"This project has been funded under the fourth AAL call, AAL-2011-4. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein"

PROJECT Nº: AAL-2011-4- 027

PRIVACY AND DATA SECURITY MODULE

Start Date of Project : 01/05/2012 **Duration :** 36 months

PROJECT FUNDED BY THE AAL JOINT PROGRAMME	
Due date of deliverable	1 May 2013
Actual submission date	31 May 2013
Organisation name of lead contractor for this deliverable	UNIGE
Author(s)	UNIGE
Participant(s)	HIB, CETIEX, Careyn, Connected Care, AGIM
Work package	WP3
Classification	Restricted
Version	31 May 2013

Table of Contents

1. Introduction

The overall objective of the MyGuardian project is to design, implement and evaluate services that facilitate safe and secure mobility of seniors with mild cognitive impairments while preserving their autonomy and dignity. MyGuardian improves wellbeing and efficiency of voluntary caregivers (e.g., family and friends) by ensuring their peace of mind and keeping them informed when the senior is experiencing confusion states and risk situations when out and about, and improves efficiency of professional caregivers by providing them with up-to-date information and by supporting coordination of their care efforts. Third, MyGuardian enables new business models for professional caregivers by enabling them to assist voluntary caregivers and to step in when needed.

Four countries: Spain, France, the Netherlands and Switzerland actively participate in the implementation of the project, while user trials will take place in Spain, France and the Netherlands. This report presents planned deployment with respect to ensuring the privacy and data security in the MyGuardian system. In each of the subsequent sections we discuss the important legislation and/or organizational aspects influencing the requirements for the data privacy and security in MyGuardian.

As there is NOT a separate privacy and data security software module envisioned for the MyGuardian solution – the deliverable is organized such the authors indicate the *implications* of the above-mentioned legislation and/or organizational aspects on the MyGuardian design and operational aspects. These implications are highlighted in sub-sections of this deliverable.

2. Background and Motivation

When referring to information of personal data, its referred to all data that identify an individual, or made them identifiable, this information is protected by the right of data protection staff, in the Directive 95/46/EC of the European Parliament and 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 The European Constitution recognizes twice the fundamental right to data protection. It also states that all member countries of the European Union must have an authority ensure independent and will safeguard that right. This implies that the MyGuardian project must take all preventive and reactive measures that can be provide, with technological systems and possible organizations safeguard and to protect the information, so that it can be maintained the confidentiality, availability and data integrity required for this project (as depicted at large in Figure 1). This concept of information security should not be confused with computer security, which is responsible for security in the computer environment, an issue also necessary in the implementation of the project to be developed. The security information includes various aspects including availability, communication, problem identification, risk analysis, integrity, confidentiality and the recovery of risks. Noting that data users require a high level of security and legal requirements of computer security measures will be tightened.

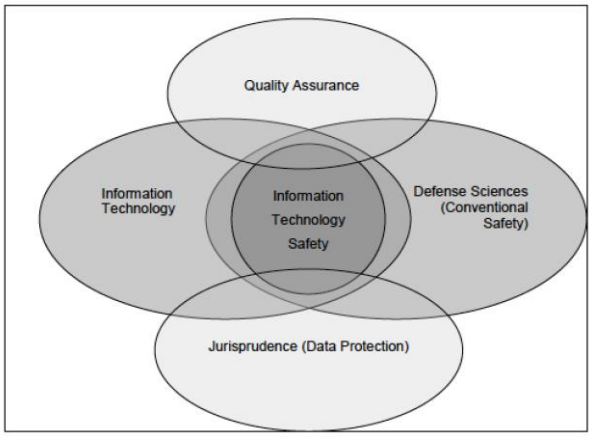

Figure 1 Data Protection, Defense, Information Technology

3. Overall Regulatory Framework

European Union has adopted the Data Protection Directive of 1995 (Directive 95/46/EC). The directive sets out compulsory rules for the protection of individuals and the handling of personal data. Through this regulation basic principles of data processing have to be followed by all the Member States. The first one is *transparency*, where the data subject has the right to access all data processed about him and to be informed when his personal data are being processed. The name and the address of the data subject have to be provided, as well as the purpose of the data processing, the recipients of the data and all other information required to ensure the processing is fair. (Article 10 and 11) Following Article 7 Member States shall provide that data may be processed only under the following criteria:

- User has given his consent (use an easy to read and to understand language, use large typefaces for consent)
- Data processing is necessary for the performance of a contract or prior to entering into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary in order to protect the vital interests of the data subject
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Furthermore, accordingly the legal framework, the personal and data protection is defined by the EU Legislation, as indicated in the:

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML)
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:es:NOT)
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users‟ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Text with EEA relevance (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:es:NOT)

4. Implications for MyGuardian Security Solution

Given the directives, the following dimensions of security must be adopted in MyGuardian:

- Confidentiality - is the property of preventing disclosure of information to unauthorized persons or systems. The loss of confidentiality of information can take many forms: someone looking over your shoulder while you have confidential information on the screen, when you publish private information, when a laptop containing sensitive information about a company is stolen, when it discloses confidential information over the phone etc. All these cases may constitute a violation of confidentiality.

- Integrity - For information security, integrity is the property you are looking to keep the data free of unauthorized modifications. The violation of integrity occurs when an employee, program or process (accidentally or maliciously) modify or delete important data that are part of the information, so it makes its contents remain unchanged unless modified by authorized personnel and this change is recorded, ensuring accuracy and reliability. The integrity of a message is obtained by attaching another set of data integrity checking: the digital signature is one of the cornerstones of information security.

- Availability - Is the property, quality or condition of information for being available to those who need to access to it, whether people, processes or applications. In the case of computer systems used to store and process information, the security controls used to protect it, and protected communication channels used to access it should be working properly. The goal is to provide MyGuardian services available at all times, preventing service disruptions due to power outages, hardware failures, and system updates. Ensuring availability also involves preventing denial of service attack. The availability as well as being important in the process of information security, is also varied in the sense that there are several mechanisms to meet the service levels required, such mechanisms are implemented in technological infrastructure, e-mail servers, database, web, etc., by using clusters or arrays, high availability equipment at the network level, mirrors, data replication, storage area networks (SAN), redundant links, etc. The range of possibilities will depend on what we want to protect and the level of service you want to provide.

- Authentication - is the property that allows identifying the generator of the information. For example when receiving a message from someone, make sure it is that someone who has commanded, and not a third person posing as the other (identity theft). In a computer system this factor is usually achieved with the use of user accounts and passwords.

Another part necessary to mention into MyGuardian project implementation are the security services to improve the security of data processing systems and information transfer. The security services are designed to counter security attacks and make use of one or more security mechanisms to provide the service.

For the success of this secure communication protocols, which are nothing more than a set of rules that govern in the transmission of data between communication devices to exercise confidentiality, integrity, authentication and non-repudiation of information. They are: (1) Cryptography (Data Encryption), deals with message encryption. A message is sent by the issuer is making transpositions or hides the message until it reaches its destination and can be decrypted by the receiver. (2) Logic (Structure and sequence). Carry out an order in which the message data grouped the meaning of the message and know when it will send the message. (3) Authentication. It is a validation of identification; it is the technique by which a process verifies that the communication partner is who is supposed to be and not an impostor.

To cover all these dimensions MyGuardian system development must consider privacy and security along the concepts of:

- Personal Data - Shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; (Directive 95/46/EC), Act CXII of 2011 on Informational Self-determination and Freedom of Information

- Data subject's consent - Shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. (Directive 95/46/EC), Act CXII of 2011 on Informational Self-determination and Freedom of Information Controller Natural or legal person or organization without legal personality, which alone or jointly with others determines the purposes and means of the control of the data; makes and executes decisions concerning data control (including the means used) or contracts a data processor to execute it.

- Personal Data Protection - It is a right included in Charter of Fundamental Rights of the EU (2000/C 364/01) Article 8 Protection of personal data: Everyone has the right to the protection of personal data concerning him or her. 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 or her, and the right to have it rectified.

MyGuardian compliance with these rules shall be subject to control by an independent authority

5. Privacy and Data Security: Geo-Localization

Due to the fact that MyGuardian concerns the privacy of seniors, we shall consider geo-location data as any personal data. Whatever is the nature of MyGuardian services, we know that geo-location data will play a significant role in the care process. We have to apply the same protection principles as for any personal data, even if the current European legal framework does not explicitly mention geo-location data as personal data.

6. Conclusions

All the entities participant in MyGuardian project are committed to taking appropriate technical, physical and organizational measures to protect against the MyGuardian users data from unauthorized access, unlawful processing, loss or accidental damage and unauthorized destruction. The data are stored in systems protected by secure network architectures and controlled entities from unauthorized access to applicant data by third parties. The organizations involved in the MyGuardian system development meet all safety and security measures for the protection of personal data and will follow the above-mentioned principles when developing the system and its services.