through a private virtual network from one site to the other, and the collected data will be then added to the database by authorized users (who will need the decryption password).

At HERMES:

Types of protection expected: Although there are alternative ways to assure security for the data and applicants should prepare their plans in a manner that best meets their needs, some or all of the following features are typically found in successful data protection plans:

- Password protection for all files containing data (note that password protection is not regarded as sufficient protection by itself)
- Removable storage media holding the data (e.g., CDs, diskettes, zip disks, etc.) kept in a locked compartment/room when not in use
- Printouts derived from data analysis stored in a locked compartment/room when not in use
- No storage of the personal data any network, including LANs, Internet enabled, etc.
- No transmittal of data or analysis output derived from the data via e-mail, e-mail attachments, or FTP (either over the Internet, an Intranet system, or within a local area network)
- Use of the data on a dedicated computer kept in a secure room and not connected to a network
- No backup copies of the data outside from the project to be made
- Data stored in strongly encrypted form

Disclosure Rules

The HERMES Data Protection Plan carefully describes how researchers and staff members will avoid inadvertent disclosure of respondents' geographic locations or identity in all working papers, publications, and presentations.

At minimum, researchers must agree to exclude from any type of publication or presentation, the following information:

- Listing of individual cases;
- Description of individual cases;
- Listing, description, or identification of a participants by number, by name, or by descriptive information;

As an international consortium between multiple partners that operate partly on the same data, the consortium will have to communicate data about the participants among each other. This data will only be communicated in an anonymous way. The data communicated will be sent in an encrypted, password-accessible form on a need-to-know basis, with access only to the staff directly related to the project. The data is subsequently stored at the individual partner locations in the manner described above.

5. HERMES at Runtime

The HERMES run-time system will be privacy friendly (e.g., following principles outlined in [21]). It will respect user preferences, while also enabling end-users, as well as system administrators/deployers to configure and control its privacy settings. HERMES will include a configurable rule-based sub-system enabling end-users (and/or deployers) to configure the system at a privacy level required by the end-user (i.e. based on an appropriate sub-set of available rules and features). The system will also encompass reasoning about trust and risk involved in the interactions between end-users and HERMES assistive services. It is envisaged that HERMES will maintain a shared model of context for all computing entities in the (in-door and out-door) locations where the HERMES systems will be deployed. Accordingly, the system will enforce the privacy policies defined by the users when sharing their contextual information (using techniques based on ontologies [22-23]).

Specifically:

- HERMES will define and implement different specialized access control models for protecting the privacy of the end-users.
- Each of these access control models will consist of a set of (inference) rules that the HERMES system will test/employ in order to grant permission to user data, as well as to other functionalities requesting access to users contextual information.

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] Privacy and Human Rights 2002. Electronic Privacy Information Center (EPIC) and Privacy International, 56-57, Washington, D.C., 2002.
- [5] L. E. Rothenberg. Re-thinking privacy: peeping toms, video voyeurs, and failure of the criminal law to recognize a reasonable expectation of privacy in the public space. American University Law Review, 49:1127, June 2000.
- [6] Information Commissioner (United Kingdom). CCTV code of practice. July 2000. Accessed on March 13, 2002, available at: <<http://www.dataprotection.gov.uk/>>
- [7] The Federal Judiciary (United States). Wiretap Reports. Accessed on March 13, 2003: <<http://www.uscourts.gov/wiretap.html>>
- [8] Employee Privacy: Computer-Use Monitoring Practices of Selected Companies. Washington, D.C.: United States General Accounting Office, September 2002. Accessed on March 13, 2003: <<http://www.gao.gov/new.items/d02717.pdf>>; Privacy and Human Rights 2002, pages 90-91.
- [9] R. Glover and A. Worlton. Trans-national employers must harmonize conflicting privacy rules. In The Metropolitan Corporate Counsel, Mid-Atlantic Edition. page 20 (November 2002)
- [10] U.K. JISC Data Protection Principles. Accessed on March 13, 2003: <http://www.jisc.ac.uk/legal/index.cfm?name=lis_dp_prin> and U.S. NIH Office of Human Subjects Research. Accessed on March 14, 2003: <<http://206.102.88.10/ohsr/site/>>
- [11] World Intellectual Property Organization (WIPO). Berne Convention for the Protection of Literary and Artistic Works. Accessed on March 14, 2003: <<http://www.wipo.int/treaties/ip/berne/index.html>>
- [12] European Parliament. Directive 2001/29/EC of the European Parliament and of the Council. Accessed on March 14, 2002: <http://www.patent.gov.uk/copy/notices/pdf/implement.pdf>
- [13] D. S. Karjala. Chart showing changes made and the degree of harmonization achieved and disharmonization exacerbated by the Sonny Bono Copyright Term extension Act (CTEA).

May 15, 2002. Accessed on March 14, 2003:
<http://www.law.asu.edu/HomePages/Karjala/OpposingCopyrightExtension/legmats/HarmonizationChartDSK.html>

[14] Patent Office (United Kingdom). Copyright History. Accessed on March 13, 2003:
<<http://www.patent.gov.uk/copy/history/>>

[15] Council of European Communities. Council Directive 93/98/EEC of 29 October 1993 Harmonizing the Term of Protection of Copyright and Certain Related Rights, 29 October 1993. Accessed on March 14, 2003:
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31993L0098&model=guichett

[16] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[17] Greek Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data - as amended by Laws 2819/2000 and 2915/2000

[18] Privacy law - Datenschutzgesetz 2000 or in short DSG 2000 (long name: Bundesgesetz über den Schutz personenbezogener Daten)

[19] Data security law for medical information - Gesundheitstelematikgesetz or in short GTelG (long name: Bundesgesetz betreffend Datensicherheitsmaßnahmen beim elektronischen Verkehr mit Gesundheitsdaten und Einrichtung eines Informationsmanagement, Stammfassung BGBl. I Nr. 179/2004)

[20] The Protection of Privacy Law 5741-1981, 1011 Laws of the State of Israel 128, amended by the Protection of Privacy Law (Amendment) 5745-1985.

[21] M. Langheinrich. Privacy by design—principles of privacyaware ubiquitous systems. In Proceedings of UbiComp 2001: International Conference on Ubiquitous Computing, 2001.

[22] Chen, H., Finin, T. and Joshi, A. 2004. A Pervasive Computing Ontology for User Privacy Protection in the Context Broker Architecture. Technical Report TR-CS-04-08, University of Maryland, Baltimore County

[23] H. Chen, T. Finin, and A. Joshi. An ontology for context-aware pervasive computing environments. Special Issue on Ontologies for Distributed Systems, Knowledge Engineering Review, 2003

6. ANNEX I

LEGAL ADVISORY FORM FOR IMAGES PROCESSING

When [INGEMA (Fundación Instituto Gerontológico Matia) or other partner] will obtain, or allow third parties to obtain, images including people, the subject must be informed about the intended use of the images and his/her consent must be obtained

INGEMA [Partner Name] must keep the document proving that the person has been informed and has expressly consented. This document will be kept in a restricted access area and will be traceable and accessible at any time

It is very important that the publication or graphic communication media does not keep in its photograph file the image of the subject

Following, there is a legal warning to be included in the contracts, giving in this way compliance to the obligations related to the information to be provided to the subject at the moment that images are obtained:

By filling in this form you expressly consent to the fact that your image will be taken by INGEMA (Matia Foundation) [Partner name] and the use of it in graphic communication media with the purpose of informing about the activities of the Foundation, and/or for research purposes that have been supervised and approved by the Ethical Committee.

Moreover, you are informed that you can exercise your rights to access, rectification, cancellation and opposition in Camino de los Pinos, nº 27, Donostia (Gipuzkoa)

In these cases, it is convenient to have **the signature** of the subject involved, since the **Ley Orgánica 1/1982 de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen** reads in its article 2:

1. The civil protection of honour, intimacy and self image will be delimited by the laws and social uses, attending to the area that due to self actions has every person for him/herself or his/her family.
2. Illegitimate interference in the protected area will not be considered when it is expressly authorised by the law or **when the right holder had given his/ her express consent**
3. The above referred consent will be revocable at any moment, but it will be necessary to compensate if it proceeds, the caused damages including the justified prospects

Name:....., **ID nº**.....

PostalAddress

.....**Box**.....**city/**
town.....**county**.....

....

Country.....

By filling in this form you expressly consent to the fact that your image will be taken by INGEMA (Fundación Instituto Gerontológico Matia) [Partner name] and the use of it in graphic communication media with the purpose of informing about the activities of the Foundation and/or research purposes that have been previously supervised by an Ethical Committee.

Moreover, you are informed that you can exercise your rights to access, rectification, cancellation and opposition in Camino de los Pinos, nº 27, Donostia (Gipuzkoa)

Place and Date: _____

Signed by:

7. ANNEX II

PERSONAL CHARACTER DATA PROTECTION

INFOR 10
Page 27 of 28
Revision 0
30/09/02

1. OBJECT

To warranty and protect the confidentiality and security, regarding to Information and personal data treatment, in every process of the Organisation according to the Organic Law 15/99 of Personal Data Protection.

2. SECURITY RESPONSIBLE: Nerea Alberdi

3. SCOPE

The scope of this document covers all Centres /Services and departaments of Matia Foundation which own files with data of personal character or the ones they wan to create.

4. OPERATIVE SYSTEM

4.1 INVENTORIES OF FILES AND ANALYSIS OF THE SITUATION

The responsables of the FHG (Functionals Homogeneous Groups) should make an inventory of the files that intervene in their processes, stating the persons that have access to the different files, their responsables, the finality of the file, the types of data that contain and if the files have relation with third entities and will send it to the Security Responsible.

After receiving this Information, the Security Responsible of data, with the responsible of computing of the Organisation, will make an analysis of every file with the objective of stablishing if the computer environment and the different files meet with the legislation about protection and confidentiality of the containing data.

After the realization of this analysis, a plan will be made to adapt the files to the current legislation, in a thecnical and organizative way. Behavioural guidelines will also be established and obligations of security for people with access to files of personal character data.

4.2 CREATION, MODIFICATION AND SUPPRESSION OF FILES

4.2.1. Creation of new files

The responsables of the FHG/Process which have the need of creating a new file, that contain data of personal character will communicate the Responsible of Security of the creation of this file through the printed model INFOR 1001.

4.2.2. Modification of files

Due to need of modifying a file which contain data of personal character, the responsables of the FHG/Process will communicate the Responsible of Security through the printed model INFOR 1001 the causes of this modification and the data of said modification.

4.2.3 Suppression of files

The files that has been created in a temporary way, when the object of creation disappear, will be deleted of the computer system through a notification of the responsables of the FHG/Process to the Responsible of Security through the printed model INFOR 1001.

The Responsible of Security, once received any of these communications, will proceed to notify to the Agency of Protection of Data through the oficial forms, who at the same time register it in his/her database.

5. RELATED DOCUMENTS

Organic Law 15/99 of Protection of data of Personal Character

Royal Decreto 994/1999 of 11 June. Art. 8. The measurements of the security files containing data of personal character will be regulated.

Print. Mod. INFOR 1001: Communication of creation, modification, o suppretion of personal character files.

Rev.	Description of changes	Date
0	Elaboration of the initial document	30/07/02

6. DISTRIBUTION

Managing Dtor.	Quality Dtor.	Human Resources Dtor.	Nursery Dtor.	Social Services Dtor.
Accounting	R. Bermingham Hospital		R. Bermingham Gerontological Unit	
Alai Etxe	Txara I	Fraisoro	San Jose	Julian Rezola
Rehabilitation Service (7)		Pharmaceutical Service		Certifying Entity
Admission	Feeding	Almacén	Rezola Day Center	Txara 1 Day Center
Fraisoro Day Center	Bermingham Day Center		Purchasing	Invoicing
Rezola Ruler	R. B. Ruler	Computting	Laboratory	Finnacial
Maintenance	Radiology	Prevention Service		

Approved by the Managing Comitee

08/02/03