COVER PAGE

DELIVERABLE

Project Acronym: i-locate
Grant Agreement number: 621040
Project Title: Indoor/outdoor LOCation and Asset management Through open gEodata

D1.2 Regulatory constraints

Revision: 2.4
Authors:
Claudio Eccher (FBK), Elisa Morganti (FBK), Simona Anzivino (FBK), Scott Cadzow (C3L), Giuseppe Conti (TRILOGIS), Massimo Barozzi (TRILOGIS), Stefano Piffer (TRILOGIS), Catherine Delevoye (Technoport), Theo Arentze (TU/e), Sorin Pop (FiFIDAda), Daniele Miorandi (u-Hopper), Abdur Rahim Biswas (ZIGPOS), Erik Mademann (ZIGPOS), Cvelic Josipa (Rijeka), Ramona Falamas (Indsoft), Anastasios Trypitsidis (EPSILON), Sergio Farruggia (GISIG), Fabio Tenore (Municipality of Genova), Marco Morelli (Municipality of Genova), Tim Camilleri (Geosys), Massimo Bosio (TRE).

Project co-funded by the European Commission within the ICT Policy Support Programme		
Dissemination Level		
P	Public	X
C	Confidential, only for members of the consortium and the Commission Services	

REVISION HISTORY AND STATEMENT OF ORIGINALITY

Revision History

Revision	Date	Author	Organisation	Description
v0.0.1	6/03/2014	Simona Anzivino	FBK	1st draft and European
v0.0.2	6/03/2014	Simona Anzivino	FBK	Rovereto regulatory constraints
v0.0.3	7/03/2014	Cvelic Josipa	Rijeka	Croatia regulatory constraints
v0.0.4	7/03/2014	Stefano Piffer	Trilogis	Usability and inclusiveness
v0.0.5	7/03/2014	Anastasios Trypitsidis	EPSILON	Greece regulatory constraints
v0.0.6	7/03/2014	Catherine Delevoye	Technoport	Technoport regulatory constraints
v0.0.7	10/03/2014	Ramona Falamas	Indsoft	Albahospital, Brasov, Mnb,
v0.0.8	12/03/2014	Sorin Pop	Fida	Baiasprie regulatory constraints
v0.1	13/03/2014	Simona Anzivino	FBK	2st draft
v0.1.1	19/03/2014	Theo Arentze	TU/e	UMC regulatory constraints
v0.1.2	19/03/2014	Daniele Miorandi	u-Hopper	Electromagnetic compatibility
v0.1.3	19/03/2014	Sergio Farruggia	GISIG	Genova regulatory constraints
v0.1.4	20/03/2014	Abdur Rahim Biswas, Erik Mademann	ZIGPOS	ETSI certification and UNIDRES regulatory constraints
v0.1.5	20/03/2014	Giuseppe Conti	TRILOGIS	Review of first complete document
v1.0	25/03/2014	Simona Anzivino	FBK	3st draft
v1.0.1	25/03/2014	Scott Cadzow	C3L	Contribution about data
v1.0.2	26/03/2014	Tim Camilleri	Geosys	St James Hospital regulatory
v2.0	11/04/2014	Simona Anzivino	FBK	Consolidate draft
v2.1	15/04/2014	Sergio Farruggia, Theo Arentze	GISIG, TU/e	Revised draft
v2.2	18/04/2014	Massimo Bosio	TRE	Tremosine regulatory constraints
V2.3	22/04/2014	Giuseppe Conti	Trilogis	Final document including new contributions from pilot in Tremosine
V2.4	20/01/2015	Irene Facchin	Trilogis	Final Check

Statement of originality:

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

1 List of references

Number	Full reference
1	*Charter of Fundamental Rights of the European Union.* Available online at: www.europarl.europa.eu/charter/pdf/text_en.pdf
2	*European Convention for the Protection of Human Rights and Fundamental Freedoms.* Available online at: www.echr.coe.int/Documents/Convention_ENG.pdf
3	*World Medical Association Declaration of Helsinki. Ethical Principles for Medical Research Involving Human Subjects.* Available online at: www.wma.net/en/30publications/10policies/b3/17c.pdf
4	*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 1 January 1981, Strasbourg.* conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
5	*Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks, Paolo Guarda.* Available online at: eprints.biblio.unitn.it/1524/1/DataProtection_SecurityMeasures_Guarda.pdf
6	Available online at: europa.eu/rapid/press-release_IP-12-46_en.htm
7	*Directive 95/46/EC.* Available online at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
8	*Directive 2002/58/EC.* Available online at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
9	*Italian Personal Data Protection Code. Legislative Decree no. 196 of 30 June 2003.* Available online at: www.privacy.it/privacycode-en.html
10	Available online at: www.sabor.hr/fgs.axd?id=17074
11	Available online at: www.mvep.hr/zakoni/pdf/315.pdf
12	Available online at: narodne-novine.nn.hr/clanci/sluzbeni/2013_02_25_403.html
13	Available online at: www.mvep.hr/zakoni/pdf/319.pdf
14	Available online at: hidra.srce.hr/arhiva/263/33319/038991.pdf
15	Available online at: www.azop.hr/download.aspx?f=dokumenti/Razno/Regulation_on_the_procedure_for_storage_and_special_measures_relating_to_the_technical_protection_of_special_categories_of_personal_data.pdf

16	*Law 2472/97. Available online at: www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-APRIL010-EN%20_2_.PDF*
17	*Available online at: www.dgipi.ro/administrare/_uploads/_documente/26_20101019161007094188400_5.pdf*
18	*Available online at: www.spitalalba.ro/wp/wp-content/uploads/2013/07/Legea-nr.46-din-21-ianuarie-2003-Legea-drepturilor-pacientului.pdf*
19	*Available online at: dataprotection.ro/servlet/ViewDocument?id=35*
20	*Available online at: dataprotection.ro/servlet/ViewDocument?id=451*
21	*Available online at: dataprotection.ro/servlet/ViewDocument?id=861*
22	*Available online at: dataprotection.ro/servlet/ViewDocument?id=859*
23	*Available online at: www.legi-internet.ro/legislatie-itc/criminalitate-informatica/prevederi-legislative-privind-prevenirea-si-combaterea-criminalitatii-informatice/legea-1612003-pentru-prevenirea-si-sanctionarea-coruptiei.html*
24	*ISO 27001. Available online at: en.wikipedia.org/wiki/ISO/IEC_27001:2005*
25	*P. Kalampouka-Giannopoulou, Protection of the patient as a consumer, Nomiki Bibliothiki, Athens, 2011, p. 149, 166-*
26	*G.Vasilakopoulos, Security of electronic medical records: International trends and Greek reality in medical confidentiality, Sakkoulas Athens – Thessaloniki, 2006, p.306.*
27	*Annual Report of DPA, 2011, p.68. Available online at: www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2011/ARXH_PROSTASIAS_2011.PDF*
28	*P. Tsantila, Ch. Latsiou, Medical confidentiality in light of the personal data protection, Review of the Social Security Law, Vol.3-4, 2011, pp 161-167.*
29	*Law 2071/1992. Available online at: www.elinyae.gr/el/item_details.jsp?item_id=2736&cat_id=686*
30	*Available online at: www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/codul-civil.html*
31	*Available online at: spitalalba.ro/docs/date/ROF_2012.pdf*
32	*Available online at: www.spitalalba.ro/wp/wp-content/uploads/2014/02/REGULAMENT-DE-ORDINE-INTERIOARA2013-ROI.pdf*
33	*Available online at:*

	www.brasovcity.ro/documente/public/regulamente/Regulament_de_organizare_si_functionare.pdf
34	Available online at: www.brasovcity.ro/documente/public/regulamente/Regulament_intern.pdf
35	Available online at: www.brasovcity.ro/documente/public/regulamente/Codul%20de%20conduita%20al%20angajatilor.pdf
36	Available online at: www.brukenthalmuseum.ro/pdf/rof.pdf
37	*Van der Jagt Stibbe, F. (2012) The Netherlands. In: Data protection and privacy laws: Annual review. Financier Worldwide, Birmingham, UK.*
38	*Oostveen, M., and F. Zuiderveen Borgesius (2012) Netherlands: Amendment of the Telecommunications Act. In IRIS Legal Observations of the European Audiovisual Observatory. IRIS 2012-7:1/32.*
39	Available online at: ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf
40	Available online at: www.iuscomp.org/gla/statutes/BDSG.htm
41	*HIPPA Regulations.* Available online at: www.hhs.gov/ocr/privacy
42	*Malta Data Protection Act: Chapter 440.* Available online at: ec.europa.eu/justice/policies/privacy/docs/implementation/malta_en.pdf
43	Available online at: www.comune.genova.it/pages/privacy
44	Available online at: www.comune.genova.it/sites/default/files/privacy_schede_allegate_regolamento.pdf
45	Available online at: www.comune.genova.it/sites/default/files/privacy__schede_allegate_regolamento_2.pdf
46	Available online at: www.consiglio.provincia.tn.it/documenti_pdf/clex_25161.pdf
47	Available online at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:EN:PDF
48	Available online at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:108:0001:0014:en:PDF
49	Available online at: www.camera.it/parlam/leggi/deleghe/05082dl.htm
50	Available online at: www.camera.it/parlam/leggi/deleghe/06036dl.htm

51	Available online at: www.gazzettaufficiale.it/atto/stampa/serie_generale/originario
52	www.unesco.org/culture/natlaws/media/pdf/romania/rom_lege_182_romorof.pdf
53	Available online at: www.cimec.ro/Monumente/pdf/Legea-422-2001-republicata-2006.pdf
54	Available online at: www.cultura.abt.ro/Files/GenericFiles/Legea311-2003-2007-04-10.pdf
55	Available online at: www.brukenthalmuseum.ro/vizitare/index.html
56	Available online at: www.brasovcity.ro
57	IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).
58	Bluetooth Core Specifications. Available online at: https://www.bluetooth.org/en-us/specification/adopted-specifications
59	IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
60	ITU-R Radio Regulations. Available online at: www.itu.int/pub/R-REG-RR/en
61	Available online at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:247:0021:0055:en:PDF
62	Available online at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1993:169:0001:0043:EN:PDF
63	WAI (Web Accessibility Initiative). Available online at: www.w3.org/WAI/
64	WCAG (Web Content Accessibility Guidelines). Available online at: www.w3.org/WAI/intro/wcag
65	UAAG (User Agent Accessibility Guidelines). Available online at: www.w3.org/WAI/intro/uaag
66	ATAG (Authoring Tool Accessibility Guidelines). Available online at: www.w3.org/WAI/intro/atag.php
67	WAI-ARIA (Accessible Rich Internet Applications Suite). Available online at: www.w3.org/WAI/intro/aria
68	W3C (World Wide Web Consortium). Available online at: www.w3.org/
69	W3C Validator suite. Available online at: https://validator-suite.w3.org/
70	Communication from the Commission to the European Parliament, the Council, the

	European Economic and Social Committee and the Committee of the regions safeguarding privacy in a connected world a European data protection framework for the 21st century (COM/2012/09 final). Available online at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009
71	*Privacy code of Municipality of Genova. Available online at:* http://www.comune.genova.it/pages/privacy
72	*Regulation for handling sensitive data or judicial data of the Municipality of Genova. Available online at:* www.comune.genova.it/sites/default/files/regolamento_dati_sensibili_giudiziari.pdf
73	*Annexes to the regulation for handling sensitive data or judicial data of the Municipality of Genova. Available online at: www.comune.genova.it/sites/default/files/privacy__schede_allegate_regolamento_2.pdf*
74	Decree of the President of the Autonomous Province of Trento no. 27-129*. Available online at:* www.consiglio.provincia.tn.it/documenti_pdf/clex_25161.pdf

2 Table of Acronyms

Acronym	Description
ATAG	Authoring Tool Accessibility Guidelines
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
CC-ILDG	Comité de Coordination de l'Infrastructure nationale Luxembourgeoise de Données Géographiques
CE	Communautès Europèennes
CEPT	European Conference of Postal and Telecommunication Administration
ECC	Electronic Communications Committee
ECHR	European Convention for the protection of Human Rights and Fundamental Freedoms
EEA	European Economic Area
EMC	Electromagnetic compatibility
ERM	Electromagnetic compatibility and Radio spectrum Matters
ERP	Effective Radiated Power
ETSI	European Telecommunications Standards Institute
HER	Electronic Health Records
HIPAA	Health Insurance Portability and Accountability Act
HIPERLAN	HIgh PErformance Radio LAN
HW	Hardware
ICT	Information and Communications Technology
IDPC	Italian Data Protection Code
IEEE	Institute of Electrical and Electronic Engineers
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
ITU-R	Radiocommunication sector of the International Telecommunication Union

JCI	Joined Commission International
LR-WPAN	Low-Rate Wireless Personal Area Networks
MAC	Medium Access Control
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit (Dutch Post and Telecommunications Authority)
PHY	Physical Layer
R&TTE	Radio and Telecommunications Terminal Equipment
RF	Radiofrequency
RLAN	Radio LAN
SAR	Specific Absorption Rate
SRD	Short-Range Devices
SSID	Service Set Identifier
SW	Software
UAAG	User Agent Accessibility Guidelines
W3C	World Wide Web Consortium
WAI	Web accessibility initiative
WAI-ARIA	Accessible Rich Internet Applications Suite
WCAG	Web Content Accessibility Guidelines
WMA	World Medical Association

3 Executive Abstract

The goal of this document is twofold. On the one hand it will list all the reference norms that will have to be addressed during the creation of the i-locate system. On the other hand it will represent a comprehensive set of norms that will be used as baseline for contractual arrangements or for the definition of service level agreements as planned in later work packages of this project.

The scope of the document is to provide an overview of European, National and local regulatory constraints, in the context of the problem statements identified by the pilot user partners as detailed within ***D.1.1 – "Use cases description and Privacy Threat Vulnerability and Risk Analysis"***. The overview has been carried on with the support of the technical partners, to identify the requirements that the pilots will have to comply with from a regulatory/legal standpoint in terms of ethical issues, security and privacy, hardware characteristics and usability.

The analysis starts in the 4th chapter with the study of aspect related to ethics, privacy and security of personal data. In particular, after the presentation of the most relevant European regulations about the personal data management, informed consent and public space accessibility, it shows the National and local norms identified by the pilot user partners with the support of technical partners. It should be noted that often the text introduced within the following sections, which follows the reference to the legal framework, is either made of excerpt of the legal text (law, decree, etc.) or a translation of the text if this is another language than English.

All the other local regulatory constraints not included above but of interest for the implementation of the pilots are presented in the 5th chapter.

The rules that regulate hardware and software and, in particular electromagnetic compatibility with medical devices (particularly important for the hospital scenarios) are reported in the 6th chapter while usability norms are presented in the 7th chapter.

Table of Content

4 Ethical issues, security and privacy regulations

4.1 Fundamental rights

Charter of Fundamental Rights of the European Union

A number of articles within the **Charter of Fundamental Rights of the European Union** [1] clearly highlight several element of relevance for i-locate in terms of ethical, privacy and security issues. The following articles are particularly worth mentioning.

- **Article 3** - Right to the integrity of the person: Everyone has the right to respect for his or her physical and mental integrity. In the fields of medicine and biology, the following must be respected in particular:
  - The free and informed consent of the person concerned, according to the procedures laid down by law.
  - The prohibition of eugenic practices, in particular those aiming at the selection of persons.
  - The prohibition on making the human body and its parts as such a source of financial gain.
  - The prohibition of the reproductive cloning of human beings.
- **Article 7** - Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications.
- **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 that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

European Convention for the Protection of Human Rights and Fundamental Freedoms

The **European Convention for the protection of Human Rights and Fundamental Freedoms (ECHR)** [2] builds the framework for the development of specific legislations to protect the interest of the citizen when ICT is used in healthcare. In particular **Article 8** states that:

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Declaration of Helsinki

The **Declaration of Helsinki on Ethical Principles for Medical Research Involving Human Subjects** [3], which has been adopted by the World Medical Association (WMA), outlines ethical principles for medical research involving human subjects, including research on identifiable human material and data. According to its principles the physicians participating in medical research should protect the life, health, dignity, integrity, right to self-determination, privacy, and confidentiality of personal information of research subjects.

In medical research involving human subjects, the well being of the individual research subject must take precedence over all other interests. In particular the declaration states that “Every precaution must be taken to protect the privacy of research subjects and the confidentiality of their personal information and to minimize the impact of the study on their physical, mental and social integrity”.

4.2 Personal data management: privacy and security at EU and member States level

4.2.1 Europe

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 1 January 1981

The scope of **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** [4] is "to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them. There is a need for such legal rules in view of the increasing use made of computers for administrative purposes. Compared with manual files, automated files have a vastly superior storage capability and offer possibilities for a much wider variety of transactions, which they can perform at high speed. Further growth of automatic data processing in the administrative field is expected in the coming years *inter alia* as a result of the lowering of data processing costs, the availability of "intelligent" data processing devices and the establishment of new telecommunication facilities for data transmission."

The convention addresses also trans-border flow of personal data undergoing automatic processing or collected with the goal of being processed in an automatic manner.

The legal framework on privacy and security issues related to data protection within the EU is essentially represented by the "**Data Protection Directive**" and the **"ePrivacy Directive",** as detailed hereafter.

Data Protection Directive (95/46/EC) and ePrivacy Directive (2002/58/EC)

The **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** [7] and 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)** [8] provide indications about data processing.

The privacy principles are summarized as follows:

- The collection and processing of personal data shall neither intrude on the data subjects' privacy nor interfere with their autonomy and integrity.
- Personal data shall be collected and processed only after the person involved provides explicit consent.
- Personal data shall be collected for specified, lawful and legitimate purposes.
- The collection and processing of personal data shall be limited to the minimum necessary for achieving the specific purpose. This includes that personal data shall be retained only for the time necessary to achieve the specific purpose.
- The disclosure of personal data to third parties shall be restricted and only occur upon certain conditions.

- Personal data shall be accurate, relevant, and complete with respect to the purposes for which they are collected and processed.
- The data subject shall be able to check and influence the processing of his/her personal data.
- The processing of personal data, which are particularly sensitive for the data subject, shall be subject to more stringent protection measures than other personal data.
- Personal data shall be processed in a way that guarantees a level of security appropriate to the risks presented by the processing and the nature of the data. [5]

In relation to security of personal data processing, the main reference at the EU level is **Article 17** of Directive 95/46/EC according to which:

- "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
- "The Member States shall provide that the controller must, where processing is carried out on his/her behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures".

On 25 January 2012 the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy [6].

The major novelty of the proposed regulation is reported in the **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions safeguarding privacy in a connected world a European data protection framework for the 21st century (COM/2012/09 final)** [70] and include:

- A single set of rules on data protection, valid across the EU.
- Instead of the current obligation of all companies to notify all data protection.
- Activities to data protection supervisors the Regulation provides for increased responsibility and accountability for those processing personal data.
- Organisations will only have to deal with a single national data protection authority in the EU country where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when a company based outside the EU processes their data.
- Wherever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed.

- People will have easier access to their own data and be able to transfer personal data from one service provider to another more easily (right to data portability). This will improve competition among services. A 'right to be forgotten' will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it.
- EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.
- Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules [6].

4.2.2 Italy

The Italian transposition of the rules established at the European level is one of the most restrictive ones.

Legislative Decree 30 June 2003, n. 196

The reference in Italy is the Legislative Decree 30 June 2003, n. 196 "**Codice in materia di protezione dei dati personali**" (**Italian Data Protection Code - IDPC**) [9], that implemented the relevant European Directives. In particular, **Article 4**, par. 1, item d, of IDPC defines so-called "sensitive data" as follows: "personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life".

The Code provides also a specific regulation on the treatment of health data in Part II, Title V "Processing of personal data in the health care sector", **Articles 75-94**.

Article 3 of IDPC states the so-called "Data minimization principle" according to which "information systems and software shall be configured by minimizing the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively".

This principle represents an advanced rule in respect to the fulfilment provided by Title V and it imposes data controllers to adopt organizational measures to minimize the use of personal and identification data. That point can be reached by using anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity.

According to **article 37**, par. 1, item a, a notification to the Data Protection Authority is mandatory if the treatment involves: "genetic data, biometric data, or other data disclosing geographic location of individuals or objects by means of an electronic communications network".

The notification of processing operations shall have to be submitted to the Authority in advance of the processing and only once, regardless of the number of operations to be performed and the duration of the processing, and may concern one or more processing operations for related purposes. A notification shall only be effective if it is transmitted via the Data Protection Authority's

Website by using the ad-hoc form, which shall contain the request to provide all the pieces of information listed in **article 38**, par. 2.

A proper health data treatment should require, given the delicacy of the content, the adoption of security measures of technical nature.

The security measures provided in the IDPC are classified as:

- suitable and preventative security measures (Title V, Chapter I) and
- minimum-security measures (Title V, Chapter II).

The regulation is contained in **articles 31** and following, within the "Technical Specifications Concerning Minimum Security Measures (Annex B)", and in **article 3** on "Data Minimization Principle".

Article 31 ("Security Requirements") states: "Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimize, by means of suitable preventive security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected".

Chapter II of the IDPC, **article 33** ("Minimum Security Measures") states: "Within the framework of the more general security requirements referred to in Section 31, or else provided for by specific regulations, data controllers shall be required in any case to adopt the minimum security measures pursuant to this Chapter in order to ensure a minimum level of personal data protection".

Regarding the processing of personal data by electronic means, it shall only be allowed if the minimum-security measures below are adopted, in accordance with the arrangements laid down in the technical specifications as in Annex B (**article 34**):

- Computerized authentication;
- Implementation of authentication credentials management procedures;
- Use of an authorization system, that can allow the user to access to specific resource to pinpoint the authorization profile;
- Regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenance of electronic means;
- Protection of electronic means and data against unlawful data processing operations, unauthorized access and specific software;
- Implementation of procedures for safe keeping of backup copies and restoring data and system availability;
- Implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

4.2.3 Croatia

Constitution of the Republic of Croatia

Article 37 of the **Constitution of the Republic of Croatia** [10] states:

- Everyone shall be guaranteed the safety and secrecy of personal data. Without consent from the person concerned, personal data may be collected, processed and used only under conditions specified by law;
- Protection of data and supervision of the work of information systems in the Republic shall be regulated by law;
- The use of personal data contrary to the purpose of their collection shall be prohibited.

Act on personal data protection

Personal data protection and supervision over collecting, processing and use of personal data in the Republic of Croatia is regulated by **the Act on personal data protection** (Official Gazette No. 103/03, 118/06 and 41/08, 130/11; consolidated text: OG 106/12) [11].

The main article of relevance are:

- **Article 2**, which states that personal data means any information relating to an identified natural person or an identifiable natural person (hereinafter: 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.
- **Article 6**, which states that personal data must be relevant for the accomplishment of the established purpose and shall not be collected in quantities more extensive than necessary for achieving the purpose defined.
- **Article 7**, which states that personal data may be collected and subsequently processed with the consent of the data subject, or in cases established by law. In cases of personal data collecting and processing with the consent of the data subject, such personal data may be processed only for the purpose the data subject has given his/her consent for. Personal data may be collected and subsequently processed without the consent of the data subject:
    - For the purpose of carrying out legal obligations to which personal data filing system controller is subject, or
    - For the purpose of protecting the life or physical integrity of the data subject or another person in cases when the data subject is physically or legally unable to give his/her consent, or
    - If data 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 personal data filing system controller, or
    - If the data subject discloses such data on his/her own.

In cases referred to in Paragraph 1, Subparagraph 1 and Paragraph 3, Subparagraph 4 of the Article the data subject has the right to revoke his/her consent at any time, and request the termination of further processing of his/her data, unless these data are processed for statistical purposes when personal data can no longer be used for the identification of the person it relates to.

Personal data pertaining to underage persons may be collected and subsequently processed in accordance with the Act by applying special protection measures prescribed by special acts.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

As a Member State of the Council of Europe, the Republic of Croatia has accepted provisions of the Convention 108 (**Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**).

Right to Information Access Act

Furthermore, right to access to information is regulated by the **Right to Information Access Act** (Official Gazette 25/13). The Act also lays down the principles of right to access, exemptions from right to access and process for exercise and protection of right to information access. The aim of the Act is to enable and ensure information to natural and legal persons through the openness and availability of public authority actions, pursuant to the legislation. [12]

Information Security Act

The **Information Security Act** (Official Gazette No. 79/07) establishes the term information security, information security measures and standards, fields of information security, and competent authorities responsible for the adoption, implementation, and supervision of information security measures and standards [13]. The most relevant articles are:

- **Article 8** identifies that the fields of information security for which information security measures and standards are set forth are as follows:
  - Security check,
  - Physical security,
  - Data security,
  - Information system security,
  - Business co-operation security.
- **Article 9** states that:
  - Security check is a field of information security in the scope of which information security measures and standards are established that apply to the persons with access to classified information.
  - Persons referred to in paragraph 1 shall obtain a certificate of security check of the person.

- Authorities and legal persons referred to in **article 1**, paragraph 2, which use classified information assigned the confidentiality level “Confidential”, “Secret”, and “Top Secret”, shall set up:
    - a list of persons who have access to classified information,
    - a register of received certificates with validity thereof.

- **Article 10** states that:
    - Physical security is a field of information security in the scope of which information security measures and standards are established for the protection of facilities, rooms, and apparatus containing classified information.
    - Authorities and legal persons referred to in **article 1**, paragraph 2, which use classified information with the assigned confidentiality level “Confidential”, “Secret” and “Top Secret”, shall categorize the facilities and rooms into security zones, as set forth by the information security measures and standards.
- **Article 11** states that:
    - Data security is a field of information security for which information security measures and standards are established that apply as general protective measures for preventing, detecting and rectifying the damage caused by the loss or unauthorized disclosure of classified and unclassified information.
    - Authorities and legal entities referred to in **article 1**, which use classified and unclassified information within their scope of operation, shall apply the procedures for handling classified and unclassified information, about the content, way of maintaining records of the carried out access to classified information, and the supervision of data security, and the laid down information security measures and standards.
- **Article 12** states that:
    - Information system security is the field of information security in the scope of which information security measures and standards are established for classified and unclassified information, that is saved or transmitted in the information system, and the protection of integrity and availability of the information system in the process of planning, design, construction, use and termination of operation of the information system.
    - Security accreditation of information systems shall be carried out for information systems where classified information assigned the confidentiality level “Confidential”, “Secret” and “Top Secret” is used.
    - Persons who take part in the process referred to in paragraph 1 shall have to possess a certification of the level “Top Secret”, or one level higher that the highest level of confidentiality of the classified information which is saved or transmitted in the information systems under their jurisdiction.

- Physical protection measures of the area where the information systems are placed shall be implemented in accordance with the highest confidentiality level of the classified information that is processed, saved or transmitted therein.
- Central state authorities responsible for information security shall set up a register of certified equipment and apparatus that are used in the classified information system assigned the levels of “Confidential, “Secret”, and “Top Secret”.

The register of certified equipment and apparatus shall be set up based on taking over relevant registers from international organizations, or by own certification in accordance with the relevant international standards.

Electronic Communications Act

The **Electronic Communications Act** (Official Gazette No. 73/08, 90/11, 133/12, 80/13) regulates the field of electronic communications, including the use of electronic communications networks and the provision of electronic communications services, the provision of universal services and the protection of rights of users of services, construction, installation, maintenance and use of electronic communications infrastructure and associated facilities, competition conditions and rights and obligations of participants in the market of electronic communications networks and services, addressing, numbering and management of the radio frequency spectrum, digital broadcasting, data protection and security in electronic communications and the performance of inspection and expert supervision and control in electronic communications, as well as the establishment of a national regulatory authority for electronic communications and postal services and its organization, scope and competence, including the decision-making procedure and resolution of disputes concerning electronic communications [14].

Regulation on the Procedure for Storage and Special Measures Relating to the Technical Protection of Special Categories of Personal Data

Croatia has very detailed security measures set forth in **the Regulation on the Procedure for Storage and Special Measures Relating to the Technical Protection of Special Categories of Personal Data** (Official Gazette No. 103/03). This Regulation lays down:

- measures, tools and conditions for the storage, safety and protection and for the transfer of special categories of personal data and the corresponding data filing systems;
- measures for the maintenance and control of correct functioning of the computer and telecommunication equipment and of the software of the system for the maintenance ("system") of filing systems containing special categories of personal data;
- provision of working premises for such equipment; persons authorized for the implementation of anticipated measures, and persons competent for the supervision of their implementation [15].

4.2.4 Greece

In Greece an independent administrative agency, the Data Protection Authority, was founded and operated since November 1997, according to the **Law 2472/97** [16]. The fundamental principle of the Authority is that “every citizen should always be able to know who, where, when, how and why processes his/her personal data.”

Greek Law on the protection of individuals and the protection of personal data as supplemented by the decisions of the Chairman of the Commission for Personal Data Protection

The management and protection of personal data of the visitor/user of a website and of online services are subject to relevant provisions of Greek Law (**Law 2472/1997**) on the protection of individuals and the protection of personal data as supplemented by the decisions of the Chairman of the Commission for Personal Data Protection, **P.A. 207/1998** and **79/2000** and **article 8** of **Law 2819/2000** and **Law 2774/1999** and European law (**Directives 95/46/EP** and **97/66/EP**).

Greek Constitution

Besides the Data Protection Law, **article 9A** was added to the Greek Constitution during the Constitutional Revision of 2001 and it provides for the protection of personal data and the establishment of the relevant independent authority, i.e. the Greek Data Protection Authority. The new Article reads as follows: "All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is established and operates as specified by law". Generally speaking the Greek data protection law is quite similar to the European directive.

With regard the abovementioned and as a general comment regarding Mitera HOSPITAL pilot, it has to be clearly stated that no medical information will be stored in i-locate application apart from Patient Name; Phone Number; and Medical Departments that he/she will visit. Therefore, no conflict between the regulations and the implementation of the pilot will occur.

4.2.5 Luxembourg

Law of 2 August 2002 on the Protection of Persons

Directive 95/46/EC on data protection (Data Protection Directive) has been implemented in Luxembourg through the **Law of 2 August 2002 on the Protection of Persons** with regard to the Processing of Personal Data, as modified by the **Law of 27 July 2007**.

According to this law, health data is a special category of personal data, considered as sensitive. It includes any information about the data subject's physical or mental state, including genetic information. The data subject must give its express consent to the processing of any health data, except if the processing is necessary:

- to protect the vital interests of the data subject,
- in the public interest for historical, statistical or scientific reasons,
- for the purpose of preventive medicine,
- for the purposes of medical diagnosis,
- for the provision of care or treatment that may be carried out by the medical authorities or research projects approved under the legislation applicable to biomedical research,
- for the management of healthcare services.

According to the **Law of 2 August 2002 on the Protection of Persons** with regard to the Processing of Personal Data, as modified by the **Law of 27 July 2007**, localisation and tracking of people is considered especially sensitive in Luxembourg when performed by an employer on its employees, considering the subordination link between the parties. Localisation and tracking require the prior authorisation of the Commission for Data Protection and can only be authorised in very specific cases.

In any other situation, localisation and tracking is a mere processing of personal data, however regulated since it is being made for supervision purposes. Data subjects must be informed by appropriate means such as signage, circulars and/or letters sent by registered post or electronic means of the processing.

Consent of the data subject is required except in private places where the resident legal person is the controller of the data. Consent can be given in any form, including online, provided that it is free, specific (given for determined processing) and informed (that is, the data subject must have given his consent with the full knowledge of the facts).

The prior information that must be given to data subjects about data processing includes:

- The identity of the data controller and its representative, if any.
- The purpose(s) of the data processing.
- The data or categories of data that are to be processed.
- The recipients or categories of recipients to whom such data can be disclosed.
- Their rights to access and rectify their data and oppose the data processing, and in this case the consequences of the decision.
- Any information that may be deemed necessary to ensure fair data processing, given the circumstances under which the data are collected.

Relevant information must be transmitted, at the latest, at the time the personal data is collected, if collected directly from the data subjects. The controller must ask the prior authorization of the National Commission for Data Protection before processing the data if the data is recorded. Lastly, data cannot be kept for longer than 3 months.

4.2.6 Romania

Romanian Constitution

The Romanian Constitution adopted in 1991 recognizes under Title II (Fundamental Rights, Freedoms and Duties) the rights of privacy, inviolability of domicile, freedom of conscience and expression.

In particular. **article 26** states that public authorities shall respect and protect intimacy, family and private life.

Government Decision regarding the protection of the employ/office classified information

Another relevant act is the **Government Decision 781 of August 5th, 2002 regarding the protection of the sensitive information within working environments [17]**, which was published in the official gazette no. 575 of August, 5th, 2002.

The national standards for the protection of classified information in Romania, approved by Government Decision no. 585/2002, shall apply accordingly to sensitive employment-related information. The decision specifies:

- Classification, declassification and minimum protection measures.
- General rules of evidence, preparation, storage, processing, copying, handling, transportation, transmission and destruction.
- Obligations and responsibilities of public authorities and institutions managers, companies and other legal entities.

Law on patient rights

According to **Law no. 46 of 21.01.2003 on patient rights** published on Official Journal no. 51 of 29.01.2003 [18], the following principles apply:

- **Article 2**. Patients have the right to the highest quality care that the society can provide in accordance with human financial and materials resources.
- **Article 3**. The patient has the right to be respected as a human person, without any discrimination.
- **Article 20**. The patient cannot be photographed or filmed in a medical unit without his/her consent, unless the images are necessary for diagnosis or treatment and to avoid suspicion of a medical fault.

The right to information confidentiality and privacy of patient are detailed in CHAPTER IV within the following articles.

- **Article 21**. All information on patient conditions, results of investigations, diagnosis, prognosis, treatment, personal data are confidential even after death.
- **Article 22**. Confidential information can be provided only if the patient explicitly gives its consent or if expressly required by law.
- **Article 24**. The patient has access to personal medical data.
- **Article 25**. Any interference in the private and family life of the patient is prohibited, with the exception where this interference positive influence diagnosis, treatment or care given and only with patient consent. Are considered exceptions the cases when a patient is dangerous to himself or to public health.

Law on the Protection of Individuals

A further relevant law is **No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data** [19], amended and completed, published in the Official Journal of Romania, Part I, No. 790/12 December 2001; adopted by the Chamber of Deputies in the session of the 22nd of October 2001, in accordance with the provisions of Article 74 paragraph (2) of the Romanian Constitution.

The Law No 677/2001 transposes into domestic legislation the **Directive 95/46/EC** and it establishes the fundamental legal framework for the protection of individuals with regard to processing of personal data in Romania. The purpose of this law is to guarantee and protect the individual's fundamental rights and freedoms, especially the right to personal, family and private life, with regard to the processing of personal data. The present law applies to personal data processing, performed, totally or partially, through automatic means, as well as to the processing through means other than automatic, which are part of, or destined to, a personal data filing system.

For the purposes of this law, the following terms are defined:

- **Personal data**: any information referring to an identified or identifiable person. In turn, an identifiable person is a person that can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific factors of his physical, physiological, psychological, economic, cultural or social identity.
- **Personal data processing**: any operation or set of operations that is performed upon personal data, by automatic or non-automatic means, such as collecting, recording, organizing, storing, adapting or modifying, retrieval, consultation, use, disclosure to third parties by transmission, dissemination or by any other means, combination, alignment, blocking, deletion or destruction.
- **Storage**: keeping the collected personal data on any type of storage support.
- **Personal data filing systems**: any organized personal data structure that may be accessed according to some specific criteria, regardless of the fact that this structure is distributed according to functional or geographical criteria.
- **Data controller**: any natural or legal person, including public authorities, institutions and their legal bodies, that establishes the means and purpose of the personal data processing; if the purpose and means of the personal data processing is set out or based on a legal provision, the data controller shall be the natural or legal person assigned as data controller by that specific legal provision.
- **Data processor**: a natural or legal person, of private or public law, including public authorities, institutions and their legal bodies, which processes personal data on the data controller's behalf.
- **Third party**: any natural or legal person, of private or public law, including public authorities, institutions and their local bodies other than the data subject, than the controller, or the processor who, under direct authority of the controller or of his processor, is authorized to process data.
- **Recipient**: any natural or legal person, of private or public law, including public authorities, institutions and their local bodies, to whom the data are disclosed, regardless of the fact that it is a third party or not; the public authorities which receive data in accordance with a special type of inquiry competence will not be considered consignees.
- **Anonymous data**: data that, due to its specific origin or specific manner of processing, cannot be associated to an identified or identifiable person.

The most relevant articles of Law No 677/2001 are:

- **Article 4**, which states that personal data to be processed must be:
  - Processed fairly and in accordance with the existing legal provisions.
  - Collected for specific, explicit and legitimate purposes. Further processing of personal data for statistical, historical or scientific research, will not be considered incompatible with the purpose they were initially collected for, if it is carried out according to the provisions of the law, including those referring to the notification submitted to the supervisory authority, as well as according to the guarantees regarding personal data processing, set out by the legal provisions on statistics' activity or the historical or scientific research.
  - Adequate, pertinent and non-excessive in relation to the purpose for which they are collected and further processed.
  - Accurate and, if necessary, updated. For this purpose, appropriate measures shall be taken in order to erase and/or rectify inaccurate or incomplete data, from the point of view of the purpose for which they were collected and later processed.
  - Stored in such a manner that allows the identification of the data subject only for the time limit required to fulfil the purposes for which they are collected and later processed. The storage of data for a longer period of time than the one mentioned, for statistical, historical or scientific research purposes, shall be carried out in accordance with the guarantees regarding personal data processing, provided in the relevant legal framework, and only for the period of time required to achieve these purposes.
- **Article 8**, on processing of personal data with an identification function, which states that:
  - The processing of the personal identification number or of other personal data with a general identification function may be carried out only if:
    - The data subject has given his/her express and unequivocal consent; or
    - The processing is expressly stated by a legal provision.
  - The supervisory authority may establish other situations in which the processing of data may be carried out, only after adequate guarantees have been provided in order to observe the data subject's rights.
- **Article 9** on processing personal data regarding the state of health, which states:
  - The processing of health data may be carried out only by, or under the supervision of, medical staff who are under a pledge of professional confidentiality, except for the cases when the data subject has given, in writing, his/her unequivocal consent and as long as the consent has not been withdrawn, as well as except for the cases when the data processing is necessary for the prevention of an imminent danger, the prevention of a criminal offence or the prevention of the result of such an action or for the removal of the damaging results of such an action.
  - The medical staff, health institutions and their staff may process personal health data without the authorization of the supervisory authority only when the data processing is

required in order to protect the data subject's life, physical integrity or health. When the mentioned purposes refer to other people or to the general public and the data subject has not given his/her written and unequivocal consent, the preliminary authorization of the supervisory authority must first be demanded and obtained. The processing of personal data is forbidden beyond the limits of the authorization.

- Except for emergency reasons, the authorization may be given only after consulting the Romanian Medical College.
- Personal health data may only be collected from the data subjects themselves. Exceptionally, these data can be collected from other sources only when it is required in order not to compromise the processing's purpose, and when the data subject cannot or doesn't wish to provide them.

The rights of the data subject in the context of personal data processing are further analysed in Chapter IV of the law and, in particular, in the following articles:

- **Article 12**: Informing the Data Subject
- **Article 13**: The Right of Access to Data
- **Article 14**: The Right of Intervention upon the Data
- **Article 15**: The Right to Object
- **Article 17**: The Right Not to be Subject to an Individual Decision
- **Article 18**: The Right to Refer to a Court of Law
- **Article 19**: Confidentiality of Data Processing
- **Article 20**: Security of Data Processing. In particular the following statements are made:
  - It is the data controller's obligation to apply adequate technical and organizational measures in order to protect the data against accidental or unlawful destruction, loss, alteration, disclosure or unauthorized access, notably if the respective processing involves the data's transmission within a network, as well as against any other form of illegal processing.
  - These measures shall ensure, depending on the state of the art techniques employed and the costs, adequate security against processing risks as well as observing the nature of the data that must be protected.
  - When appointing a data processor, the data controller has the obligation to assign a person who presents sufficient guarantees regarding technical security and the organizational measures concerning the data to be processed, as well as the obligation to ensure that the assigned person complies with these measures.
  - The supervisory authority may decide, in individual cases, that the data controller should adopt additional security measures, except such measures that regard the guaranteed security of telecommunication services.
  - Data processing performed by an appointed data processor shall be initiated following a written contract which should necessarily contain the following:

- The processor's obligation to act strictly in accordance with the instructions received from the data controller;
- The fact that accomplishing the obligations also applies to the data processor. The minimum security requirements shall be issued by the supervisory authority and shall be periodically updated, according to the technological progress and the accumulated experience.

- Any person who acts under the authority of the data controller or of the data processor, including the data processor, who has access to personal data, may process them only in accordance with the data controller's specific instructions, except when the above-mentioned person's actions are based on a legal obligation.

Ratification of the Convention on the protection of individuals

Law no. 682 / 28th November 2001 ratifies the Convention on the protection of individuals with regard to automatic processing of personal data [20], with its annex addressing the protection of individuals with regard to automated processing of personal data.

Order on the minimum safety requirements for personal data processing

It is also worth mentioning the **order no. 52 dated April 18, 2002** which stated the minimum safety requirements for personal data processing [21], as published in the Official Journal no. 383 of June 5, 2002.

These minimum safety requirements for personal data processing set the grounds for controllers to adopt and implement appropriate technical and organisational measures to ensure the confidentiality and integrity of personal data. Accordingly, the controllers shall set their own safety procedures and policies.

The minimum safety requirements for personal data processing cover several aspects, the most important being the following:

- **User's identification and authentication**. A user is any person that acts under the controller's, or the authorised representative's authority, with an acknowledged access right to personal databases.
- **Access type**. The users shall access only personal data necessary to fulfil their job related tasks. In order to do so, the controllers shall set the access types according to the functionality (such as: administration, entering, processing, saving etc.), and according to the actions to be performed on the personal data (such as: writing, reading, deleting etc.), and shall also set out the procedures for these access types.
- **Data collection**. The controller designates authorised users for personal data collection and input within an IT system.
- **Back-ups**. The controller shall set the time frames for carrying on back ups of personal data, and of the software used for computer processing.
- **Access to files**. The controller shall take measures to ensure that any access to databases containing personal information is registered either in an log file –in case of automatic

processing- or in a registry for non-automatic processing of personal data, as determined by the controller.

- **Telecommunication Systems**. The controller shall periodically check the authentication and the access types in order to detect any malfunctions regarding the use of the telecommunication systems.
- **Employees' Training**. During the users' training courses, the controller shall inform them on the provisions of Law 677/2001 regarding the protection of individuals with regard to personal data processing and the free flow of such data, on the minimum safety requirements for personal data processing, and on the risks involved by personal data processing, according to the user's specific activity.

Law on the processing of personal data and the protection of privacy in electronic communications sector

The **law no 506/2004** on the processing of personal data and the protection of privacy in the electronic communications sector [22], which was published in the Official Journal of Romania, Part I, no. 1101 of November 25 2004, closely follows the Directive 2002/58/CE of the European Parliament and the Council on personal data processing and privacy protection in the electronic communication sector.

The law establishes the specific conditions for safeguarding the right to privacy with respect to the processing of personal data in the electronic communications sector. The provisions of this law apply to the providers of public electronic communications networks and of publicly available electronic communications services, as well as to the providers of value added services and of directories of subscribers who, in the frame of their commercial activity, are processing personal data.

The most important topics addressed by the law regard:

Security measures. In fact, according to the law, the provider of a publicly available el electronic communications service must take appropriate technical and organisational measures to safeguard security of its service. With respect to network security, if necessary, the provider of the publicly available electronic communications service shall take those security measures in conjunction with the provider of the public electronic communications network. Having regard to the state of the art and the cost of their implementation, the measures taken shall ensure a level of security appropriate to the risk presented. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must:

- Inform the subscribers of such risk and of the possible consequences;
- Inform the subscribers of any possible remedy;
- Inform the subscribers of the likely costs involved to eliminate the risk.

- **Confidentiality of the communications.** Confidentiality of communications and the related traffic data by means of public electronic communications networks and publicly available electronic communications services must be guaranteed.

Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data are prohibited, except for the following cases:

- These operations are carried out by the users who participate in that communication;
- The users who participate in that communication have previously given their written consent;
- These operations are carried out by the competent authorities, under the conditions set out by the legal provisions in force.

The provisions of previous paragraphs shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

The use of an electronic communications network to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that:

- The subscriber or user concerned was provided with clear and comprehensive information in accordance with Art. 12 of Law no. 677/2001, inter alia about the purposes of the storage or access to information stored.
- The subscriber or user concerned was offered the possibility to refuse such storage or access to information stored.

The previous provisions shall not prevent the technical storage or access in the following cases:

- When these operations are performed for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network.
- When these operations are strictly necessary for the provision of an information society service explicitly requested by the subscriber or user.

Anti-corruption law

According to the **anti-corruption law 161/2003 [23]**, as published in the Official Journal on 21/04/2003: Title III, the following provisions are defined in order to help preventing and fighting cyber-crime:

- “Data on the users” are represented by any information that can lead to identifying a user, including the type of communication and the serviced used, the post address, geographic address, IP address, telephone numbers or any other access numbers and the payment means for the respective service as well as any other data that can lead to identifying the user.
- ”Security measures” refer to the use of certain procedures, devices or specialised computer programmes by means of which the access to a computer system is restricted or forbidden for certain categories of users.

The following offences against the confidentiality and integrity of data and computer systems are identified:

- Illegal access to a computer system.
- Illegal interception of any transmission of computer data that is not published to, from or within a computer system.
- Illegal alteration, deletion or deterioration of computer data.
- Unauthorised data transfer from a computer.
- Unauthorised data transfer by means of an information data storing means.
- Serious hindering, without right, of a computer system operation, by the introduction, transmission, altering, deleting or deteriorating computer data or by restricting the access to these data.

The law also defines the following computer-related offences:

- Input, alteration or deletion, without right, of computer data or restriction, without right, of the access to these data, resulting in inauthentic data, with the intent to be used for legal purposes. 3
- Causing the loss of property to a person by the input, alteration of deletion of computer data, by restricting the access to such data or by preventing in any way the operation of a computer system, in order to obtain an economic benefit for oneself or for another.

According to the law no. 677/2001**, location data** is defined as any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

With regard to **location data and other traffic data** the following provisions apply:

- Where location data other than traffic data, relating to users or subscribers of public electronic communications networks or publicly available electronic communications services, can be processed, such data may only be processed in the following situations:
  - The data concerned are made anonymous;
  - With the prior express consent of the user or subscriber to whom that data relate, to the extent and for the duration necessary for the provision of a value added service;
  - When the value added service with user location function is intended for one-way undifferentiated transmission of information to users.
- The provider of the publicly available electronic communications service must make available to the user or subscriber, prior to obtaining his/her consent, information on:
  - The type of location data other than traffic data which will be processed;
  - The purposes and duration of the processing;
  - The potential transmission of data to a third party for the purpose of providing the value added service.

- The users or subscribers giving their consent for the processing of data shall have the right to withdraw their consent for the processing of data at any time or to temporarily refuse the processing of each connection to the network or for each transmission of a communication. The provider of the publicly available electronic communications service must make available to users or subscribers a simple means, free of charge, to exercise these rights.
- Processing of location data other than traffic data may only be carried out by the persons acting under the authority of the provider of the public electronic communications network or publicly available communications service or of the third party providing value added services, and is allowed only to the extent it is necessary for the purposes of providing the value added service.

4.2.7 The Netherlands

Dutch Data Protection Act

The **Dutch Data Protection Act** ("wet bescherming persoonsgegevens") implements the European Privacy Directive 95/46/EC and is therefore based upon same principles as the data protection laws in the other EU countries [37]. The Dutch implementation closely follows the structure and wording of the Directive. In the Netherlands, opportunities for the national regulatory body to impose fines are rather limited compared to neighbouring EU nations. There are exceptions, for example, some forms of processing are more restricted than in other EU countries.

In 2012, amendments were made to the Dutch Data Protection Act aimed at relieving the administrative burden that rests upon the data controller. The most important change is that a permit from the Dutch Ministry of Security and Justice for the transfer of personal data to a third country is no longer necessary when a data controller uses the unchanged Standard Contractual Clauses which have been adopted by the European Commission.

Another important change is that an explicit opt-in should be obtained for the use of cookies. Companies will not be allowed to obtain permission via the browser settings. The rationale of the Act is that the person concerned should have provided his or her permission for the use of the data. When the data are asked to the person him or herself than he or she should be informed in advance about how the data will be used. Moreover the permission may be withdrawn at any moment in time, after which the use of the data under concern must be stopped. So, formally admission must be asked for creation of a cookie and using the cookie to create a personal profile of the user. Apart from the obligation to provide this information in advance, persons whose data are included in a file have the right to view their data and to know how and for what purpose they are used.

With regard to **localisation and tracking of people,** geolocation data which can be linked to persons is regarded as person data and, hence, legislation in the area of localization and tracking people is covered by the same Dutch Data Protection Act.

There is no special legislation in the area of tracking and tracing. However, the interpretation of the law in this area has been developed in recent years in the context of what providers of navigation systems, such as TomTom, may and may not do regarding storage and use of tracking data. The Dutch Data Protection Act requires that the person tracked:

- Is informed in advance correctly and completely about how and for what purpose the data is used and
- Has given his or her permission to use the data for this.

This is not different than in the general case of person data. However, it is stressed that the fact that someone (through his mobile device) is sending signals (e.g. SSID) allowing a third party (e.g., Google) to localize the person in time and space does not count as permission. In other words, it is not allowed to tap the data unless the person has explicitly provided permission to do so.

Based on this law it is not allowed to use real-time information on online devices and smartphones even if this is for the purpose of obtaining traffic congestion information (as TomTom does) without permission of the user of the navigation system. After having been warned TomTom has undertaken action and have now included the explanation and permission request in their navigation system software.

Furthermore, interpretation of the law in this area has been developed in recent years in the context of employers tracking and tracing their employees. Employers wishing to install and use a tracking and tracing system for their employers must have a Tracking en Tracing Policy where they show three requirements in particular:

- The checking (tracking and tracing) must have a justified goal. The committee for the protection of person privacy considers the following goals as justifiable:
  - Safety of the employees;
  - Protection of the business car (for example, against theft);
  - Optimization of management of trips for the business purposes (help services, taxi services etc.)
  - Monitoring the performances of the employee.
- The checking must be proportional to the goal.
- The employees must be informed.
- Employees wishing to install a tracing and tracking system must communicate it to the committee for the protection of person privacy.

4.2.8 Germany

Federal Data Protection Act

The reference law is the **Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)** whose most important provisions are illustrated below:

- **Article 4 on admissibility of data processing and use**, states:
  - Processing and use of personal data shall be admissible only if the BDSG or any other legal provision permits or prescribes them or if the data subject has consented.

- When consent is obtained from the data subject, he or she shall be informed of the purpose of storage and of any envisaged communication of his data and, at his or her request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, the declaration of consent shall be made distinguishable in its appearance.
- In the field of scientific research, a special circumstance shall also be deemed to exist where the defined purpose of research would be impaired considerably if consent were obtained in writing. In such case the information to be collected and the reasons from which considerable impairment of the defined purpose of research would arise shall be recorded in writing.

- **Article 5 on Confidentiality**, states that persons engaged in data processing shall not process or use personal data without authorization (confidentiality). On taking up their duties, including whenever they work for private bodies, they shall be required to give an explicit commitment to maintain such confidentiality. This undertaking shall continue to be valid after termination of their activity.
- **Article 6 on inalienable rights of the data subject**, states:
  - The person's right to be informed (articles 19, 34) and to correction, erasure or blocking (articles 20, 35) may not be excluded or restricted by a legal transaction.
  - If the data are stored in a data file which can be stored by several bodies and if it is not possible to identify the controller of the data file, the person may approach any of these bodies. Such body is obliged to forward the request to the controller of the data file. The person shall be informed of the forwarding of the request and of the controller of the data file. Public prosecution and police authorities as well as public finance authorities may, as long as they store personal data to perform their legal duties within the area of application of the Fiscal Code for monitoring and control purposes, inform the Federal Commissioner for Data Protection instead of the person.
- **Article 7 on compensation by public bodies**, states:
  - Where a public body causes harm to the person through automated processing of his or her personal data that is inadmissible or incorrect under the provisions of BDSG or other data protection provisions, such body is obliged to compensate the person for the harm thus caused, irrespective of any fault.
  - In grave cases of violation of privacy, the person shall receive adequate pecuniary compensation for the immaterial harm caused.
  - If, in the case of a data file, several bodies are entitled to store the data and the injured person is unable to ascertain the controller of the data file, each body shall be liable.
  - Where several parties are responsible they shall be jointly and severally liable.
- **Article 8 on compensation by private bodies**, states that, if a person asserts a claim against a private body for compensation because of automated data processing that is inadmissible or incorrect under the BDSG or other data protection provisions, and if it is

disputed whether the harm caused results from a circumstance for which the controller of the data file is responsible, the burden of proof shall rest with the controller of the data file.

- **Article 9 on technical and organizational measures**, states that public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organizational measures necessary to ensure the implementation of the provisions of the BDSG.
- **Article 11 on commissioned processing or use of personal data**, states:
  - Where other bodies are commissioned to process or use personal data, the responsibility for compliance with the provisions of BDSG and with other data protection provisions shall rest with the principal.
  - The agent shall be carefully selected, with particular regard for the suitability of the technical and organizational measures taken by them. The commissioning shall be stated in writing, specifying the processing and use of the data, the technical and organizational measures and any sub-contracting.
  - The agent may process or use the data only as instructed by the principal. If the agent thinks that an instruction of the principal infringes the BDSG or any other data protection provisions, he or she shall point this out to the principal without delay.

The second part of the **Federal Data Protection Act** specifically addresses the issue of data processing by public bodies, with the first chapter focusing on the establishment of the legal basis for data processing, as follows.

- **Article 12 on scope**, states:
  - The provisions shall apply to public bodies of the Federation in so far as they do not participate in public-law enterprises.
  - Where data protection is not governed by Land legislation, articles 12 to 17, 19 and 20 shall also apply to public bodies of the Länder in so far as they:
    - execute federal law and do not participate in competition as public-law enterprises or,
    - act as bodies of the judicature and are not dealing with administrative matters.
- **Article 13 on collection of data**, states:
  - Collection of personal data shall be admissible if knowledge of them is needed to perform the duties of the bodies collecting them.
  - Personal data shall be collected from the person. They may be collected without his or her participation only if:
    - A legal provision prescribes or peremptorily presupposes such collection or,
    - The nature of the administrative duty to be performed necessitates collection of the data from other persons or bodies or,

- Collection of the data from the data subject would necessitate disproportionate effort and there are no indications that overriding legitimate interests of the data subject are impaired.

- If personal data are collected from the data subject with his or her knowledge, he or she shall be informed of the purpose of collection. If information is collected from the data subject pursuant to a legal provision that makes the supply of particulars obligatory or if such supply is the prerequisite for the granting of legal benefits, the person shall be informed that such supply is obligatory or voluntary, as the case may be. At his or her request he or she shall be informed of the legal provision and of the consequences of withholding details.

- Where personal data are collected from a private body and not from a person, such body shall be informed of the legal provision requiring the supply of details or that such supply is voluntary, as the case may be.

- **Article 14 on storage, modification and use of data**, states:

  - The storage, modification or use of personal data shall be admissible where it is necessary for the performance of the duties of the controller of the data and if it serves the purposes for which the data were collected. If there has been no preceding collection, the data may be modified or used only for the purposes for which they were stored.

  - Storage, modification or use for other purposes shall be admissible only in the following cases:

    - A legal provision prescribes or peremptorily presupposes this.

    - The person has consented.

    - It is evident that this is in the interest of the data subject and there is no reason to assume that he or she would withhold consent if he or she knew of such other purpose.

    - Details supplied by the person have to be checked because there are actual indications that they are incorrect.

    - Data can be taken from generally accessible sources or the controller of the data file would be entitled to publish them, unless the data subject clearly has an overriding legitimate interest in excluding the change of purpose.

    - It is necessary for immediate threat to public safety.

    - It is necessary to prosecute criminal or administrative offences, to implement sentences or measures as defined by the Penal Code or to execute decisions imposing administrative fines.

    - It is necessary to avoid a grave infringement of another person's rights.

    - It is necessary for the conduct of scientific research when scientific interest in conducting the research project substantially outweighs the interest of the

person in excluding the change of purpose, and the research purpose cannot be achieved by other means or can be achieved only with disproportionate effort.

- Processing or use for other purposes shall not be deemed to occur if this serves the exercise of powers of supervision or control, the execution of auditing or the conduct of organizational studies for the controller of the data file. This shall also apply to processing or use for training and examination purposes by the controller of the data file, unless the data subject has overriding legitimate interests.
- Personal data stored exclusively for the purpose of monitoring data protection, safeguarding data or ensuring proper operation of a data processing system may be used exclusively for such purposes.

- **Article 15 on communication of data to public bodies**, states:
  - Communication of personal data to public bodies shall be admissible if:
    - It is necessary for the performance of duties of the communicating body or the recipient and
    - If the requirements of article 14 are met.
  - Responsibility for the admissibility of communication shall rest with the communicating body. If the data are communicated at the request of the recipient, the latter shall bear the responsibility. In such case the communicating body shall merely examine whether the request for communication lies within the responsibility of the recipient, unless there is special reason to examine the admissibility of communication.
  - The recipient may process or use the communicated data for the purpose for which they were communicated. Processing or use for other purposes shall be admissible only if the requirements of article 14 are met.
  - The previous provisions shall apply mutatis mutandis to the communication of personal data to bodies of religious organisations, provided it is ensured that the recipient takes adequate data protection measures.
  - Where personal data that may be communicated is linked to other personal data or a third party records in such a way that separation is not possible or is possible only with unreasonable effort, communication of the latter data shall also be admissible, unless the person or a third party clearly has an overriding justified interest in keeping them secret; use of these data shall be inadmissible.
  - The above provisions shall apply mutatis mutandis if personal data are transmitted within a public body.
- **Article 16 on communication of data to private bodies**, states:
  - Communication of personal data to private bodies shall be admissible if:
    - It is necessary for the performance of the duties of the communicating body and the requirements of article 14 are met or;

- The recipient credibly proves a justified interest in knowledge of the data to be communicated and the person does not have a legitimate interest in excluding their communication.

- Responsibility for the admissibility of communication shall rest with the communicating body.
- The communicating body shall inform the person of the communication of his data. This shall not apply if it can be assumed that he or she will acquire knowledge of such communication in another manner or if such information would jeopardize public safety or otherwise be detrimental to the Federation or a to Land.
- The recipient may process or use the communicated data only for the purpose for which they were communicated to him or her. The communicating body shall point this out to the recipient. Processing or use for other purposes shall be admissible if communication above would be admissible and the communicating body has consented.

- **Article 17 on communication of data to bodies outside the area of application of the BDSG**, states:
  - Article 16 in conjunction with the relevant laws and agreements as well as article 16 shall apply to the communication of personal data to bodies outside the area of application BDSG and to supranational or international bodies.
  - Communication shall not occur where there is reason to assume that this would be incompatible with the purpose of a German law.
  - Responsibility for the admissibility of communication shall rest with the communicating body.
  - It shall be pointed out to the recipient that the communicated data may be processed or used only for the purpose for which they were communicated to him.

The second chapter of the BDSG focuses on personal rights, in particular the following articles apply:

- **Article 19 on provision of information to the person**, states:
  - The person shall, at his or her request, be provided with information on:
    - Stored data concerning him or her, including any reference in them to their origin or recipient, and
    - The purpose of storage.
  - The request should specify the type of personal data on which information is to be provided. If the personal data are stored in records, information shall be provided only in so far as the data subject supplies details making it possible to locate the data and the effort needed to provide the information is not out of proportion to the interest in such information expressed by the person. The controller of the data file shall exercise due discretion in determining the procedure for providing such information and, in particular, the form in which it is provided.

- The paragraph above shall not apply to personal data which are stored merely because they may not be erased due to legal, statutory or contractual provisions on their preservation or exclusively serve purposes of data security or data protection control.
- If the provision of information relates to the communication of personal data to authorities for the protection of the constitution, to the Federal Intelligence Service, the Federal Armed Forces Counterintelligence Office and, where the security of the Federation is concerned, other authorities of the Federal Ministry of Defence, it shall be admissible only with the consent of such bodies.
- Information shall not be provided if:
    - This would be prejudicial to the proper performance of the duties of the controller of the data file,
    - This would impair public safety or order or otherwise be detrimental to the Federation or a Land or,
    - The data or the fact that they are being stored must be kept secret in accordance with a legal provision or by virtue of their nature, in particular on account of an overriding justified interest of a third party, and for this reason the interest of the data subject in the provision of information must be subordinated.
- If no information is provided to the person, it shall at his or her request be supplied to the Federal Commissioner for Data Protection, unless the relevant supreme federal authority determines in a particular case that this would jeopardize the security of the Federation or a Land. The communication from the Federal Commissioner to the person must not allow any conclusions to be drawn in terms of information at the disposal of the controller of the data file, unless the latter consents to more extensive information being provided.
- Information shall be provided free of charge.

- **Article 20 on correction, erasure and blocking of data**, states:
    - Incorrect personal data shall be corrected. If it is discovered that personal data in records are incorrect or if the person disputes that they are correct, a note to this effect shall be made in the record or it shall be recorded by some other means.
    - Personal data in data files shall be erased if:
        - Their storage is inadmissible or
        - Knowledge of them is no longer required by the controller of the data file for the performance of his or her duties.
    - Instead of erasure, personal data shall be blocked in so far as:
        - Preservation periods prescribed by law, statutes or contracts rule out any erasure,

    - There is reason to assume that erasure would impair legitimate interests of the data subject or,
    - Erasure is not possible or is only possible with disproportionate effort due to the specific type of storage.
- Personal data in data files shall also be blocked if the data subject disputes that they are correct and it cannot be ascertained whether they are correct or incorrect.
- Personal data in records shall be blocked if the authority determines the particular case that, without blocking, legitimate interests of the person would be impaired and the data are no longer required for the performance of the authority's duties.
- Blocked data may be communicated or used without the consent of the data subject only if:
    - This is indispensable for scientific purposes, for use as evidence or for other reasons in the overriding interests of the controller of the data file or a third party and
    - Communication or use of the data for this purpose would be admissible if they were not blocked.
- If necessary to protect legitimate interests of the person, the correction of incorrect data, the blocking of disputed data and the erasure or blocking of data due to inadmissible storage shall be notified to the bodies to which these data are transmitted for storage within the framework of regular data communication.

Lastly, the last part of the BDSG addresses special provisions, with the following article.

- **Article 40 on processing and use of personal data by research institutes**, states:
    - Personal data collected or stored for scientific research purposes may be processed or used only for such purposes.
    - Communication of personal data to other than public bodies for scientific research purposes shall be admissible only if these undertake not to process or use the communicated data for other purposes and to comply with the provisions of the following paragraph.
    - Personal data shall be anonymised as soon as the research purpose permits this. Until then, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research purpose.
    - The bodies conducting scientific research may publish personal data only if:
        - The data subject has consented or
        - This is indispensable for the presentation of research findings.

4.2.9 Republic of Malta

All regulations defined in Health Insurance Portability and Accountability Act - HIPAA [41] and Malta Data Protection Act have to be adhered to and the patient need to be informed of any data that might be used or disclosed in any way.

All security rules defined in HIPAA and Malta Data Protection Act have to be adhered to.

With particular regard to localisation and tracking of people, all regulations defined in HIPAA and Malta Data Protection Act have to be adhered to and the person has to be informed of location tracking that might be used or disclosed in any way.

4.2.10 Local organization policies

In addition to international and national regulations a number of local policies apply at some of the pilot sites as stated below. Pilot sites that are not listed below simply have to comply with the national law.

- **Mitera Hospital (Greece).** The hospital complies with **ISO 27001** [24], regarding the Information Security Policy.
- **Elder Nursing Homes in Baia Sprie (Romania)**. The Baia Sprie City Hall is registered as a data processing unit and its regulations and security policy apply for the Elder Nursing Homes as well.
- **Technoport (Luxembourg).** The institution has a generic authorisation from the National Data Protection Commission in Luxembourg to process data for access control purposes. i-locate would target basically the same goals, "beneficiaries" and data than the current system.
- **Municipality of Genova (Italy).** The site has to comply with **City Council resolution 123/05** and integrated with the **City Council resolution 46/08**, and their annexes regarding identification and disclosing of sensitive and judicial data as well as their treatment. This Regulation, according to the legislative decree 30 June 2003, n. 196, identifies the sensitive and judicial data types and the operations executed by the municipality in carrying out his official duties. A general description of the Municipality of Genoa policy regarding the personal data management is available within the Municipality web site [71].

  In particular, the Regulation for the treatment of personal and judicial data, within the meaning of articles 20 (paragraph 2) and 21 (paragraph 2) of the legislative decree no. 196/2003, is available from their website [72]. Specifically, according to the provisions of the article 20 (paragraph 2) and the article 21 (paragraph 2) of the legislative decree 196/2003, forty-two tables (refer to [73]) identify the types of sensitive and judicial data for which their treatment is allowed, as well as what action can be carried on in relation to the specific purpose of overriding public interest sought in the individual cases and expressly listed in the DL.196/2003 (art.s.59, 60, 62-73, 86, 95, 98, and112).
- **Rovereto Hospital (Italy).** Relevantly for this pilot site, a **decree of the President of the Autonomous Province of Trento no. 27-129 on management of sensitive and judicial data** [74], identifies, data types and operations executable by the structures of the Autonomous Province of Trento, institutions and provincial agencies and other entities for

which the Autonomous Province exerts powers of address and control, according to the art. 33 of provincial law 16 June 2006, no.3 (rules governing of Trentino).

These include the local public health agency (i.e. Azienda Provinciale per i Servizi Sanitari or APSS which is partner of i-locate) in the performance of their official duties, with regard to the processing of sensitive and judicial data carried out for the achievement of the relevant objectives of public interest identified by express provision of law, when data types and executable operations are not legislatively specified.

The aforementioned decree of the President of the Autonomous Province of Trento follows the provisions of art. 20 and 21 of the national Legislative Decree 30 June 2003, no. 196 (relating to the protection of personal data).

A further resolution that must be accounted for is the **Resolution no. 1177 05/18/00 of the General Manager of APSS** on the establishment of the working group on privacy and security of data processing with the following main responsibilities:

- Definition of the security of the organisation.
- Definition of an implementation plan.
- Definition of the training plan.
- Preparation of draft training action for Managers.
- Preparation of draft training action for experts and for system administrators.
- Definition of a control plan.
- Update of the security plan.
- Coordination activities.

With regard to the **localization and tracking of people**, Rovereto Hospital follows the **Resolution no. 584/2010 of the General Manager of APSS**, an update of the document containing business directives concerning video surveillance adopted with the **General Manager Resolution no. 1427 of 15 December 2004**.

- **Saint James Hospital** is working towards Joint Commission International (JCI) certification thus all rules need to be adhered to.

4.3 Informed consent

4.3.1 Europe

Consent is the main instrument through which the principle of self-determination is expressed (**Directive 95/46/EC**) [7]. Consent must be considered a prerequisite and an essential provision to any treatment of data, even more when the processing modalities through which it is carried on result in the creation of risks and potential problems to the security and integrity of the data itself. Although consent is regulated in partially different ways across the various legal framework, however, its need is consistently acknowledged in all the countries.

From a technical point of view, consent to the processing of health data must generally be made in writing (**Directive 95/46/EC art .2**). This formality, even if it is easily manageable through traditional paper-based interactions at the time of the first contact between the patient and the health care body that provides the health service, may, however, be a critical point to solve if not properly managed also from a digital point of view.

Most relevantly, the Article 29 Working Party, which was established under the **Directive 95/46/EC** of the European Parliament and of the Council of 24 October 1995 for the protection of individuals with regard to the processing of personal data, published an "Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011" [39] that has to be taken into account in the wording of any security, privacy & contractual disclaimer.

4.3.2 Italy

Processing of personal data shall only be allowed if the person gives his or her express consent, according to **article 23**, par. 1, of the Italian Data Protection Code (IDPC) [9]. Consent has to be given “freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Article 13” (art. 23, IDPC).

The consent shall always be accompanied by the specific Information Notice, reporting all the information required by **article 13**, that is: the terms of service, the voluntary nature, the right to data access set by art. 7 of IDPC, the processing operations carried out for scientific purposes.

Regarding the processing of sensitive data, **article 26**, par. 1 establishes a particular discipline, stating that “sensitive data may only be processed with the data subject’s written consent and with the Data Protection Authority’s prior authorization, by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations”.

Within the health sector, **article 76**, par. 1, of IDPC provides a specific regulation that states that “health professionals and public health care bodies may process personal data disclosing health, also within the framework of activities in the substantial public interest pursuant to **Article 85**,

> a) With the data subject’s consent, also without being authorized by the “Garante” (the supervising authority), if the processing concerns data and operations that are indispensable to safeguard the data subject’s bodily integrity and health;
>
> b) Without the data subject’s consent, based on the Garante’s prior authorization, if the purposes referred to under a) concern either a third party or the community as a whole”.

Article 81 mentions two possibilities to express consent:

- The consent to process one's sensitive data (disclosing health) can be expressed in a unique declaration which can be oral or written;
- In the case of an oral declaration, the healthcare professional or public health care authority takes note of the consent expressed and of the delivery to the interested person of the General Privacy Informative Note.

Article 82, however, states that the Information Notice and the consent on the processing of one's personal data can take place after the delivery of the healthcare treatment, without delay, in the following cases:

- Emergencies or cases involving public hygiene;
- In cases of physical impediment, lack of legal capacity, or unable to distinguish right and wrong, when the consent cannot be obtained from the entity legally representing the data subject, or else a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted;
- In case of impending and irretrievable danger for the data subject's health or bodily integrity;
- In cases when the delivery of the necessary medical treatment were to suffer in terms of its timeliness or effectiveness - by the need to obtain the data subject's prior consent.

4.3.3 Croatia

The main ethical issues derive from threats to person's privacy. Therefore user of mobile applications should be able to read and choose whether he/she is willing to accept the terms of use of the application and comply with sharing a specified set of private information and the location itself.

4.3.4 Greece

Patients should not be treated primarily as consumers and health data should be strictly protected against unlawful processing [25]. In Greece so far mainly the ePrescription system has been developed, while significant steps have not taken place yet as regards the Electronic Health Records (HER) [26]. For the operation of the ePrescription system, special permission by the Greek Data Protection Authority has been given [27]. The protection of health data takes place in the light of legislation on medical secrecy and in the light of legislation on the protection of personal data [28].

Thus, all health data are protected by **Article 14 of the Code of Medical Ethics (law 3418/2005)**, which states, under the title "observance of medical records", the requirements for electronic record keeping by doctors, clinics and hospitals. Article 371 of the Greek Penal Code states that professional secrecy is also applied to health data.

Moreover, the provisions of the **law 2472/1997** for the data protection are applied, including Articles 7 and 7A of which contain provisions similar to those in Directive 95/46/EU.

As regards the protection of personal data in the ePrescription system, in particular, there are adequate provisions in the **law 3892/2010**, under which access to health data kept in the central electronic prescription system is regulated:

- The insured have access to and knowledge of their data, which are registered in the system (**Article 6** par. 6).
- Physicians have access to data that has been registered by them or by other doctors, provided that the express and specific consent of the patient has been given (**Article 3** par. 8).
- Pharmacists have access to prescriptions performed by themselves (**Article 4** par.9).
- Social insurers have access to data only for specific reasons and with the requirement of a specific consent (**Article 7** par.1).
- Health service units have access to health referrals which were performed by themselves (**Article 5** par.8).

Other legal constraint that is imposed by the legal framework regards the Protection of Privacy of patient as described in **article 47** in the **law 2071/1992** [29] regarding requirements for security policy of HealthCare Organizations and the time framework for health records maintenance for Hospital as from the law **1258/1981**.

4.3.5 Luxembourg

The main ethical issues related to tracking, monitoring and localisation in Luxembourg are mostly related to imposed control and supervision. Employee tracking is therefore highly restricted by law. Biometric identification is considered an issue too. Mere access and space occupation control is in contrast considered acceptable if the data subject has given its consent, the data collected is used for such purposes only, and is not communicated to any third party. Data gathered can include the following: identity, company, zones being used, badge number, movements (in/out hours, doors/zones).

4.3.6 Romania

According to **law No.677/2001** [19], all physical persons must be informed if personal data is collected. Statistical and anonymous data is not subject to laws and regulations.

When collecting personal data, users must be informed about their rights and must provide a written consent for data usage. Afterwards, users can intervene on their data or request the interruption of processing, although that request has no backwards effect.

The **Civil Code of July 17th, 2009 [30], republished by the Law 287/2009**, published in Official Gazette no. 505 of July 15th, 2011, includes **Article 71** on the right to privacy, which states that:

- Every person has the right to have respect for his private life.
- No one shall be subjected to any interference in private life, personal, family life or in inhabitation, residence or his correspondence, without his consent.

- It is also forbidden to use in any manner correspondence, manuscripts or other personal documents as well as private information, without explicit consent.

4.3.7 The Netherlands

Concerning “storing of information” or “accessing information already stored”, **Article 11.7a** of the **Dutch Telecommunications Act** implements **Article 5.3** of the e-Privacy Directive (**Directive 2002/58/EC**, amended by **Directive 2009/136/EU**). As this article is specifically relevant for legal restrictions regarding the use of cookies it is the sometimes called the cookie clause [38] (for ease of reading, the word “cookies” is used below), however the scope of the provision is broader and it applies to any “storing of information” or “accessing information already stored” in the terminal equipment of a user.

Article 11.7a only allows storing and reading of cookies after obtaining the informed consent of the user. Consent cannot be inferred from browser settings, unlike what appears to be the case in some other member states. Furthermore, the Dutch legislator added a legal presumption about tracking cookies and similar technologies. Such use of cookies is presumed to entail the processing of personal data. The general rule of Article 11.7a is as follows. Anyone, whether based in the Netherlands or not, that stores a cookie on a user’s device must obtain the prior informed consent of the user. The user must be provided with clear and complete information.

Consent is defined as any freely given, specific, and informed expression of will. During the Dutch legislative history it was noted that consent for cookies cannot be inferred from browser settings, because current browsers are not suitable for expressing consent. For instance, most browsers accept all cookies by default. A party that obtained consent to store a cookie on a user’s device does not have to ask consent again when accessing the cookie. According to the Dutch National Regulatory Authority (OPTA), consent can be obtained through a pop-up window.

Two categories of functional cookies are exempted from the consent requirement. First, no consent is needed for cookies having the sole purpose of carrying out communication over an electronic communications network. Second, no consent is needed for a cookie that is strictly necessary for providing a service that the user requested. An example is a cookie for a digital shopping cart.

The Dutch provision adds a legal presumption about tracking cookies and similar technologies for behavioural targeting, the tracking of people’s online behaviour for targeted advertising. Such use of cookies is presumed to entail the processing of personal data. In most cases this means that the prior “unambiguous” consent of the user is required. In principle, a party using tracking cookies could prove it does not process personal data. This legal presumption enters into effect on 1 January 2013. The rest of the provision entered into effect on 5 June 2012.

4.3.8 Germany

Article 34 of **Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)** states that:

- The data subject may request information on:
  - Stored data concerning him or her, including any reference in them to their origin and recipient.
  - The purpose of storage and

  - Persons and bodies to whom his or her data are regularly communicated if his or her data are processed automatically.

- If the personal data are stored in the normal course of business for the purpose of communication, the data subject may request information on their origin and recipient only if he or she has well-founded doubts about the correctness of the data. In such case, information on the origin and recipient shall be provided even if these particulars are not stored.
- In the case of bodies that store personal data in the normal course of business for the purpose of supplying information, the data subject may request information on his or her personal data even if they are not stored in a data file. The data subject may request information on their origin and recipient only if he or she proves that he has well-founded doubts about the correctness of the data.
- Information shall be provided in writing unless special circumstances warrant any other form.
- Information shall be provided free of charge. However, if the personal data are stored in the normal course of business for the purpose of communication, a fee may be charged if the data subject can use the information vis-à-vis third parties for commercial purposes. The fee shall not exceed the costs directly attributable to the provision of information. No fee may be charged in cases where special circumstances give rise to the assumption that stored personal data are incorrect or that their storage was inadmissible, or where the information has revealed that the personal data have to be corrected or have to be erased.
- Where information is not provided free of charge, the data subject shall be given the possibility to acquire personal knowledge of the data and particulars concerning him or her within the framework of his entitlement to information. This shall be pointed out to him or her in a suitable manner.

4.3.9 Republic of Malta

Patients have to provide and be informed of any patient data being exchanged (e.g. appointment details). Data Protection rules [42] as within **Malta Data Protection Act – Chapter 440** have to be applied.

4.3.10 Local organization policies

In addition to international and national policies, some of the pilots have in place local policies as detailed below (pilot sites not listed below simply have to comply to general national legislation):

- **Technoport (Luxembourg)** already has an access control policy in place, which is not considered an issue by the entrepreneurs. Participation to i-locate would be on a voluntary basis. People will be able not to register to the system or not use it on a continuous basis. That would however hamper the impact of the pilot.
- **Alba Iulia Emergency Hospital (Romania).** The two relevant local policies are:
  - The **Internal Regulation of Organization and Functioning of Alba County Emergency Hospital (ROF) no 11882 / 2012** [31].

  - The **Internal Code of Conduct of Alba County Emergency Hospital no 13981/2013** [32].

- **Municipality of Brasov (Romania).** The following internal rules apply:
  - **Internal Regulation of Organization and Functioning of the Municipality of Brasov (2012)** [33].
  - The **Internal Code of Conduct of the Municipality of Brasov** [34].
  - The **Municipality of Brasov Employees' Code of Conduct** [35].
- **Brukenthal National Museum (Romania).** The only applicable rule is the **Internal Regulation of Organization and Functioning of the Brukenthal National Museum** [36] (2011).
- **Municipality of Genova (Italy).** According to the council regulations as in [73] with respect to the informed consent constraint, two approaches will be adopted:
  - Council officials: an official will enable implicitly the "traceability" of the presence service with the acceptance of fire risk and / or first aid responsible role,
  - Differently abled employees, citizens and professionals: an authorization will be released by a service user when he requires it.
- **Rovereto Hospital (Itlay)** follows the procedure of the Province of Trento for the integrated management of the information and consent to the processing of data concerning health by the Azienda Provinciale per i Servizi Sanitari and of General Practitioners/Pediatricians.

4.4 Public space accessibility and preservation of patrimony

Due to the fact that i-locate can provide access to mapping data, the following analysis lists the legal constraints that are in place at the different countries of the pilots with regard to accessibility of data regarding public spaces.

4.4.1 Europe

In order to facilitate the re-use of information held by public sector bodies of the Member States, the European Union adopted the **Directive 2003/98/EC** [47] that has delegated to each administration the possibility of authorizing the re-use of information collected, produced and disseminated to pursue their duties.

According to the **article 17**, par. 7, of the **Directive 2007/2/EC** [48] establishing an Infrastructure for Spatial information in the European Community (INSPIRE), “by way of derogation from this Article, Member States may limit sharing when this would compromise the course of justice, public security, national defence or international relations”.

4.4.2 Italy

According to the **Legislative Decree 82/2005**, the important principle of availability of public data (**article 2**, par. 1 and art. 50, par. 1) was introduced [49]. It consists in the possibility, for public and private entities, to access data without restrictions not related to explicit laws.

The Italian legal system transposed the Directive 2003/98/EC through the **Legislative Decree 36/2006** [50]. According to this decree, public data must not be provided public access if this can determine violation of:

- Public security, national defence, execution of criminal or disciplinary investigations,
- The right of the third parties to industrial, statistical and trade secret, or other secrecy constraints established according to the laws,
- Intellectual property rights,
- Right to protection of personal data,

Finally, according to the **Law no. 221 of 17 December 2012** (art. 9) [51], public administrations have to:

- Regulate electronic access and re-use of data and documents of which they are owners or of which they have availability;
- Annually publish their accessibility objectives, for the current year.

4.4.3 Luxembourg

According to the **Law of 28 July 2010 incorporating the European INSPIRE directive**, public authorities or the CC-ILDG (coordination committee for geographical data) can restrict access to geographical data or sharing of geographical data when such an access would be a threat for public safety.

4.4.4 Romania

In Romania, the legal regime of national cultural treasures, regardless of their owner is currently regulated by **Law no. 182 of October 25, 2000 on the protection of national mobile cultural treasures** [52] and by some provisions of the Government Ordinance no. 27/1992, on measures for the protection of the national cultural heritage and the Government Ordinance no. 68/1994 on the protection of the national cultural heritage, and **Law no. 422/2001 on the protection of historical monuments [53]**.

By regulating specific protective actions, these normative acts have in mind: the evidence, examination, classification, research, storage, preservation, restoration and enhancement of such treasures for the democratic access to culture and in order to transmit these values to future generations.

The state guarantees the property and ensures, according to the law, the protection of the goods that are included in the national cultural patrimony. The state also provides the material and financial resources to detect, record, expertise, classify research, store, preserve, restore, protect and enhance the value of such assets.

Law no. 311 of July 8th 2003, for museums and public collections [54] regulates the general legal status, classification and principles of organization and functioning of museums and public collections, as well as private collections accessible to the public.

The owners and holders of other real rights upon museums and public collections, have, according to the Civil Code and this law, the following obligations:

- To ensure the integrity, security, conservation and restoration of assets classifies in the national movable cultural heritage which are subject to the museum heritage.
- To carry out and, where appropriate, classify assets which are subject to the museum heritage.
- To emphasize the museum heritage.
- To ensure and guarantee the access of the public and of specialists to assets constituting the museum heritage.
- To provide research or, where appropriate, making available for research, of assets belonging to the museum heritage.
- To prevent the use of museum heritage for purposes other than those stipulated by the regulations in force.
- To ensure the guarding of the museum or its public collections and provide them with effective protection systems.

4.4.5 Local organization policies

- **Alba Iulia Emergency Hospital (Romania).**
    - Internal Regulation of Organization and Functioning of Alba County Emergency Hospital (ROF) no 11882 / 2012 [31].

  - The Internal Code of Conduct of Alba County Emergency Hospital no 13981/2013 [32].

- **Municipality of Brasov (Romania).**
  - Internal Regulation of Organization and Functioning of the Municipality of Brasov (2012) [33].
  - The Internal Code of Conduct of the Municipality of Brasov [34].
  - The Municipality of Brasov Employees' Code of Conduct [35].
- **Brukenthal National Museum (Romania).** The Internal Regulation of Organization and Functioning of the Brukenthal National Museum (2011) [36].
- **Mitera Hospital (Greece).** Mitera is a private hospital which means that it has a security officer and security staff who are responsible for controlling access to a hospital and protecting the safety and well-being of its patients and staff.
- **Municipality of Genova (Italy).** Currently, a new emergency management procedure regarding "Matitone" building is being defined.

5 Other regulations and policies of interest

5.1 Alba Iulia Emergency Hospital (Romania)

Internal Regulation of Organization and Functioning of Alba County Emergency Hospital (ROF) no 11882 / 2012 [31] defines the hospital's structure and responsibilities, the management, the activity of the Emergency Care Unit, the activities related to hospitalization / release of the patients, the organizations of the activities inside the hospital's articles, the hospital's procedures, the hospital's circuits, the patients' rights and duties.

The **functional circuits** of the hospital represent the direction of movement for persons, material, supplies, laundry and instruments inside the hospital. The hospital has several circuits organized to ensure a continuous flow of activity and to avoid crossing different septic and aseptic circuits. **Chapter XXIV** presents in detail the hospital's circuits: the sick peoples' circuit, the biological samples' circuit, the employees' circuit, the visitors' circuit, the medical materials' circuit, the medicines' circuit, the food circuit, the laundry circuit, the wastes' circuit. These are also mentioned in a short summary inside the Internal Code of Conduct.

It is worth mentioning the **Internal Code of Conduct of Alba County Emergency Hospital no 13981/2013 [32].** In particular, Chapter II on the Rights and obligations of employees, states that they are required to respect the confidentiality of all medical data related to the patients of the hospital. Employees must supervise the equipment used for the medical activities and to avoid its intentional deterioration. Employees should not access the workplaces that are restricted to some specific use. Employees should behave ethically towards the patients and must keep the professional secret. Visitors are prohibited to visit the following sections: Intensive Care Unit, Surgery Section, and Neonatology.

In addition the following provisions from the **internal Regulation of Organization and Functioning of Alba County Emergency Hospital (ROF) no 11882 / 2012 [31]** apply:

- Hospital employees are allowed to access the unit only through the staff entrances, respecting the functional circuits of the hospital.
- The visitors are allowed to access the unit only during the visiting hours, as shown at the entrance of the hospital.
- The access of external personnel in hospital's risk areas it is forbidden. The public access prohibited areas are: dangerous waste collection point, hitting station, the kitchen, and laundry.
- The healthcare personnel takes all the measure needed on respecting the access indications in the risk areas, the access rules and circulation within the hospital and the rules of civilized behaviour.
- In case of any irregularities, the healthcare personnel has to notify emergency security service.
- During the quarantine periods the visitor access is prohibited or limited, as the case.
- The access for business purposes is based on the ID card or access card.

- The access of mass-media representatives is based on the accreditation cards and identity documents and also by the manager's approval.
- The access in the parking lot is allowed only for authorized vehicles and possessing access cards.

5.2 Brukenthal National Museum (Romania)

The Internal Regulation of Organization and Functioning of the Brukenthal National Museum [36] (2011) defines the activities and patrimony of the museum, the rules of organization and functioning, describes its functional structure, and the rules of conduct.

The web-site [55] presents the schedule of visiting the museum for the public, the permanent and temporary exhibitions, and other general information of interest for potential visitors.

5.3 Municipality of Brasov (Romania)

Internal Regulation of Organization and Functioning of the Municipality of Brasov (2012) [33] defines the management, the activities and responsibilities of each department inside the organization, including the competencies of the entities responsible for providing public services to citizens, the relationships between the structures inside the municipality, the circuit of the documents and the quality management system.

The Internal Code of Conduct [34] defines the rights and duties of the employees, the access of the employees inside the institutions, the working time, rules regarding the work safety.

The Employees' Code of Conduct [35] defines the rules concerning the ethical behaviour and the general principles regarding the way the employees should act when performing their duties (confidentiality, integrity).

The institution web-site [56] includes the schedule of the different departments regarding the program with the public (citizens, business entities).

5.4 Municipality of Genova (Italy)

The "Matitone" building has an emergency management procedure in place. From the emergency management point of view, it is useful outline that "Matitone building" is a 24-floor tall building, with two accesses (East and West side) provided with front-desk. In addition to the Municipality of Genoa, within "Matitone" some private companies have their headquarters (mainly floors 7, 8 and 20-23).

The following lifts are available: six lifts for floors 0-10, five lifts for floors 11-24, one lift for exclusive use of floors 20-23 (used by a private company), one direct lift to the 24th floor. Furthermore, there are four emergency stairs, properly flagged and equipped with cold rooms at each floor. Finally, an alert emergencies system, voice and siren (bell) signal exists.

The new procedure being set in place is being based on the needs identified by the officials and on the distribution of the already qualified personnel. The coordination protocol for the emergency management will be deployed by the Security service staff which is located at the East side front-desk and it ensures 24/7 surveillance. Any emergency will have to be signalled to the front-desk who, being informed of the presence of workers in the building, will deploy them and communicate

to the "emergency coordinator". Each employer will provide daily/weekly list of staff on duty at their organization. Coordination of emergency management activities will also be arranged with private companies inside the building.

5.5 Tremosine (Italy)

Particularly relevant to the pilot will be the technical standards on the construction of technological systems in road tunnels as within the **guidelines for the design of safety measures in road tunnels**.

The first edition of the Guidelines was issued in November 2006 following a double examination of the Higher Council of Public Works and still is the only national technical document that sets forth the procedures for the design of safety for road tunnels in compliance with the Legislative Decree 264/06, which in turn implements the European Directive 2004/54/EC.

The Guidelines make practical application of Legislative Decree 264/06, detailing the minimum requirements and structural plant, describe in detail the model of Risk Analysis defined by law.

The legal reference for the design of safety is the European Directive 2004/54/EC, promulgated by the European Parliament relating to the Minimum Requirements for Safety Galleries Trans-European Road Network. The European Directive 54/2004/EC implemented in Italy by **Legislative Decree n.264/2006**, identifies the security objectives to be pursued, identifies a set of security parameters to be considered, fixed groups of minimum safety requirements to be met, suggests a systemic approach to the formulation and comparative content for the design of tunnel safety of new construction, indicating the risk analysis as the analytical tool used to determine the level of safety of a tunnel, setting the conditions for applying and detailing the objectives to be pursued. The guideline are based basically on analytical risk analysis, but also contain minimum requirements (building, equipment) that replace the analysis of risk.

Lastly, it is worth noting that, in the case of the pilot site of i-locate, the section of road subject to analysis is composed of two short tunnels for the geometric dimensions, amount of traffic, it must not be equipped with technological equipment (lighting, ventilation, etc.).

6 HW/SW constraints

6.1 ETSI certification

Standardization is a key factor for single market and is needed for coexistence of various technologies sharing the same physical medium. Use of wireless technologies in different environment's needs to accord with actual regulation and legislation. ETSI, the European Telecommunications Standards Institute, produces standards for Information and Communications Technologies (ICT) that are used by national governments to enforce regulations. The standard "**EN 301 489-1** (v1.8.1) (**Council Directive 2004/108/EC** on Electromagnetic Compatibility) Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements" needs to be fulfilled to operate with radio equipment.

Manufacturer, that produces or import products inside the European Union have to certify their products and sign it with the CE logo of the "Communautès Europèennes". Therefore, it is needed to fulfil all terms of references. The manufacturer himself asserts conformance based on its compliance assessment.

6.2 Electromagnetic compatibility requirements

Indoor localization in i-locate will make use of radiofrequencies (RF). In particular, three technologies will be used:

- ZigPos-RTLS: based on the IEEE 802.15.4 standard [57].
- HAIP by Quuppa: based on Bluetooth Low Energy, part of the Bluetooth standard since Core Specifications Version 4.0 [58].
- Wi-Fi: based on IEEE 802.11 family of standards (a commercial solution will be chosen by the Consortium in the upcoming months) [59].

The usage of radio spectrum is regulated at the national, European and international level. All the technologies to be used in i-locate for indoor localization purposes operate in the so-called ISM (Industrial, Scientific and Medical) bands.

The ISM bands are portions of the radio spectrum reserved internationally for the use of RF energy for industrial, scientific and medical purposes. Large portions of the ISM bands (and, in particular, those used within i-locate) are unlicensed, i.e., no license is required to operate a device transmitting in such a band. Which implies, conversely, that devices may be operating in a harsh environment characterised by high levels of interference.

The ISM bands are defined by the ITU-R in 5.138, 5.150, and 5.280 of the Radio Regulations [60]. Individual countries' use of the bands designated in these sections may differ due to variations in national radio regulations. The bands in which the i-locate enabling devices will transmit are available for unlicensed use in all countries where i-locate pilots will be deployed.

In the EU, low power wireless devices are generally referred to as short-range devices (SRD). The allocation of frequency bands and their use in the EU are based on recommendations by the Electronic Communications Committee (ECC), which is part of the European Conference of Postal and Telecommunication Administration (CEPT). The ECC document covering SRD is ERC/REC 70-03. The 45 member countries of the CEPT must then adopt these recommendations into law for

them to be binding, so there are occasionally differences between the member countries. No significant difference has been identified for the purposes of the i-locate piloting activities.

ECC recommendation defines 13 different types of SRD applications. The SRD applications relevant for i-locate are n.1, "*Non-specific Short Range Devices*" and n. 3, "*Local Area Networks, RLANs and HIPERLANs*". The ECC recommendation 70-03 defines both the maximum transmit power and limits to the duty cycle and the bandwidth of the transmitter for each allocated frequency band. For example a limit of -10dB on the ERP (Effective Radiated Power) is required when operating in the band 2400MHz-2483.5 MHz, which is one of the bands in which i-locate devices will operate.

Electromagnetic Compatibility (EMC) refers to the ability of a device to operate properly in its intended environment without producing excessive interference to other devices. All electronic devices must meet certain regulations regarding EMC. These regulations cover both intentional (for example, transmission signals) and non-intentional (electrical noise) radiation.

Other potential regulatory issues are induced radiation and RF exposure. Induced radiation refers to how well a device withstands unintentional radiation from an external source (e.g. high voltage line or microwave oven). RF exposure regulations, on the other hand, determine if the device emits radiation that is harmful to human beings. This is normally only a concern for high-power transmission devices, but there have been some concerns (yet to be proven) that long-term exposure to even low-levels of electromagnetic radiation could potentially result in cancer and other health problems. For devices that may be positioned within 20 cm of a human body, SAR (Specific Absorption Rate) testing is required to ensure radiation levels are below a certain limit. In Europe, compliance in terms of RF exposure for the kind of devices used within i-locate is standardized as CENELEC EN 62479:2010, which has been made part of 2006/95/EC directive.

The procedure required to bring wireless equipment to the EU market is outlined in the Directive 199/5/EC of the European Parliament and of the Council (R&TTE - Radio and Telecommunications Terminal Equipment directive). The R&TTE directive is based on self-declaration, that is, the manufacturer who supplies wireless equipment to the market declares that the product satisfies the legal requirements. Basically, the entity that places the equipment on the market is responsible for its compliance.

The CE marking is a mandatory conformity marking for some categories of products sold within the European Economic Area (EEA). It consists of the CE-Logo and, if applicable, the four digit identification number of the notified body involved in the conformity assessment procedure. The CE marking states that the product is assessed before being placed on the market and meets EU safety, health and environmental protection requirements. Devices to be used in i-locate should be required to be CE marked.

6.3 Medical devices (or operation in medical domain)

According to the **Directive 2007/47/EC** [61] amending Council Directive 93/42/EEC [62] "medical device means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:

- Diagnosis, prevention, monitoring, treatment or alleviation of disease,

- Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
- Investigation, replacement or modification of the anatomy or of a physiological process,
- Control of conception,

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means".

According to the same law, "devices shall be divide into Classes I, IIa, IIb and III. Classification shall carried out in accordance with Annex IX".

6.3.1 Certification

The CE marking indicates a product's compliance with EU legislation and so enables the free movement of products within the European market. It is mandatory according to the Directive 2007/47/EC amending Council Directive 93/42/EEC.

According to this Directive, the EC type-examination is "the procedure whereby a notified body ascertains and certifies that a representative sample of production covered fulfils the relevant provisions of the Directive".

"Member States shall presume compliance with the essential requirements referred to Article 3 in respect of devices which are in conformity with the relevant national standards adopted pursuant to the harmonized standards the references of which have been publishes in Official Journal of the European Communities; Member States shall publish the references of such publish the references of such national standards".

7 Usability and inclusiveness

7.1 Web accessibility initiative (WAI)

The Web Accessibility Initiative (WAI) [63] is an effort to improve the accessibility of the World Wide Web for people with disabilities and it is part of the W3C consortium.

People with disabilities (visual, auditory, physical, speech, cognitive, and neurological) may encounter difficulties when using computers generally, but also on the Web. Since people with disabilities often require non-standard devices and browsers, making websites more accessible also benefits a wide range of user agents and devices, including mobile devices, which have limited resources. WAI develops a series of accessibility standards and guidelines.

The Web is an increasingly important resource in many aspects of life: education, employment, government, recreation, and more. It is essential that the Web be accessible in order to provide equal access and equal opportunity to people with disabilities. An accessible Web can also help people with disabilities more actively participate in society.

Much of the focus on Web accessibility has been on the responsibilities of Web developers. Software needs to help developers produce and evaluate accessible Web sites, and be usable by people with disabilities.

WAI is composed by a series of different accessibility standards and guidelines (WCAG, UAAG, ATAG, WAI-ARIA) [64, 65, 66, 67].

7.2 World Wide Consortium (W3C)

The World Wide Web Consortium (W3C) [68, 69] is the main standards organization where member and the public work together to develop standards for the Web. W3C's mission is to lead the Web to its full potential developing protocols and guidelines. To accomplish this work, W3C follows processes that promote the development of high-quality standards based on the consensus of the membership, team, and public. In many cases, the goal of this work is a W3C recommendation, the W3C equivalent of a Web standard.

Here is a general overview of how W3C standardizes a Web technology. People generate interest in a particular topic. W3C is likely to organize a workshop to bring people together to discuss about this topic that interest the W3C community. When there is enough interest in a topic a working group is open. The working group is composed by W3C members, invite experts, and team representatives. Working groups generally create specifications and guidelines that after revision and review are update to a final version. At the end of the process, the advisory committee reviews the mature technical report, and if there is support, W3C publishes it as a recommendation.

7.3 Web Portal

Websites often have text that is difficult to read, controls that are difficult to click, or audio and videos that are difficult to hear. Fortunately your computer can be customized to improve Web browsing experience. Customizations are generally easily reversible and do not delete files. Customization options and accessibility features are usually documented in the "*help*" menu of the software. WCAG (Web Content Accessibility Guidelines) and User Agent Accessibility Guidelines (UAAG) are the most important to follow in the development of i-locate.

WCAG it is developed with a goal of proving a single shared standard for Web content accessibility that meets the needs of individuals, organizations, and governments internationally. Guidelines addresses the information in a Web site, including text, images, forms, sounds etc.

The guidelines are organized around the following four principles:

- Perceivable - Information and user interface components must be presentable to users in ways they can perceive.
- Operable - User interface components and navigation must be operable.
- Understandable - Information and the operation of user interface must be understandable.
- Robust - Content must be robust enough that it can be interpreted reliably by a wide variety of user agents.

The WCAG documents explain how to make Web content more accessible to people with disabilities. Web "content" generally refers to the information in a Web page or Web application, including:

- Natural information such as text, images, and sounds, etc.
- Code or mark-up that defines structure, presentation, etc.

WCAG is primarily intended for:

- Web content developers (page authors, site designers, etc.).
- Web tool developers.
- Web accessibility evaluation tool developers.
- Others who want or need a standard for Web accessibility.

Here is a list of guidelines from the Web Content Accessibility Guidelines 2.0 (WCAG 2.0), part of the W3C recommendation.

- **Text Alternatives**: Provide text alternatives for any non-text content so that it can be changed into forms people need (large print, braille, speech). It is include short equivalents for images (including icons, buttons, and graphics), description of data represented von charts and diagrams and illustrations or brief descriptions of non-text content such as audio and video files.
- **Time-based Media**: Provide alternatives for time-based media. People who cannot hear audio or see video need alternatives. Examples of alternatives for audio and video include text transcripts and captions of audio content, such as recordings of people speaking; audio descriptions, which are narrations to describe important visual details in a video; sign language interpretation of audio content.
- **Adaptable**: Create content that can be presented in different ways (for example simpler layout) without losing information or structure. Headings, lists, tables, and other structures in the content are marked-up properly. This allows content to be correctly read aloud, enlarged, or adapted to meet the needs and preferences of the user. For instance, it can be

presented using custom colours combinations, text size, or other styling to facilitate reading.

- **Distinguishable**: Make it easier for users to see and hear content including separating foreground from background and not used colours as the only way of conveying information or identifying content. In example the visual presentation of text has a contrast ratio of at least 1:7 (this except large text where the ratio is 4.5:1). If any audio on a Web page plays automatically for more than 3 seconds, either a mechanism is available to pause, stop or change the audio volume. Another point is that captions and images of text and text can be resized without assistive technology up to 200% without loss of content or functionality.
- **Keyboard accessible**: All functionality that are available by mouse are also available by keyboard and all functionality available from a keyboard are available without requiring specific timings for individual keystrokes.
- **Enough Time**: Provide users enough time to read and use content and consent the re-authenticate when a session expires without losing data.
- **Seizures**: Do not design content in a way that is known to cause seizures. Content that flashes at certain rates or patterns can cause photo-sensitive reactions, including seizures. Flashing content is ideally avoided entirely, or only used in a way that does not cause known risks.
- **Navigable**: Provide ways to help users navigate, find content, and determine where they are. Information about the user's location within a set of Web pages is available and a mechanism is available to allow the purpose of each link to be identified from link text alone. The keyboard focus is visible and the focus order follows a meaningful sequence.
- **Readable**: Make text content readable and understandable. One example is that the default human language of each Web page can be programmatically determined and use the clearest and simplest language possible, or providing simplified versions. Providing definitions for any unusual words, phrases, idioms, and abbreviations.
- **Predictable**: Make Web pages appear and operate in predictable ways. Many people rely on predictable user interfaces and are disoriented or distracted by inconsistent appearance or behaviour. When any component receives focus, it does not initiate a change of context. Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the sane relative order each time they are repeated, unless a change is initiated by the user.
- **Input Assistance**: Help users avoid and correct mistakes. If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text. It helps people who do not understand the functionality, are disoriented or confused, forget, or make mistakes using forms and interaction for any other reason.
- **Compatible**: Maximize compatibility with current and future user agents (browsers, assistive technologies, and other user agents).

The User Agent Accessibility Guidelines (UAAG) explain how to make user agents accessible to people with disabilities, particularly to increase accessibility to the Web. User agents include Web browsers, media players, and assistive technologies, which are software that some people with

disabilities use in interacting with computers. UAAG is primarily for developers of Web browsers, media players, assistive technologies, and other user agents.

Here is a list with a selection of guidelines from the UAAG 2.0, part of the W3C recommendation.

- **Render Alternative Content**: The user can choose to render any type of recognized alternative content that is present for a content element. This is the case where a person with low vision could finds some image painful (e.g. high contrast).
- **Text Size, Colour and Font** (by Element and/or Globally): The user can set all of the following characteristics of visually rendered text content.
- **Speech Rate, Volume, and Voice**: If synthesized speech is produced, the user can specify the volume, (independently of other sources of audio).
- **Allow Zoom**: The user can rescale content within top-level graphical view (zoom in at least 500% respect the default size and zoom out less the 10% respect the default size)
- **Follow Text Keyboard Conventions**: The user agent follows keyboard conventions for the operating environment.
- **Sequential Navigation Between Elements**: The user can move the keyboard focus backwards and forwards through all recognized enabled elements in the current view.
- **Provide text search**: The user can perform a search within rendered content, including rendered text alternatives and rendered generated content, for any sequence of printing characters from the document character set.
- **Provide structural navigation**: Users can view, navigate, and configure the elements used in navigating hierarchy.
- **Support other input devices**: If the platform supports text input using an input device, the user agent is compatible with this functionality
- **Ensure that the user interface is understandable**: Users can turn off non-essential messages from the author or user-agent.
- **Help users avoid and correct mistakes**: Users can have form submissions require confirmation, go back after navigating, have their text checked for spelling errors, undo text entry, avoid or undo settings changes, and receive indications of progress activity.

7.4 Mobile

"Mobile accessibility" generally refers to making websites and applications more accessible to people with disabilities when they are using mobile phones. The WAI work in this area includes people using a broad range of devices to interact with the Web like phones, tablets, TVs.

There are not separate guidelines for mobile accessibility. Mobile is covered in existing WAI accessibility guidelines (particularly WCAG regarding the part of the information in a Web site and UAAG regarding how to make user agents accessible to people with disabilities).

W3C plan to provide more guidance on applying WCAG in the mobile context and work is in progress.

8 Conclusions

This document collects the relevant European and National laws and regulations, as well as local policies, which constitutes the regulatory frameworks in the context of the problem statements identified by the pilot partners. The regulatory framework taken in consideration addresses ethical issues, security and privacy, hardware characteristics, software and hardware certification related to safety, electromagnetic compatibility and usability.

The framework outlined by the regulations and norms in this document must guide the design and development of both functional and non-functional tools and services.

To summarize the results of this document, a list of requirements for the i-locate platform is provided, grouped according to their relevance in relation to the type of problem statements identified by the pilot partners. These are requirements of the i-locate platform common to all pilots.

Ethics, privacy and security:

1) Need to inform the user of the aims and modalities of treatment of personal data and to collect his/her consent (informed consent) about the processing of personal data and data allowing the localization of people indoor and outdoor.

2) Use of the above data only for the purposes stated in the informed consent, in respect to the data protection laws.

3) In the case of collection, storage and management of sensitive data, in particular data able to disclose the health status of a person (even the location of a person inside a specialist's room can fall into this category), technical solutions compliant to a minimum common set, extracted from the European and national regulations, should be implemented, in particular:

- Computerized authentication;
- Use of an authorization system, that can allow the user to access to specific resource to pinpoint the authorization profile;
- Regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenance of electronic means;
- Protection of electronic means and data against unlawful data processing operations, unauthorized access and specific software;
- Implementation of procedures for safe keeping backup copies and restoring data and system availability (i.e. back-up copies);
- Encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

4) In the presence of local policies for accessing/managing personal and localization data, the solution must be customized in order to comply with the local regulations (see local organization policies subchapters).

Public space accessibility and protection of patrimony

In principle, the European regulation, also when transposed in national laws, states the principle of availability of public data allowing public and private entities to access data without restrictions. This principle applies also to data concerning the maps of public buildings, fundamental for the i-locate project. There are important exception, though, that the project must analyse and deal with:

- when the disclosure of public data can violate public security, national defence, execution of criminal or disciplinary investigations, or secrecy constraints established according to the laws (e.g., sensible targets in city halls or hospitals);
- when the disclosure of public data can put in danger the national cultural and heritage patrimony (e.g. damages of masterpieces in museums).

HW/SW constraints and Usability and Inclusiveness

There are several standards, recommendations and procedures for hardware and software devices (e.g. ETSI) that need to be addressed during the development of i-locate, specifically addressing electromagnetic compatibility (2006/95/EC directive, 199/5/EC), medical devices (Directive 2007/47/EC), usability and inclusiveness (WAI, W3C). The compliance to these essential requirements is a key factor to bring the system into the market.