DAPHNE

Data-as-a-Service Platform for Healthy lifestyle and preveNtive medicinE

SEVENTH FRAMEWORK PROGRAMME

DAPHNE

Data-as-a-service platform for healthy lifestyle and preventive medicine

610440

D2.2 Privacy & Security Legal Issues Report

Lead Author: Ross Little
With contributions from: -
Reviewer: Alberto Olmo (Treelogic)

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Restricted to other programme participants (PP)
Contractual delivery date:	31/01/2014
Actual delivery date:	31/01/2014
Version:	0.4
Total number of pages:	53
Keywords:	Data Protection Directive Privacy Security Regulation Electronic Health Record

Abstract

The present deliverable examines the data protection and privacy regulations pursuant to the European legal framework and national legislations (of trial partners) with respect to health data processed in the DAPHNE DaaS project. The deliverable further provides a high level classification of the data that will be processed in a DAPHNE DaaS service.

Executive summary

This deliverable D2.2 first identifies and analyses all the data protection and privacy rules and regulations inherent to the use of personal health data in the European Union as applicable for the DAPHNE DaaS project. The regulations themselves affirm that DAPHNE wellbeing data is classed as health data from the data protection legal perspective.

Also as the DAPHNE project also includes a non EU medical group partner who will be assisting with the trial, analysis of the national legislation pursuant to Israel law has been included.

In the course of analysing the relevant directives, regulations and commission communications the task highlights the important rules and regulations that are relevant to DAPHNE and which will feed into the DAPHNE requirements.

Included in the scope of the task is a high level classification of DAPHNE data, i.e. raw medical device data uploaded to DAPHNE and analysed by DAPHNE heuristics application to give feed back to the end-user / patient. This patient feedback data is determined, in this initial analysis, to be added to Patient Health Records (PHRs) in DAPHNE whereas professional medical analysis would be included in Electronic Health Records (EHRs). It must be noted however that the actual use of PHRs and EHRs still needs to be clarified in the DAPHNE projects as the data model is still to be defined. Nevertheless the data stored and processed by DAPHNE is then clarified as being able to be used for a Bulk Data research service pursuant to the safeguards in national legislation.

Finally it is important point to note is that the data protection laws in the EU are currently being harmonised under one General Data Protection Regulation. This will simplify the legal landscape in the EU and also bring it up to date in our modern world and take into account globalisation, social networks and cloud computing. It is expected to be passed in the EU Parliament before the May parliament election in 2014 and therefore once passed the project will need to consider whether it needs to be implemented in DAPHNE.

Document Information

IST Project Number	610440	**Acronym**	DAPHNE
Full Title	Data-as-a-service platform for healthy lifestyle and preventive medicine		
Project URL	http://www.DAPHNE-fp7.eu/		
Document URL			
EU Project Officer	Mr. Benoit Abeloos		

Deliverable	**Number**	D2.2	**Title**	Privacy and Security Legal Issues report
Work Package	**Number**	WP2	**Title**	Business models definition and platform design

Date of Delivery	**Contractual**	M04	**Actual**	M04
Status	version 0.4		final □	
Nature	prototype □ report ☑ demonstrator □ other □			
Dissemination level	public ☑ restricted □			

Authors (Partner)	Ross Little (ATOS)			
Responsible Author	**Name**	Ross Little	**E-mail**	Ross.little@atos.net
	Partner	ATOS	**Phone**	+34 626699162

Abstract (for dissemination)	The deliverable D2.2 examines the data protection and privacy regulations pursuant to the European legal framework and national legislations (of trial partners) with respect to health data processed in the DAPHNE DaaS project. The deliverable further provides a high level classification of the data that will be processed in a DAPHNE DaaS service.
Keywords	Data Protection Directive Privacy Security Regulation Electronic Health Record

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
23/01/2014	0.4	Ross Little	Updates from internal review and some extra clarifications and re-wording.

Table of Contents

Executive summary 3
Document Information 4
Table of Contents 5
Abbreviations 6
Definitions 7
1 Introduction 8
1.1.1 About this Document 8
1.1.2 Scope 8
1.1.3 Key 8
2 Legal Foundations 9
2.1 EU Data Protection Framework 9
2.1.1 Data Protection Directive 95/46/EC 9
2.1.2 Article 29 WP131 - Data Protection Working Party Working Document on Processing of Personal Data Relating to Health in EHR 16
2.1.3 Council of Europe, Recommendation No. R (97) 5 on the Protection of Medical Data 25
2.1.4 Patients´ Rights Directive 2011/24/EU cross-border healthcare 29
2.1.5 Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling 31
2.1.6 Directive 2002/58/EC on Privacy and Electronic Communications 32
2.1.7 Recommendation No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes 32
2.1.8 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] 33
2.1.9 Article 29 WP196 - Opinion 05/2012 on Cloud Computing 33
2.2 National Legislations 36
2.2.1 Italy 36
2.2.2 Israel 48
2.3 Communications from the Commission to the European Parliament 49
2.3.1 eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century - COM(2012)736 49
2.4 Future Data Protection Regulation Implications 50
2.4.1 Single Set of Rules 51
2.4.2 Responsibility & Accountability 51
2.4.3 Consent 51
2.4.4 Data breaches 51
2.4.5 Right to be Forgotten 51
2.4.6 Data Portability 51
2.4.7 Pseudonymous data 52
3 Classification of DAPHNE Data 53
3.1 Anonymous Bulk Data for Research Purposes 53
3.2 Private Data for Personal Health Services 53
4 Privacy Level Agreement (PLA) 55
5 Conclusions 57
References 58

Abbreviations

CSA Cloud Security Alliance

CSC Cloud Standards Coordination

CSP Cloud Service Provider

DaaS Data as a Service

DPD Data Protection Directive

DPR Data Protection Regulation

EDPS European Data Protection Supervisor

EEA European Economic Area

EHR Electronic Health Record

EMR Electronic Medical Record

eID Electronic Identity

GDPR General Data Protection Regulation

ICT Information and Communication Technologies

MDR Medical Device Record

PHR Personal Health Record

PET Privacy Enhancing Technology

PLA Privacy Level Agreement

Definitions

All definitions that are used in this document are defined under the different directives and regulations included in the Legal Foundations section 2.

1 Introduction

1.1.1 About this Document

This is deliverable D2.2 of the DAPHNE project. Its overall aim is to identify privacy and security legal issues and classify the type of information involved in offering a DAPHNE DaaS service.

1.1.2 Scope

The scope of this deliverable concerns the data protection and privacy framework in the EU as regards to the processing of health data and further gives an analysis of the respective national legislations pertaining to the DAPHNE medical partners.

It should be noted that the DAPHNE project will make use of medical devices to monitor patients' health and that these are also subject to EU regulations (e.g. Directive 2007/47/EC), however an analysis of the medical device regulations is not within the scope of this deliverable.

It is for the DAPHNE partners that are providing the medical devices to ensure that they conform to the appropriate EU regulations pursuant to the national legislations of the DAPHNE medical partners and that the devices are identified by the CE mark.

1.1.3 Key

To aid the readability and highlight the most important areas when reviewing the different directives and regulations in terms of DAPHNE the following key will be used:

KEY:

Underlined text:	Where text from a directive or regulation is included then the applicable parts of the text in relation to DAPHNE are underlined.
Highlighted text:	Where text is highlighted in grey background then this is summing up regulation or directive applicability to DAPHNE and is important.
Boxed text:	Where text has been boxed this is to explicitly show that this text has been copied from the document under inspection from DAPHNE perspective, where it would be otherwise unclear, and that it is applicable to DAPHNE.

2 Legal Foundations

This section provides an analysis of the legal foundations on EU citizens data protection and privacy in relation to offering an EU based DAPHNE DaaS service in a cloud computing environment. However as the DAPHNE trial will also include a non EU based medical partner from Israel serving Israel citizens, as well as a medical partner from Italy serving Italian citizens, the national legislation of Israel will determine under what conditions it can take part in the DAPHNE DaaS trial. Likewise the national legislation for Italy must be analysed to check for specific implementation of the EU data protection framework.

The legal foundations will feed into task 2.3 to give requirements on the protection of personal health data in the DAPHNE DaaS trial in relation to how it is processed by the projects different stakeholders and actors. As such it is foreseen for example that DAPHNE medical partners will need to be consulted in some detail on their health data processing and medical devices will need to be analysed to be aware of security mechanisms available. Therefore it is strongly recommended that especially DAPHNE medical partners and device partners should become familiar with this deliverable so to be aware of data protection areas that affect them.

2.1 EU Data Protection Framework

2.1.1 Data Protection Directive 95/46/EC

2.1.1.1 Introduction

The **Data Protection Directive** (DPD) 95/46/EC is a European Union (EU) directive which regulates the processing of personal data within the European Union and covers the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The DPD builds upon Article 8 of the European Convention on Human Rights[1] (ECHR) which provides the right to respect for one´s "private and family life, his home and his correspondence ", and of which all EU member states are signatories.

The DPD provides the framework upon which all member states have based their national data protection laws. The directive is not legally binding on EU citizens and is transposed into internal law by the different EU member state´s national legislations. All member state legislations respect the word of the directive, however some member states implement more stringent rules than others, when allowed by the directive, and thus today the EU member states have partly diverging legislations. This is being currently addressed with a new General Data Protection Regulation [7] to create the one set of rules throughout all member states as discussed later in section 2.3.

2.1.1.2 Definitions

To properly understand implications of the directive, it is important to describe the following terms used in the directive:

- **Anonymous data:** Any data that is rendered in such a way that the data subject is no longer identifiable either directly or indirectly[2], in particular by reference to an identification number or by one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
- **Data Subject:** The data subject is an identifiable natural person whose personal data are collected, held or processed.
- **Data controller:** The data controller is the person or administrative entity (e.g. a General Director or a Head of Unit of the European Commission) that determines the purposes and means of the processing of personal data on behalf of an institution or body. In particular, the controller has the duties of ensuring the quality of data and, in the case of the EU institutions and bodies, of notifying the processing operation to the data protection officer (DPO). In addition, the data controller is also

[1] All the member states of the European Union (EU) are also signatories of the ECHR [2].

[2] This is further clarified so that data is considered anonymous if: (1) identification requires an unreasonable amount of time and manpower (2) the data subject is not identifiable through malicious collusion with a 3rd party.

responsible for the security measures protecting the data. The controller is also the person or entity that receives a request from a data subject to exercise his or her rights. The controller must co-operate with the DPO, and may consult him or her for an opinion on any data protection related question.

- **Personal Data:** Any information relating to an identified or identifiable natural person, referred to as "data subject". An identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity".
- **Processor:** A processor is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". The essential element is therefore that the processor only acts "on behalf of the controller" and thus only subject to the controller´s instructions.
- **Processing (of personal data):** Processing of personal data refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."
- **Sensitive data**: Sensitive data include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".

2.1.1.3 DAPHNE DaaS Scenario Considerations

As DAPHNE will handle personal health data which is classified as sensitive data in the DPD, the service must make sure that it follows the directive and implements the specific national legislations, as applicable to its deployment in EU member states[3]. Specifically according to the directive, it is the Data Controller that is responsible for making sure that the Data Protection law is followed and who will be subject to severe penalties in the case of any breaches (see section 2.1.1.4.13). It is therefore an important exercise to identify the data controller(s)[4] in the DAPHNE DaaS service.

However as the detailed use cases for DAPHNE are not yet defined, some different scenarios are given below showing the variation that may occur[5].

Scenario 1: Cloud Service Provider (CSP) offering Health Data DaaS Service (as a Controller)
In this scenario, the user buys market available wellbeing health monitoring equipment in the market place. The equipment as well as being able to use in isolation with a PC program also has the ability to securely connect to smart phone for use with a DAPHNE DaaS service.

If the user selects to register with a DAPHNE CSP it will be offered data upload to the DAPHNE cloud to capture and store all of their information, with the capability to automatically analyse their data performing intelligent heuristics on it so to give useful feedback to the user. Additionally DAPHNE can offer interfaces with 3rd party Personal Health Services that provide wellbeing services or indeed offer its service to public and private medical groups so to add its analysis to Electronic Health Records. In this service it is heavily emphasised that it is user centric and that the user has total control over what institutions or health professionals (or similarly recognised individuals) have access to his records[6].

[3] Further applicable regulations and commission communications pertaining specifically to personal health data are analysed later in the document so to fully determine the EU data protection framework for processing personal health data.
[4] To have a clearer understanding of how to determine data controller(s) and processors please refer to Article 29 WP169 [16].
[5] As the DAPHNE scenarios (including trial scenarios) are yet to be defined by the project this is only included to show the different variations of data processors and controllers that could occur depending on how DAPHNE is realised.
[6] This user centric control obliges the CSP to include in its data protection terms of service that it does not disclose user data to 3rd parties if not first authorised to do so by the user.

In this case the DAPHNE DaaS CSP is the controller having a direct service relationship with data subject and determines the range of 3rd party services that it can integrate to. It may also further use the stored data subject´s data for an anonymous bulk data service pursuant to national legislation. Depending upon the scenario, a PHS could be a joint controller who would have their own direct relationship with the user or could be purely a processor handling the data as specified by the controller or alternatively may only use anonymous or pseudonymised data delivered through DAPHNE and not subject to data protection rules.

Scenario 2: Private Health Provider offering Health Data DaaS Service
In this scenario, the user may be receiving specialist post-operative obesity medical care from their Health Provider. They are provided with specialist monitoring medical devices that are able to connect through their own connection point or through specialist smart phone applications to their clinic´s PHS services.

In this case, the Private Health Provider itself is the private cloud owner and collects and processes the data for its own PHS applications. The situation could be expanded where the PHS outsources to specialist partner services to take care of post-operative care. In this situation if the partner PHS carries out only the process as instructed by the controller it will be deemed as a processor. Otherwise if it were to carry out the post care on its own terms and use the data subjects data for its own purposes it would also qualify as a data controller (and therefore be required to obtain the data subject´s consent and be fully liable for their data protection and privacy).

- In the most limited case of the DAPHNE trial, the clinical partners taking part in the trial could implement this type of scenario where they are the owner of their own private cloud; are responsible for their own patient Data Subjects and implement their own PHS. Therefore in this scenario the medical partners would take on the role of controllers.

- An extension to the above scenario could be that the EU clinical partner extends their DAPHNE service to other clinical partners. In this case the clinical partner OPBG based in Italy could extend its services to Nevet in Israel and so offer an international DAPHNE service based in the EU. Nevet and its patients would then benefit from PHS services offered by OPBG and they would also be subject to EU Data Protection pursuant to Italian law (article 4). However whether this meets the requirements of Israel law and Nevet policy rules is subject to further analysis as cross border data flows involve certain restrictions pursuant to national legislation.[7]

Scenario 3: Cloud Service Provider (CSP) offering Health Data DaaS Service (as a Processor)
In this scenario, the user buys market available wellbeing health monitoring equipment in the market place. The equipment as well as being able to use in isolation with a PC program also has the ability to securely connect to smart phone for use with DAPHNE partnered non clinical Personal Health Services (PHS) offered in the smart phones online store or market place such as Weight Watchers or other healthy lifestyle apps.

In this case, the PHS is the Controller as it has contracted the DAPHNE DaaS Service to collect and process the data and the CSP is limited to process the data as contracted, and will not use personal data for its own purposes. Outside this processing contract, the CSP could make additional service agreements with the PHS Controller to receive anonymous health data so that the CSP is able to use the anonymous data for its own bulk data services[8]. Bulk data services could be offered for example to local and national public authorities so that they are able to better determine any policies in the area of obesity and also dimension health care in this area.

[7] Even though national legislation may permit this service, it is still advisable that the DPAs of each country are consulted on such an international service as this entails international flow of sensitive data from Israel to Italy and back to Israel.
[8] As anonymous data is not regulated by the DPD there is no need for the CSP to consider data protection legislation, however it is still subject to legislation on profiling and statistical processing as per national legislation (see section 2.1.5 & 2.1.7 respectively).

2.1.1.4 DAPHNE Specific Analysis of the Data Protection Directive

An analysis of the key data protection principles in the directive that affect DAPHNE privacy and protection measures is carried out in this section. The most important areas that will have impact on design requirements for DAPHNE have been underlined.

2.1.1.4.1 National law applicable (Article 4)

The DAPHNE controller(s) are required to implement national Data Protection laws in the EU subject to the following conditions:

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
    a. the processing is carried out in the context of the activities of an establishment of the DAPHNE controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
    b. the DAPHNE controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
    c. the DAPHNE controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

2.1.1.4.2 Principle relating to Data Quality (Article 6)

1) Personal data in DAPHNE must be:
    a) processed fairly and lawfully;
    b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
    c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
    d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
    e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2) It shall be for the DAPHNE controller to ensure that paragraph 1 is complied with.

2.1.1.4.3 Legitimate Data Processing of Personal Data (Article 7)

Personal data may be processed in DAPHNE only if:
a) the data subject has unambiguously given his consent; or
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
d) processing is necessary in order to protect the vital interests of the data subject; or

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

2.1.1.4.4 The processing of special categories of data (Article 8)

1. By default the processing of personal sensitive data (including health data) shall be prohibited in DAPHNE unless specific measures are applied as described below.
2. Health data may be processed by DAPHNE if any of the following apply:
   a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition may not be lifted by the data subject's giving his consent; or
   b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
   c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
   d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
   e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Additionally health data may be processed by DAPHNE where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.
6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.
7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Considering DAPHNE non clinical PHS then from the view point of this article in paragraph 2.a it is wholly needed the data subject’s explicit consent, unless the member state law prohibits the processing of health data by consent alone.

For clinical PHS it is seen in paragraph 3 that processing of health data is allowed if it is in accordance with the provision of care treatment or the management of health-care services.

2.1.1.4.5 Information in cases of collection of data from the data subject (Article 10)

DAPHNE controller(s) or representatives must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

a) the identity of the controller and of his representative, if any;
b) the purposes of the processing for which the data are intended;
c) any further information such as
   - the recipients or categories of recipients of the data,
   - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
   - the existence of the right of access to and the right to rectify the data concerning him
d) in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

2.1.1.4.6 Information where the data have not been obtained from the data subject (Article 11)

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with information outlined in Article 11 in the DPD.

This would apply in DAPHNE in the case that there exists more than one controller and personal information is passed between them.

2.1.1.4.7 Right of access (Article 12)

DAPHNE shall guarantee every data subject the right to obtain from the controller:

a) without constraint at reasonable intervals and without excessive delay or expense:
   - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
   - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
   - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

2.1.1.4.8 The data subject's right to object (Article 14)

DAPHNE shall grant the data subject the right:

a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;
b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

c) Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

In the case of DAPHNE this should be related to the patient's right to withdraw from the service at any time.

2.1.1.4.9 Automated individual decisions (Article 15)

1. DAPHNE shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
2. Subject to the other Articles of this Directive, DAPHNE shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
    a. is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
    b. is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

Specific to the DAPHNE service to promote a high level of user confidence and trust all automatic processing should be handled as opt-in rather than opt-out.

2.1.1.4.10 Confidentiality of processing (Article 16)

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

2.1.1.4.11 Security of processing (Article 17)

1. DAPHNE 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.
2. DAPHNE shall provide that the controller must, where processing is carried out on his 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.
3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
    a. the processor shall act only on instructions from the controller,
    b. the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

The measures stated here are very high level and more guidance is available from Article 29´s WP131 (see section 2.1.2) and also from national legislations (see section 2.2).

2.1.1.4.12 Obligation to notify the supervisory authority (Article 18)

1. DAPHNE shall provide that the controller or his representative, if any, must notify (see Article 19) the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.
2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the specific conditions specified in the DPD.
3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.
4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).
5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

2.1.1.4.13 Liability (Article 23)

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the DAPHNE controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

2.1.2 Article 29 WP131 - Data Protection Working Party Working Document on Processing of Personal Data Relating to Health in EHR

2.1.2.1 Introduction

The Working Document WP131, being analysed in this section, relates to the processing of personal health data in electronic health records (EHR), and gives guidance from the Article 29[9] Working Party on the interpretation of the applicable data protection legal framework for EHR systems.

Article 29 define an EHR as "A comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form and providing for ready availability of these data for medical treatment and other closely related purposes".

In DAPHNE, health data is primarily captured from heuristic analysis of data received from patients´ medical devices to be used for clinical and non-clinical applications and services. Furthermore depending on the use case scenarios (still to be defined in the project) the health data stored in DAPHNE could include data added by health care professionals or equivalent, direct input by patients, input from patient EMRs and even synchronisation with patient´s medical EHRs could be possible.

Therefore to be able to manage health data in DAPHNE this would ideally be through the use of EHR type records and considering that DAPHNE is aimed at being a patient centric system it could be more apt to store all patient health data in PHRs. PHRs could then synchronise data to and from patients´ medical EHRs when DAPHNE data is used for medical group applications and services.

[9] The Article 29 Working Party is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor (EDPS) and the European Commission. Its name comes from the DPD and its main role is to give expert advice to the regarding data protection and promote the same application of the Data Protection Directive in all EU state members.

The actual data model will be defined later in the project and will also depend upon the use case scenarios to be proposed, however at this early stage it is considered here that DAPHNE will implement either EHRs or PHRs or both and the principles in the analysis of this Article 29 Opinion for EHRs equally apply to both EHRs and PHRs[10].

As such the following section contains the analysis of Article 29 Opinion on the processing of EHRs as per parts II & III of WP131, from the perspective of EHRs/PHRs being used in DAPHNE.

2.1.2.2 DAPHNE Specific Analysis of Article 29, WP131

2.1.2.2.1 The Data Protection Framework For Electronic Health Records (WP 131 - Part II)

In this section the document primarily addresses the general data protection principles and then classifies sensitive personal data relating to a person´s health and its protection.

1. General Principles
The general principles emphasised here and listed below all refer to Articles in the DPD that have previously been captured and underlined in section 2.1.1 in relation to DAPHNE and thus are only highlighted to show that these areas are also given relevance by Article 29 for EHRs.

- Use limitation principle (purpose principle) – Article 6(1)(b)
- The data quality principle – Article 6(1)(c)
- The retention principle – Article 6(1)(e)
- Information requirements (Transparency principle) – Article 10
- Data subject's right of access – Article 12
- Security related obligations – Article 17

2. Special Protection for sensitive personal data
Here it clarifies that "when the processing of such personal data relates to a person's health, processing is particularly sensitive and therefore requires special protection" and refers to the classification of personal data in the context of the DPD and references its Article 8(1) as highlighted previously in section 2.1.1.

Article 29 further goes on to state that any data associated to a person on medical grounds constitutes personal health data especially when included in a health record e.g. identifier even information on the occurrence of the event e.g. description of "individual injured her foot and is on half-time on medical grounds". And the note is made if the data is not relevant to the health record then it should not be included in it.

"As a consequence, the members of the Working Party are of the opinion that all data contained in medical documentation, in electronic health records and in EHR systems should be considered to be "sensitive personal data".

As regards the DAPHNE DaaS service it manages both non-medical data for "wellbeing" type services and medical data for health services and the Eurpoean Commision talks about this distinction between wellbeing and health in the communication on 'eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century" [5].

However the opinion of the EDPS on this above communication [6] is captured in statement 10 and 11 in the publicized opinion and included below for reference:

> 10. The Communication distinguishes between health data and well-being data. The EDPS would like to underline that both categories of data may involve the processing of personal data relating to health.

[10] See section 3 for more information on use of EHRs/PHRs in DAPHNE and the possible data that they may contain.

11. Processing of such data is subject to strict data protection rules as laid down in Article 8 of Directive 95/46/EC and its implementing national laws (and as foreseen in Article 9 of the proposed Data Protection Regulation). The EDPS wishes to underline that this sets a high standard with which compliance must be ensured and wishes to underline the guidance already given to controllers and processors in the area.

Therefore for DAPHNE**,** ALL the personal data handled by the DAPHNE DaaS service (whether used for health or wellbeing services) are not only subject to all the general rules on the protection of personal data in the Directive, but in addition subject to the special data protection rules on the processing of sensitive information contained in Article 8 of the Directive.

3. A general prohibition of the processing of personal data concerning health – with derogations
Article 8 of the DPD is clarified so that "All these derogations are limited, exhaustive and have to be construed in a narrow fashion".

4. Article 8(2)(a): "Explicit consent"

It is clarified here that a justification for the processing of sensitive data can be the consent of the data Subject as per Article 8 (2)(a) of the DPD.

Specifically for DAPHNE it is important to capture the following points:

a) For explicit consent to be valid it must be "freely given, specific and informed indication of the data subject's wishes", as defined in Article 2(h) of the DPD. And it is also defined that an "individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment".

b) In contrast to the provisions of Article 7 of the Directive, consent in the case of sensitive personal data and therefore in an EHR must be **explicit**. Opt-out solutions will not meet the requirement of being 'explicit'. In accordance with the general definition that consent presupposes a declaration of intent, explicitness must relate, in particular, to the **sensitivity of the data**. The data subject must be aware that he is renouncing special protection. Written consent is, however, not required.

c) The Article 29 Working Party has observed that it is sometimes complicated to obtain consent due to practical problems, in particular where there is no direct contact between the data controller and the data subjects. Whatever the difficulties, the **data controller** must be able to prove in all cases that, firstly, he has obtained the explicit consent of each data subject and, secondly, that this explicit consent was given on the basis of sufficiently precise information.

d) Again in contrast to Article 7, Article 8 (2) (a) acknowledges that there may be cases of processing of sensitive data in which **not even explicit consent** of the data subject should lift the prohibition of processing: Member States are free if, and how to regulate such cases in detail.

Therefore for DAPHNE:

- for the processing of non-medical data for wellbeing services the data controller(s) must obtain the explicit consent of each user for the processing of their data as per the national law[11] of where the controller has its service registered and operating. In the case of Italian Law it is seen in section 2.2.1 that explicit consent for processing of sensitive data requires the signature of the data subject.
- For the processing of medical data as part of ongoing medical care the data controller is able to process the patient's sensitive data as per Article 8(3) of the DPD as examined in point 6 below. However due

[11] As indicated previously, the national law may not permit the processing of sensitive data even if explicit consent has been given.

to reservations made by Article 29 on this derogation it is recommended that for DAPHNE explicit consent is always obtained.

5. Article 8 (2) (c): "vital interests of the data subject"
Not applicable to DAPHNE.

6. Article 8 (3): "processing of (medical) data by health professionals"

Article 8 (3) permits the processing of sensitive data where processing of the data is required for the purposes the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

However Article 29 Working Party point out major reservations on applying this derogation to the prohibition of processing sensitive data as follows:

- EHR systems create a new risk scenario, which calls for new, additional safeguards as counterbalance: EHR systems provide direct access to a compilation of the existing documentation about the medical treatment of a specific person, from different sources (e.g. hospitals, health care professionals) and throughout a lifetime. Such EHR systems therefore transgress the traditional boundaries of the individual patient's direct relationship with a healthcare professional or institution: The keeping of medical information in an EHR extends beyond the traditional methods of keeping and using medical documentation on patients.
- On the technical side, multiple access points over an open network like the internet increases possible patient data interception. Maintaining the legal standard of confidentiality suitable within a traditional paper record environment may be insufficient to protect the privacy interests of a patient once electronic health records are put online.
- Fully developed EHR systems thus tend to open up and facilitate access to medical information and sensitive personal data. EHR systems pose significant challenges in ensuring that only appropriate health professionals gain access to information for legitimate purposes related to the care of the data subject.
- They make the processing of sensitive personal data more complex with direct implications for the rights of the individuals. As a consequence an EHR system must be considered as a new risk scenario for the protection of sensitive personal data.
- The main and traditional safeguard in Art. 8 (3) – apart from the purpose limitation and the strict necessity requirement - is the obligation of medical professionals to confidentiality concerning medical data about their patients. This may no longer be fully applicable in an EHR environment, as one of the purposes of EHR is to grant access to medical documentation for the sake of treatment to such professionals who have not been party to the previous treatment documented in a medical file.
- Therefore, the Article 29 Working Party is not convinced that, even if Article 8 (3) is used as a justification for processing, relying only on the obligation to professional secrecy provides sufficient protection in an EHR environment.
- A new risk scenario calls for additional and possibly new safeguards beyond those required by Article 8 (3) in order to provide for adequate protection of personal data in an EHR context.

From the DAPHNE DaaS service perspective the purpose principle and transparency principle covered by Articles 6, 10, 11 & 12 of the DPD have to be strictly applied so that the data subjects´ data is only handled by authorised personnel and have access to health records to see his/her data and who was responsible for adding or accessing it[12].

7. Article 8 (4): substantial public interest exemptions
Not applicable to DAPHNE.

[12] This is subject to patient access rights implemented by member state legislation.

2.1.2.2.2 Reflections on a suitable legal framework for EHR systems (WP 131 – Part III)

In this section the document details needed safeguards for EHR systems to ensure patient rights and data protection.

1. Respecting self determination

It is identified here that even in the case that the EHR system is not based upon consent (Article 8(2) of the DPD) "the patient´s self-determination concerning when and how his data are used should have a significant role as a major safeguard".

a) It is recommended here that the functionality of "agreeing" (different from consent) should be used to cover scenarios where the patient did not need to give consent and thus still has the possibility to "opt-out" i.e. the right to refuse.

Therefore this "opt-out" capability should thus be made available in situations where by law the patient did not need to give explicit consent by default.

For the DAPHNE trial it is previously recommended that explicit consent is always obtained even in legal situations where not needed as in Article 8 (3) of the DPD. However giving the patient an opt-out capability at any time would give the patient the ability to later leave the service and thus should be included.

However where a member state law does not provide for this self-determination and is against the medical partner´s policy the option should be disabled.

b) Here it is recommended that health data is split into different categories in the EHR depending upon its sensitivity (e.g Genetic Data being more sensitive than wellbeing data), so that the patient can determine by "opt-in" measures what type of sensitive data to include in the EHR and opt-out measures for less sensitive data such as wellbeing data.

From the DAPHNE perspective this recommendation should be included in the case that the data model (to be defined) has different categories of data in the DAPHNE service.

c) It should in principle always be possible for a patient to prevent disclosure of his medical data, documented by one health professional during treatment, to other health professionals, if he so chooses. This is subject to national laws as some member states allow mandatory access to patient health records in order to provide optimal health protection.

From the DAPHNE perspective this recommendation seems very limiting and forces the patient to personally approve every health care access to their data which could be counterproductive to the manageability of the service. From DAPHNE perspective it is thus recommended that:

- the patient upon registration of the service gives explicit consent to that Personal Health Service be it a public or private medical institution or a wellbeing service. The healthcare professionals or recognised equivalent by national law will be assigned by PHS to the patient.
- the patient is able to monitor who is exactly accessing their data and for what purpose.
- the patient has the right to refuse further access and opt-out of that Personal Health Service as discussed in next point.

d) "Under the assumption that nobody could be forced to take part in an EHR system, in the legal provisions establishing an EHR system the question of possible complete withdrawal from an EHR system ought to be addressed."

From the DAPHNE perspective, and where allowed by member state law and not against a clinical partner´s policy, then by default the data retention principle DPD Article 8(1)(e) shall apply so that

the patients data is deleted or anonymised (as per national legislations´ safeguards). If PHR records are used then patients have full governance over whether the PHR data is deleted/anonymised.

2. Identification and authentication of patients and health care professionals

a) The recommendation here is that all patients are reliably identified using electronic identities (eIDs) using smart card technology.

b) For health care professionals it is not only recommended that electronic identities based on smart cards are used for reliable authentication it is advocating use of electronic signatures and to identify the different roles of the healthcare professionals associated to the identity e.g. nurse, doctor, admin etc.

From the DAPHNE perspective the recommendation for using eIDs should be taken on board for consideration in the design stage. Also the recommendation does not consider automatic access by medical devices to upload data and their authentication to the system. However this should be afforded similar levels of authentication as for natural persons and will be considered in the design phase.

3. Authorization for accessing EHR in order to read and write in EHR

a) It clarifies here that only the patient and also authorised professional health professionals who are currently involved in the patient´s treatment have access to a patient´s EHR/PHR, and that there must be a relationship of actual and current treatment between the patient and the healthcare professional wanting access to his EHR/PHR record.

It further recommends implementing modular access rights where authorisation access to different categories of health data is based on the authorisation level associated to the role of the health care professional e.g. patient´s doctor has access to all information whereas administration staff only have access to personal information.

b) The recommendation here is that patients should be able to restrict access to their EHR/PHR data to health professionals that have previously received the patient´s authorisation and should present the access token or electronically signed authorisation to get access.

This subject was discussed earlier in point 1(c) above and thus for DAPHNE it may not be suitable to have such restrictive behaviour and is possibly better to be handled on authorisation to the PHS as outlined for DAPHNE in relation to 1(c) above.

Additionally it recommends the idea that certain data may not be permitted by the patient to be included in the EHR/PHR and could instead be added to "sealed envelopes".

This should be considered in the DAPHNE design stage however it is not known if relevant at this stage for DAPHNE data.

c) Where feasible, it promotes direct access for patients to their EHRs through eID authentication so to achieve greater transparency and patient trust.

This will be considered in the DAPHNE design stage, for patient´s accessing their EHR/PHR records In relation to connecting to EHR records of PHS and medical centres this is considered out of the scope of the project.

Additionally it addresses the issue of whether a patient themselves should be able to directly enter data into the EHR themselves by (1) introducing a logging system that identifies who added what data and when, and also (2) that a specific patient module is supported in the EHR.

It is also highlighted that when considering EHR systems from the patient's perspective, the abilities and the special needs of the chronically ill, the elderly, as well as the handicapped and disabled must be taken into account.

Logging of all access and updates to the EHR/PHR should be considered in the DAPHNE design stage.

A specific patient module for patient input should be considered in the DAPHNE design stage.

The needs of all patients should be considered including the special needs of the chronically ill, the elderly, as well as the handicapped and disabled in the design phase of DAPHNE for access to PHR data.

4. Use of EHR for other purposes

It describes here how EHR access should be restricted legitimate access and exclude medical practioners acting on behalf of 3rd parties such as private insurance companies.

The recommendation is that all access to EHR/PHR data is restricted as per Article 8(3) of the DPD, and this will apply to DAPHNE.

The exception to this is that Processing of EHR-data for the purposes of medical scientific research and government statistics could be allowed as an exception to the rule set out above, provided that all these exceptions are in line with Article 8 (4) of the DPD.

As per this recommendation DAPHNE will be able to make use of EHR/ PHR data in anonymised form or at least with secure pseudonymisation, and as long as it is provided for in member state law.

5. Organisational structure of an EHR system

This part discusses different organisational alternatives for storing data in an EHR system with the following being the main alternatives:

- EHR as a system furnishing access to medical records kept by the health care professional, who has the obligation to keep records on the treatment of his patients – this is often called "**decentralised storage**", or
- EHR as a uniform system of storage, to which medical professionals have to transfer their documentation; this is often called "**centralised storage**";
- a third alternative could be to enable the data subject to be "**master**" of his own medical records by offering him storage of patients' medical data as a special *e*service under the patient's control, possibly even including the power to decide what goes into an EHR. This model has been adopted in France.

From the viewpoint of DAPHNE the actual model used, will be identified in the design phase and will also be subject to the medical partners policies of whom take part in the DAPHNE trial. The benefits and drawbacks identified under this point in the WP131 document should be referred to during design.

6. Categories of data stored in EHR and modes of their presentation

"The idea of an "EHR system" is basically to collect about one specific person all health related data which are presumably relevant for his long-term state of health, so that in case of future treatment comprehensive, relevant information is available and patients have a better chance of successful treatment."

From the DAPHNE perspective, for medical applications this sentence would hold true and it would be for DAPHNE to support a EHR/PHR that is compatible with EHRs of the DAPHNE partner medical groups.

For non-medical applications it is still needed to have a standard way of accessing health data and this could also be through the use of EHR/PHRs pursuant to national legislation providing recognised equivalent health professional status to the non-medical applications.

It is also an open point on whether the raw data captured from medical devices is required to be captured or is just processed, but if required to be stored, it could be held for example in a Medical Device Record as discussed in section 3.2.

a) It is highlighted here that According to the principles of relevance and proportionality of data collection, every compilation of data must be limited to those data which are relevant and not excessive for the defined purpose of the processing (Article 6(1)(c) of the Directive). The legitimacy of EHR systems will therefore also depend on an adequate solution of choosing the 'right' categories of data and the 'right' length of time for storing information in an EHR.

   This shall be considered during DAPHNE design phase.

b) Concerning the presentation of data within the EHR: The fact that it is possible to discern different categories of health data which require quite different degrees of confidentiality suggests that it might be generally useful to create different data modules within an EHR system with different access requirements. Refer to WP131 for more detail.

   This categorisation is considered in section 3.2 and shall be confirmed during DAPHNE design.

c) This part discusses the need for preparing presentation report of the EHR data with possibility inferred to summarise it and option to present certain categories of data.

   This shall be considered during DAPHNE design phase.

7. International transfer of medical records

This part determines that international transfer of medical data to countries outside the EU /EEA to make use of specific medical expertise is possible when the health data is anonymised or at least in pseudonymised form.

It further adds that if there is no explicit consent of the data subject for the transfer of personal data, this would also avoid the necessity of obtaining permission for this data transfer, as the data subject is not identifiable to the recipient.

Considering the elevated risk to the personal data in an EHR/PHR system in an environment without adequate protection, the Article 29 Working Party wants to underline that any processing – especially the storage – of EHR data should take place within jurisdictions applying the EU Data Protection Directive or an adequate data protection legal framework.

Within the DAPHNE trial it is not envisaged the sending of medical data belonging to EU citizens outside the EU. In relation to NEVET partner they likewise would not think to send any patient data to EU that was not at least in pseudonymised form.

8. Data security

The point makes recommendations on the use of Privacy Enhancing Technologies (PETs) where possible and covers main security principles captured below:

- the development of a reliable and effective system of electronic identification and authentication as well as constantly up-dated registers for checking on the accurate authorization of persons having or requesting access to the EHR system;
- comprehensive logging and documentation of all processing steps which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow up on correct authorization;
- effective back up and recovery mechanisms in order to secure the content of the system;

- preventing unauthorized access to or alteration of EHR data at the time of transfer or of back up storage, e.g. by using cryptographic algorithms;
- clear and documented instructions to all authorized personnel on how to properly use EHR systems and how to avoid security risks and breaches;
- a clear distinction of functions and competences concerning the categories of persons in charge of the system or at least involved in the system with a view to liability for shortcomings; regular internal and external data protection auditing.

DAPHNE will consider all of these points on board in the design phase of the project.

9. Transparency

This point emphasises the need for extra transparency concerning the content and the functioning of an EHR system in order to be able to trust in the system. It recommends notification to Data Protection supervisory authorities by the controller(s) of the system with detailed information on its service.

It additionally points to use of the Internet as the ideal information distributor to help create the necessary transparency about the EHR system and that it be free of charge, easy to use but safe access points for data subjects to check on the content and on disclosure of their EHR record.

DAPHNE will consider all these points in the design phase of the project, but it is important to note that the trial it is also subject to the policies of the medical partners.

10. Liability issues

This point stresses that any EHR system must also guarantee that the possible infringements of privacy which are caused by storing and furnishing medical data in an EHR system are adequately balanced by liability for damages caused e.g. by incorrect or unauthorized use of EHR data.

It further recommends that any introduction of EHR systems should in advance carefully conduct in-depth, expert civil and medical law studies and impact assessments to clarify the new liability issues likely to arise in this context, e.g. regarding the accuracy and completeness of data entered in EHR, defining how extensively a health care professional treating a patient must study an EHR, or about the consequences under liability law if access is not available for technical reasons, etc.

This exhaustive analysis is beyond the scope of this project and as concerns the liability damages related to DAPHNE this will be obtained from the national legislation of the country where a trial is carried out.

11. Control mechanisms for processing data in EHR

This point considers the considerable created by the establishment of EHR systems and insists on **effective control mechanisms** for evaluating the existing safeguards are necessary. The complexity and sensitivity of the information contained in an EHR together with the multitude of users calls for new procedures as follows:

a) A special arbitration procedure should be set up for disputes about the correct use of data in EHR systems; the data subjects should be able to make use of such a procedure easily and free of charge. Considering the fact that usually special medical expertise will be necessary to evaluate claims for false or unnecessarily processed information in EHR systems, the Data Protection Supervisory Authorities might not be the best choice for dealing with such claims, at least not in the first instance. Public "Patients' Advocates" could, where they exist already, be put in charge of this task.

b) An EHR system must ensure that the data subject is able to exercise his access rights without undue difficulties. In principle it is the data controller who is obliged to give access. EHR systems are, however, information pool systems with many different data controllers. In such systems with a large number of participating data controllers, a single special institution must be made responsible towards the data subjects for the proper handling of access requests. In view of the foreseeable complexity of a fully developed EHR and the necessity of building trust with patients in the system, it seems essential that patients whose data are processed in an EHR system know how to reach a

responsible partner with whom they could discuss possible shortcomings of the EHR system. Special regulations to this end will have to be included in any regulation on EHR systems.

c) In order to establish trust, a special routine for informing the data subject when and who accessed data in his EHR could be introduced. Furnishing the data subjects in regular intervals with a protocol listing the persons or institutions who accessed their file would reassure patients about their ability to know what is happening to their data in the EHR system.
d) Regular internal and external data protection auditing of access protocols must take place. The already mentioned annual access report sent to the data subjects would be an additional effective means for checking legality of use of EHR data. Data protection officers in hospitals which take part in EHR systems would certainly improve the probability of correct use of data in these systems.

DAPHNE will consider all these points in the design phase of the project, but it is important to note that the trial it is also subject to the policies of the medical partners.

2.1.3 Council of Europe, Recommendation No. R (97) 5 on the Protection of Medical Data

2.1.3.1 Introduction

The Council of Europe is an international organisation founded in 1949 and promotes the co-operation between all countries of Europe in the areas of legal standards, human rights, democratic development, the rule of law and cultural co-operation. Although recommendation was produced in 1997, it is still applicable today in relation to the collection and automatic processing of medical data in the context of data protection with appropriate confidentiality and security safeguards pursuant to implementation in member state law. As such, it has been used by Member States to base their respective laws on the processing of medical data and in turn established by medical institutions and health professionals.

The Recommendation is based on the importance of the quality, integrity and availability of medical data for the health of the data subject and his family and is aware of the increasing use of automatic processing of medical data by information systems for medical care, medical research, hospital management and public health. Simultaneously, the dependency to a great extent on the availability of medical data on individuals for the progress of medical science is recognised.

2.1.3.2 Definitions

Before analysing the recommendation it is needed to include some of its definitions:

Personal data Covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and manpower. In cases where the individual is not identifiable, the data are referred to as anonymous

Medical data Refers to all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data;

Genetic data Refers to all data, of whatever type, concerning the hereditary characteristics of an individual or concerning the pattern of inheritance of such characteristics within a related group of individuals.

2.1.3.3 DAPHNE Specific Analysis of the Rights and Principles of R(97) 5

The principles of R(97) 5 are similar to those specified by the European Data Protection Directive in the context of protection of personal data however they merit analysis from the DAPHNE perspective for their specific application to medical healthcare.

The regulation and the principles it establishes are analysed in the rest of this section and the main points relevant for DAPHNE are included.

2.1.3.3.1 3. Respect to Privacy

The Recommendation covers the basic principle that the respect of rights and fundamental freedoms and in particular the right to privacy shall be guaranteed during the collection and processing of medical data, and that the data should be collected and processed only by health-care professionals, or by individuals or bodies working on behalf of health-care professionals. Individuals or bodies working on behalf of health-care professionals who collect and process medical data should be subject to the same rules of confidentiality incumbent on health-care professionals, or to comparable rules of confidentiality."

From DAPHNE perspective this reiterates previous recommendations made in the DPD and Article 29 WP131.

2.1.3.3.2 4. Collection and processing of medical data

The applicable points for DAPHNE are underlined as follows and those principles such as concerning genetic data are not included here as are not applicable to DAPHNE:

- Medical data shall in principle be obtained from the data subject. They may only be obtained from other sources if in accordance with Principles 4, 6 and 7 of this recommendation and if this is necessary to achieve the purpose of the processing.

- Medical data may be collected and processed:
  - if provided for by law for public health reasons;
  - if permitted by law for preventive medical purposes or for diagnostic or for therapeutic purposes with regard to the data subject
  - if the data subject or his/her legal representative or an authority or any person or body provided for by law has given his/her consent for one or more purposes, and in so far as domestic law does not provide otherwise.

- If medical data have been collected for preventive medical purposes or for diagnostic or therapeutic purposes with regard to the data subject or a relative in the genetic line, they may also be processed for the management of a medical service operating in the interest of the patient, in cases where the management is provided by the health-care professional who collected the data, or where the data are communicated.

From DAPHNE perspective this mainly reiterates previous recommendations made in the DPD and Article 29 WP131.

2.1.3.3.3 5. Information of the data subject

The data subject shall be informed of the following elements:

- the existence of a file containing his/her medical data and the type of data collected or to be collected
- the purpose or purposes for which they are or will be processed
- where applicable, the individuals or bodies from whom they are or will be collected
- the persons or bodies to whom and the purposes for which they may be communicated
- the possibility, if any, for the data subject to refuse his consent, to withdraw it and the consequences of such withdrawal
- the identity of the controller and of his/her representative, if any, as well as the conditions under which the rights of access and of rectification may be exercised.

The data subject should be informed at the latest at the moment of collection. However, when medical data are not collected from the data subject, the latter should be notified of the collection as soon as possible, as well as - in a suitable manner - of the information listed above, unless this is clearly unreasonable or impracticable, or unless the data subject has already received the information.

If the data subject is a legally incapacitated person, incapable of free decision and domestic law does not permit the data subject to act on his/her own behalf, the information shall be given to the person recognised as legally entitled to act in the interest of the data subject.

From DAPHNE perspective this further clarifies information communicated to the data subject or person legally entitled to act in their interest.

2.1.3.3.4 6. Consent

Consent given in the DAPHNE context is more fully captured by the recommendations of Article 29, WP 131 as described in section 2.1.2.

What this section further clarifies for DAPHNE is the case of a legally incapacitated person who is incapable of free decision, and when domestic law does not permit the data subject to act on his/her own behalf, consent is required of the person recognised as legally entitled to act in the interest of the data subject or of an authority or any person or body provided for by law.

2.1.3.3.5 7. Communication

The conditions under which medical data can be communicated are a reiteration of those that are already covered for its processing in the DPD and Article 29 WP131, with addition that the legal representative of the data subject can act on their behalf.

2.1.3.3.6 8. Rights of the data subject

Every person shall be enabled to have access to their own medical data, either directly or through a health-care professional or, if permitted by domestic law, a person appointed by him/her. The information must be accessible in understandable form. The medical data may be restricted or delayed pursuant to national legislation if the information could cause serious harm to their health.

As concerns DAPHNE, the rights of access and of rectification are further reiterated here for medical data as previously expressed in the DPD and Article 29 WP131.

2.1.3.3.7 9. Security

This section reiterates some points previously recommended by Article 29 WP131 and provides some added guidance such as the separation of personal identifiers from health data. This will provide input for the DAPHNE design stage, and the important points are underlined below.

Appropriate technical and organisational measures shall be taken to protect personal data - processed in accordance with this recommendation - against accidental or illegal destruction, accidental loss, as well as against
unauthorised access, alteration, communication or any other form of processing.

Such measures shall ensure an appropriate level of security taking account, on the one hand, of the technical state of the art and, on the other hand, of the sensitive nature of medical data and the evaluation of potential risks.

These measures shall be reviewed periodically.

In order to ensure in particular the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, appropriate measures should be taken:

- to prevent any unauthorised person from having access to installations used for processing personal data (control of the entrance to installations);

- to prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);
- to prevent the unauthorised entry of data into the information system, and any unauthorised consultation, modification or deletion of processed personal data (memory control);
- to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment (control of utilisation);
- with a view to, on the one hand, selective access to data and, on the other hand, the security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of:
    - identifiers and data relating to the identity of persons
    - administrative data
    - medical data
    - social data
    - genetic data (access control);

- to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (control of communication);
- to guarantee that it is possible to check and establish a posteriori who has had access to the system and what personal data have been introduced into the information system, when and by whom (control of data introduction);
- to prevent the unauthorised reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media (control of transport)
- to safeguard data by making security copies (availability control).

Controllers of medical files should, in accordance with domestic law, draw up appropriate internal regulations which respect the related principles in this recommendation.

Where necessary, controllers of files processing medical data should appoint an independent person responsible for security of information systems, and data protection and competent for giving advice on these issues.

2.1.3.3.8 10. Conservation

The general principle conservation principle is previously covered by the DPD and Article 29 WP131, in that medical data shall be kept no longer than necessary to achieve the purpose for which they were collected and processed.

Importantly it clarifies for DAPHNE that upon the request of the data subject, his/her medical data should be erased - unless they have been made anonymous or there are overriding and legitimate interests, in particular those stated below not to do so, or there is an obligation to keep the data on record.

When, in the legitimate interest of public health, medical science, the person in charge of the medical treatment or the controller of the file, in order to enable him/her to defend or exercise a legal claim, or for historical or statistical reasons, it proves necessary to conserve medical data that no longer serve their original purpose, technical arrangements shall be made to ensure their correct conservation and security, taking into account the privacy of the patient.

2.1.3.3.9 11. Transborder flows

The Recommendation considers no special conditions are required to the trans-border flow of medical data to a state that has ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and which disposes of legislation which provides at least equivalent protection of medical data [8]. If the state has not ratified the Convention but has legal provisions which ensure protection in accordance with the principles of that convention and this recommendation, no restriction on trans-border data flow should be placed either.

Unless specific provisions by domestic law, trans-border flows should not occur to other countries unless necessary measures, including those of a contractual nature, to respect the principles of the convention and this recommendation, have been taken, and the data subject has the possibility to object to the transfer or the data subject has given his consent.

In the case of DAPHNE trial the transborder flow of personal identifiable data from EU citizens outside the EU is not considered. Indeed for the clinical partners taking part in the trial there is no scenario identified where personal identifiable health data of EU citizens is communicated to 3rd parties outside their own country.

2.1.3.3.10 12. Scientific research

This principle is related to the use of medical data for scientific research and as such is applicable to the bulk data service in DAPHNE and in this context it states that whenever possible, medical data used for scientific research purposes should be anonymous.

2.1.4 Patients´ Rights Directive 2011/24/EU cross-border healthcare

The directive in principle applies to individual patients who decide to seek healthcare in a Member State other than the Member State of affiliation. By following its provisions, Member States must ensure that the healthcare providers on their territory apply the same scale of fees for healthcare for patients from other Member States, as for domestic patients in a comparable medical situation (Art. 4, para 4).

The thrust of this directive is not entirely applicable to DAPHNE, as it is aimed more at national healthcare providers and covers insurance topics too. However that said it still does apply to DAPHNE DaaS service in a scenario where the DAPHNE service or DAPHNE PHS were registered as a "heathcare provider" in one EU country and offered its services to EU citizens from other member states. It is from this perspective that the main applicable articles of the Patients´ Rights Directive are analysed in relation to DAPHNE.

For the DAPHNE trial however there will be no cross-border services in the EU and therefore this is added for information only for possible exploitation scenarios.

2.1.4.1 Definitions

Healthcare	Health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices
Member State of treatment	The Member State on whose territory healthcare is actually provided to the patient. In the case of telemedicine, healthcare is considered to be provided in the Member State where the healthcare provider is established
Cross-border healthcare	Healthcare provided or prescribed in a Member State other than the Member State of affiliation
Health professional	A doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment

Healthcare provider	Any natural or legal person or any other entity legally providing healthcare on the territory of a Member State
Patient	Any natural person who seeks to receive or receives healthcare in a Member State
Medical device	A medical device as defined by Directive 90/385/EEC, Directive 93/42/EEC or Directive 98/79/EC
Medical records	All the documents containing data, assessments and information of any kind on a patient's situation and clinical development throughout the care process.

2.1.4.2 DAPHNE Specific Analysis of the Patients´ Rights directive

2.1.4.2.1 Article 1 Subject matter and scope

This Directive provides rules for facilitating the access to safe and high-quality cross-border healthcare and promotes cooperation on healthcare between Member States, in full respect of national competencies in organising and delivering healthcare.

The Directive shall apply to the provision of healthcare to patients, regardless of how it is organised, delivered and financed.

This would therefore apply to DAPHNE if it were to deliver cross-border healthcare through a Personal Health Service for example where the PHS offers an expert healthcare service where dedicated health professionals analyse a patient´s Daphne data.

2.1.4.2.2 Article 4 Responsibilities of the Member State of treatment

1. In this article it is described that each member state must take into account the principles of universality, access to good quality care, equity and solidarity, cross-border healthcare shall be provided in accordance with:
   a) the legislation of the Member State of treatment;
   b) standards and guidelines on quality and safety laid down by the Member State of treatment; and
   c) Union legislation on safety standards.

2. The Member State of treatment shall ensure that:
   a) patients receive from the national contact point referred to in Article 6, upon request, relevant information on the standards and guidelines referred (to in paragraph 1(b) of this Article above), including provisions on supervision and assessment of healthcare providers, information on which healthcare providers are subject to these standards and guidelines and information on the accessibility of hospitals for persons with disabilities.

Therefore for DAPHNE to offer cross-border healthcare the necessary provisions stipulated here must be made available at member state level. The article continues (in paragraphs b to e) to give advice on the necessary information that the healthcare providers would need to facilitate such as quality and safety of service credentials, pricing etc.

   f) in order to ensure continuity of care, patients who have received treatment are entitled to a written or electronic medical record of such treatment, and access to at least a copy of this record in conformity with and subject to national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC.

In the DAPHNE service the PHS would be connected to DAPHNE and able to input the EMR into the EHR or PHR.

2.1.4.2.3 Article 5 Responsibilities of the Member State of affiliation

Amongst the many different responsibilities outlined here an important point for DAPHNE to capture is where it states that patients who seek to receive or do receive cross-border healthcare have remote access to or have at least a copy of their medical records, in conformity with, and subject to, national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC.

The aim of DAPHNE service is that the system should be patient centric and have remote access to their health data. However this will be clarified in the design phase.

2.1.4.2.4 Article 14 eHealth

This article specifies that the Union shall support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States.

It further describes amongst objectives to work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare and to draw up guidelines on:

- a non-exhaustive list of data that are to be included in patients' summaries and that can be shared between health professionals to enable continuity of care and patient safety across borders; and
- (ii) effective methods for enabling the use of medical information for public health and research;

Additionally it is identified to support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare.

The objectives shall be pursued in due observance of the principles of data protection as set out, in particular, in Directives 95/46/EC and 2002/58/EC.

This is important input for DAPHNE in that it shows the focus in the EU at promoting cross-border healthcare and gives DAPHNE greater exploitation possibilities by including cross-border scenarios. In this context reference should be made to the successful epSOS project [9] that had the primary aim to to show conditions of legal, organizational, semantic and technical interoperability of cross-border eHealth based services.

The aim of the epSOS project goes beyond that of DAPHNE however some guidance can be taken with respect to privacy and data protection in terms of its legal implications and implementation of eID for authentication and authorisation.

2.1.5 Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling

The recommendation is concerned with the possibilities of profiling that is possible with modern Information and communication technologies (ICTs) which allow the collection and processing on a large scale of data, including personal data, in both the private and public sectors.

It highlights the that data collection and processing of large amounts of personal data is able to perform calculations, comparisons and statistical correlations to produce profiles based that could be used in many ways for different purposes and is able to be used to match with the data of actual individuals.
Through this linking of a large number of individual, even anonymous, observations, the profiling technique is capable of having an impact on the people concerned by placing them in predetermined categories, very often without their knowledge.

In summary the lack of transparency, or even "invisibility", of profiling and the lack of accuracy that may derive from the automatic application of pre-established rules of inference can pose significant risks for the individual's rights and freedoms.

Article 3(c) on Sensitive Data prohibits the collection and processing of sensitive data in the context of profiling except if these data are necessary for the lawful and specific purposes of processing and as long as domestic law provides appropriate safeguards. When consent is required it shall be explicit where the processing concerns sensitive data.

Therefore DAPHNE should take care to follow this recommendation and avoid the offering their bulk data to parties that are interested in creating profiles that are not pursuant to the national legislation.

2.1.6 Directive 2002/58/EC on Privacy and Electronic Communications

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).

This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union [10]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

This Directive complements Directive 95/46/EC and additionally provides for protection of the legitimate interests of subscribers who are legal persons.

The Directive obliges providers of electronic communications services to provide security of services on their networks, which includes the duty to inform the subscribers whenever there is a particular risk, such as a virus or other malware attack. Further provisions are made on the confidentiality of traffic data and traffic data retention.

These issues will have to be adhered to by a DAPHNE CSP implemented on a private cloud and that is responsible for the private data network and the data communication over the internet.

Relevant to all DAPHNE scenarios is the use of cookies so that pre-consent is required for use of cookies where the cookie is not essential to the running of the service.

2.1.7 Recommendation No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes

For DAPHNE it is important to capture here that processing of personal data that was collected for non-statistical purposes is not incompatible if appropriate safeguards are provided for, in particular to prevent the use of the data for supporting decisions or measures in respect of the data subject.

When processing sensitive data for statistical purposes it should be collected in a form in which the data subjects are not identifiable.

Statistical results may be published or made accessible to 3rd parties only if measures are taken to ensure that the data subjects are no longer identifiable, unless dissemination or publication present risk of infringing the privacy of the data subjects.

In the case of DAPHNE where data is primarily collected for non-statistical purposes the data subject shall be informed of the further use of their data for anonymous statistics and with all information mentioned in article 5.1 provided in a suitable manner e.g. indicate whether the additional statistical use of their data is optional or not. However in the case where national legislation provides for statistical processing of a patients data this may not be necessary.

2.1.8 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108]

The purpose of this convention is to secure for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.

Definitions:

Automated data file	Any set of data undergoing automatic processing
Automatic processing	Includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination

This convention focuses on the processing of automated data files and is thus applicable to DAPHNE. However upon review, the applicable principles are already covered in the data protection and privacy directives and regulations already analysed for DAPHNE earlier in the section.

2.1.9 Article 29 WP196 - Opinion 05/2012 on Cloud Computing

2.1.9.1 Introduction

"In this Opinion the Article 29 Working Party analyses all relevant issues for cloud computing service providers operating in the European Economic Area (EEA) and their clients specifying all applicable principles from the EU Data Protection Directive (95/46/EC) and the e-privacy Directive 2002/58/EC (as revised by 2009/136/EC) where relevant."

The Opinion acknowledges the benefits of cloud computing before detailing how the wide scale deployment of cloud computing services can generate a number of data protection risks, generalised by a lack of control over personal data as well as little transparency with regard to how, where and by whom the data is being processed/sub-processed.

The Opinion notes that these risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider. This Opinion examines the known issues associated with the cloud computing such as the sharing of resources with other parties, the lack of transparency and uncertainty with regard to the admissibility of the transfer of personal data to cloud providers established outside of the EEA.

To conclude the Opinion makes a list of recommendations of which those applicable to DAPHNE are captured in the following section.

2.1.9.2 DAPHNE Specific Analysis of Article 29 WP196

The recommendations included in this section are meant to provide a checklist for data protection compliance by cloud clients and cloud providers based on the current legal framework[13].

2.1.9.2.1 Guidelines for clients and providers of cloud computing services

Controller-processor relationship
This Opinion focuses on the client-provider relationship as controller-processor relationship (see paragraph 3.3.1 of the Opinion). Nevertheless based on concrete circumstances situations may exist where the cloud

[13] Some recommendations are also provided with a view to future developments in the regulatory framework at EU but these are not included here as are not provided for in current regulations.

provider acts as a controller as well, e.g. when the provider re-processes some personal data for its own purposes. In such a case, the cloud provider has full (joint) responsibility for the processing and must fulfil all legal obligations that are stipulated by Directives 95/46/EC and 2002/58/EC (if applicable).

The actual scenarios for DAPHNE are yet to be confirmed and guidance on whether the CSP will have full or joint controller responsibilities should refer to here and section 3.3.1 of the Opinion.

Cloud client's responsibility as a controller
The client as the controller must accept responsibility for abiding by data protection legislation and is subject to all the legal obligations mentioned in Directive 95/46/EC and 2002/58/EC, where applicable, in particular vis-à-vis data subjects. The client should select a cloud provider that guarantees compliance with EU data protection legislation as reflected by the appropriate contractual safeguards summed up below.

The possible DAPHNE clients will be clarified when the scenarios are confirmed and then the data controller responsibilities will be made clear. Also the DAPHNE will follow the recommendation that the CSP guarantees EU data protection legislation as summed up by the following safeguards summed up below.

Subcontracting safeguards
Provisions for subcontractors should be provided for in any contract between the cloud provider and cloud clients. The contract should specify that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. The cloud provider should sign a contract with each subcontractor reflecting the stipulations of his contract with the cloud client; the client should ensure that it has contractual recourse possibilities in case of contractual breaches by the provider's sub-contractors.

This recommendation is more likely to affect real deployments as no subcontractors are envisaged for the trial. However due to the sensitive data processed in DAPHNE then it should be avoided in any scenario that subcontractors process identifiable sensitive data. In the case that subcontractors will process sensitive data then the client should make sure that the CSP and subcontractor(s) follow this recommendation.

Compliance with fundamental data protection principles

- Transparency: cloud providers should inform cloud clients about all (data protection) relevant aspects of their services during contract negotiations; in particular, clients should be informed about all subcontractors contributing to the provision of the respective cloud service and all locations in which data may be stored or processed by the cloud provider and/or its subcontractors (notably, if some or all locations are outside of the European Economic Area (EEA)); the client should be provided with meaningful information about technical and organisational measures implemented by the provider; the client should as a matter of good practice inform data subjects about the cloud provider and all subcontractors (if any) as well as about locations in which data may be stored or processed by the cloud provider and/or its subcontractors;
- Purpose specification and limitation: the client should ensure compliance with purpose specification and limitation principles and ensure that no data is processed for further purposes by the provider or any subcontractors. Commitments in this respect should be captured in the appropriate contractual measures (including technical and organisational safeguards);
- Data retention: the client is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes; secure erasure mechanisms (destruction, demagnetisation, overwriting) should be provided for contractually;

Due to sensitive data handled by DAPHNE the CSP and any subcontractors must assure that data is processed and stored in EEA. The above data protection principles must all be carried out for DAPHNE.

Contractual safeguards:

- In general: the contract with the provider (and the ones to be stipulated between provider and sub-contractors) should afford sufficient guarantees in terms of technical security and organizational measures (under Article 17(2) of the directive) and should be in writing or in another equivalent form. The contract should detail the client's instructions to the provider including subject and time frame of the service, objective and measurable service levels and the relevant penalties (financial or otherwise); it should specify the security measures to be complied with as a function of the risks of the processing and the nature of the data, in line with the requirements made below and subject to more stringent measures as envisaged under the client's national law; if cloud providers aim at making use of standard contractual terms, they should ensure that these terms comply with data protection requirements; in particular technical and organisational measures that have been implemented by the provider should be specified in the respective terms;
- Access to data: only authorised persons should have access to the data; a confidentiality clause should be included in the contract vis-à-vis the provider and its employees;
- Disclosure of data to third parties: this should be regulated only via the contract, which should include an obligation for the provider to name all its sub-contractors – e.g. in a public digital register – and ensure access to information for the client of any changes in order to enable him to object to those changes or terminate the contract; the contract should also require the provider to notify any legally binding request for disclosure of the personal data by a law enforcement authority, unless such disclosure is otherwise prohibited; the client should warrant that the provider will reject any non-legally binding requests for disclosure;
- Obligations to co-operate: client should ensure that the provider is obliged to co-operate with regard to the client's right to monitor processing operations, facilitate the exercise of data subjects' rights to access/correct/erase their data, and (where applicable) notify the cloud client of any data breaches affecting client's data;
- Cross-border data transfers: The cloud client should verify if the cloud provider can guarantee lawfulness of cross-border data transfers and limit the transfers to countries chosen by the client, if possible. Transfers of data to non-adequate third countries require specific safeguards via the use of Safe Harbor arrangements, standard contractual clauses (SCC) or binding corporate rules (BCR) as appropriate; the use of SCC for processors (under Commission's decision 2010/87/EC) requires certain adaptations to the cloud environment (to prevent having separate per-client contracts between a provider and its subprocessors) which might imply the need for prior authorisation from the competent DPA; a list of the locations in which the service may be provided should be included in the contract;
- Logging and auditing of processing: the client should request logging of processing operations performed by the provider and its sub-contractors; the client should be empowered to audit such processing operations, however third-party audits chosen by the controller and certification may also be acceptable providing full transparency is guaranteed (e.g. by providing for the possibility to obtain a copy of a third-party audit certificate or a copy of the audit report verifying certification);
- Technical and organisational measures: these should be aimed at remedying the risks entailed by lack of control and lack of information that feature most prominently in the cloud computing environment. The former include measures aimed at ensuring availability, integrity, confidentiality, isolation, intervenability and portability as defined in the paper whilst the latter focus on transparency.

For DAPHNE to capture and apply the privacy and data protection agreements between the CSP and client controller it is identified to make use of a Privacy Level Agreement as detailed in section 4.

In addition to these guideline recommendations the commission has also tasked ETSI to "promote trusted and reliable cloud offerings by tasking ETSI to coordinate with stakeholders in a transparent and open way to identify by 2013 a detailed map of the necessary standards (inter alia for security, interoperability, data portability and reversibility". ETSI Cloud Standards Coordination (CSC) produced a final report [14] at the end of 2013 and should be referred to for data protection and privacy input during the DAPHNE design phase.

2.1.9.2.2 4.2 Third Party Data Protection Certifications

- Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion. Such certification would, as a minimum, indicate that data protection controls have been subject to audit or review against a recognised standard meeting the requirements set out in this Opinion by a reputable third party organisation. In the context of cloud computing, potential customers should look to see whether cloud services providers can provide a copy of this third party audit certificate or indeed a copy of the audit report verifying the certification including with respect to the requirements set out in this Opinion.
- Individual audits of data hosted in a multi-party, virtualised server environment may be impractical technically and can in some instances serve to increase risks to those physical and logical network security controls in place. In such cases, a relevant third party audit chosen by the controller may be deemed to satisfy in lieu of an individual controller's right to audit.
- The adoption of privacy-specific standards and certifications is central to the establishment of a trustworthy relationship between cloud providers, controllers and data subjects.
- These standards and certifications should address technical measures (such as localisation of data or encryption) as well as processes within cloud providers' organisation that guarantee data protection (such as access control policies, access control or backups).

Third party certification is outside the scope of the DAPHNE trial but should be realised in any real deployment.

2.2 National Legislations

2.2.1 Italy

2.2.1.1 Law

The Italian law applicable on privacy issues is the Legislative Decree no. 196 of 30 June 2003 ("*Codice in materia di protezione dei dati personali*", the "**Privacy Code**").

The Privacy Code implements Directives 95/46/EC and 2002/58/EC.

Furthermore the Italian Data Protection Authority has released a simple but comprehensive guide [15] on Cloud Computing and should be referred to. According to the guidelines, the current laws may need to be updated in order to apply adequately to cloud computing. In particular, certain key legal issues—allocation of liabilities, data security, jurisdiction and notification of breaches to the supervisory authority, as already proposed at the EU level in the new GDPR (see section 2.4) are highlighted as arising from the adoption of data processing and storage services outsourced *via* the internet.

Nonetheless, the existing rules still apply to cloud services. In particular, by entrusting an external provider with databases and processing operations, the client user (which qualifies as Data Controller), must appoint the cloud service provider as external Data Processor, formally and in writing as required by the Italian Personal Data Protection Code (see section 2.2.1.16 for more information).

2.2.1.2 Definitions

Definitions like "data controller", "data processor", or "data subject" are equivalent to how they are defined by the European Data Protection Directive.

2.2.1.2.1 Personal Data

Pursuant to section 4 of the Privacy Code, "personal data" shall mean any information relating to individuals who are or can be identified, even indirectly, by reference to any other information including a personal

identification number. Such data, according to section 2 shall be “processed by respecting data subjects’ rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection”

2.2.1.2.2 Sensitive Personal Data

Pursuant to Section 4 of the Privacy Code, "sensitive data" shall mean 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.

2.2.1.2.3 National Data Protection Authority

Garante per la protezione dei dati personali (the "**Garante**").

2.2.1.2.4 Processing

Any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank (any organised set of personal data, divided into one or more units located in one or more places). Section 30 establishes that processing operations may only be performed by persons in charge of the processing that act under the direct authority of either the data controller or the data processor by complying with the instructions received.

2.2.1.2.5 Anonymous data

Anonymous data shall mean any data that either in origin or on account of its having been processed cannot be associated with any identified or identifiable data subject.

2.2.1.2.6 Communication

When personal data are disclosed to one or more identified entities other than the data subject, the data controller or data processor and “dissemination” (when personal data are disclosed to any unidentified entities).

2.2.1.3 Notification of the Processing

In relation to DAPHNE handling personal and sensitive data the “Garante” must be notified as per the rule described below.

Pursuant to Section 37 of the Privacy Code, a data controller shall notify the processing of personal data he/she intends to perform exclusively if said processing concerns data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure.

The Garante’s website has an online form to send the notification and includes the following:

- Information to identify the data controller and, where appropriate, his/her representative, as well as the arrangements to identify the data processor if the latter has been appointed;
- The purpose(s) of the processing;
- A description of the category/categories of data subject and the data or data categories related to the said category/categories of data subject;
- The data recipients or the categories of data recipient;
- Data transfers to third countries, where envisaged;

- A general description that shall allow assessing beforehand whether the measures adopted to ensure security of the processing are adequate.

2.2.1.4 Data Minimization Principle

In accordance with the DPD, section 3 covers the minimisation principle. Information systems and software shall be configured by minimising 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.

Section 11 covers further privacy principles in that personal data undergoing processing shall be:

- processed lawfully and fairly;
- collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes;
- accurate and, when necessary, kept up to date;
- relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;
- kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

2.2.1.5 Data Protection Officer

Italy has no legal requirement for organisations to appoint a data protection officer.

2.2.1.6 Data Collection and Processing

2.2.1.6.1 Public Bodies

Sections 21-22 determine that "processing of sensitive data by public bodies shall only be allowed where it is expressly authorised by a law specifying the categories of data that may be processed and the categories of operation that may be performed as well as the substantial public interest pursued" and that they may process such data exclusively "as are indispensable for them to discharge institutional tasks that cannot be performed, on a case by case basis, by processing anonymous data or else personal data of a different nature" and "in accordance with arrangements aimed at preventing breaches of data subjects' rights, fundamental freedoms and dignity".

2.2.1.6.2 Private Bodies or Profit Seeking Public Bodies

As a general rule, processing of personal (non sensitive) data by private entities or profit seeking public bodies is only allowed if the data subject gives his/her express consent (Section 23 of the Privacy Code). The data subject's consent is deemed to be effective if it is 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 a privacy information notice compliant with section 13 of the Privacy Code.
As regards to the DAPHNE service, sensitive data may only be processed with the data subject's written consent and the Garante's prior authorisation[14], by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations.

2.2.1.6.3 Professional Secrecy

Ensuring professional secrecy is important as expressed in Section 83, also by "subjecting persons in charge of the processing that are not bound by professional secrecy under the law to rules of practice that are similar to those based on professional secrecy".

[14] The Garante has issued general authorizations for the processing of sensitive data

Code of conduct for scientific research provided as an Annex determines that "when processing data suitable for disclosing health, the entities concerned shall comply with the confidentiality and security rules health care professionals are required to apply, or else with comparable confidentiality and security rules".

2.2.1.6.4 Scientific Research

The data subject's consent shall not be required for processing data disclosing health with a view to scientific research activities in the medical, bio-medical or epidemiological sectors if said research activities are expressly provided for by legislation that specifically refers to the processing, or else are included in a bio-medical or health care research programme pursuant to Section 12-bis of legislative decree no. 502 of 30.12.92, as subsequently amended, and forty-five days have elapsed since communication of said activities to the Garante under Section 39.

2.2.1.6.5 Principles Applying to the Processing of Sensitive Data as well as to Judicial Data

1. Public bodies shall process sensitive and judicial data in accordance with arrangements aimed at preventing breaches of data subjects' rights, fundamental freedoms and dignity.
2. When informing data subjects as per Section 13, public bodies shall expressly refer to the provisions setting out the relevant obligations or tasks, on which the processing of sensitive and judicial data is grounded.
3. Public bodies may process exclusively such sensitive and judicial data as are indispensable for them to discharge institutional tasks that cannot be performed, on a case by case basis, by processing anonymous data or else personal data of a different nature
4. Sensitive and judicial data shall be collected, as a rule, from the data subject.
5. In pursuance of Section 11(1), letters c), d) and e), public bodies shall regularly check that sensitive and judicial data are accurate and updated, and that they are relevant, complete, not excessive and indispensable with regard to the purposes sought in the individual cases – including the data provided on the data subject's initiative. With a view to ensuring that sensitive and judicial data are indispensable in respect of their obligations and tasks, public bodies shall specifically consider the relationship between data and tasks to be fulfilled. No data that is found to be excessive, irrelevant or unnecessary, also as a result of the above checks, may be used, except for the purpose of keeping - pursuant to law - the record or document containing said data. Special care shall be taken in checking that sensitive and judicial data relating to entities other than those which are directly concerned by the service provided or the tasks to be fulfilled are indispensable.
6. Sensitive or judicial data that are contained in lists, registers or data banks kept with electronic means shall be processed by using encryption techniques, identification codes or any other system such as to make the data temporarily unintelligible also to the entities authorised to access them and allow identification of the data subject only in case of necessity, by having regard to amount and nature of the processed data.
7. Data disclosing health and sex life shall be kept separate from any other personal data that is processed for purposes for which they are not required. Said data shall be processed in accordance with the provisions laid down in paragraph 6 also if they are contained in lists, registers or data banks that are kept without the help of electronic means.
8. Data disclosing health may not be disseminated.
9. As for the sensitive and judicial data that are necessary pursuant to paragraph 3, public bodies shall be authorized to carry out exclusively such processing operations as are indispensable to achieve the purposes for which the processing is authorized, also if the data are collected in connection with discharging supervisory, control or inspection tasks.

2.2.1.6.6 Processing of Anonymous Sensitive Data

Italian law provides a Code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the National Statistical system.

Private entities included in the National Statistical System pursuant to Act no. 125 of 28.04.1998 shall collect and further process sensitive data for statistical purposes in anonymous format, as a rule, subject to the provisions laid down in Section 6-bis(1) of legislative decree no. 322 of 06.09.1989 as inserted by legislative decree no. 281 of 30.07.1999 including subsequent amendments and additions.

Under certain circumstances, if lawful, specific statistical purposes related to the processing of sensitive data cannot be achieved without identifying data subjects, even on a temporary basis, the following prerequisites shall have to be met for said processing to be lawful:

- the data subject must have given his/her own consent freely on the basis of the information provided;
- the data controller must take specific measures in order to keep identification data separate already at the time of data collection, unless this proves unreasonable or requires a clearly disproportionate effort;
- prior authorisation of the processing by the Garante is necessary, also on the basis of an authorisation applying to categories of data and/or types of processing; alternatively, the processing must be included in the national statistics programme.

Consent shall be given in writing. If the sensitive data are collected by specific methods such as telephone and/or computer-assisted interviews, which make it especially burdensome for the survey to obtain written consent, consent may be documented in writing on condition that is has been given expressly. In the latter case, the records giving proof of the information provided to the data subject as well as of the latter's consent shall be kept by the data controller for three years.

2.2.1.7 Data Transfer

As regards to DAPHNE the following rules described in this section apply.

The data controller may freely transfer personal data among the EU Member States. Such transfer can only be prohibited when it is made for the purposes of avoiding the measures that would be applied pursuant to the Privacy Code.

1. Personal data that is the subject of processing may be transferred from the State's territory to countries outside the European Union, temporarily or not and in any form and by any means whatsoever under the following conditions specified in section 43:

    - if the data subject has given his/her consent either expressly or, where the transfer concerns sensitive data, in writing;
    - if the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject;
    - if the transfer is necessary, pursuant to the relevant codes of conduct referred to in AnnexA) of the Privacy Code, exclusively for scientific or statistical purposes, or else exclusively for historical purposes, in connection with private archives that have been declared to be of considerable historical interest under Section 6(2) of legislative decree no. 490 of 29October 1999, enacted to adopt the consolidated statute on cultural and environmental heritage, or else in connection with other private archives pursuant to the provisions made in said codes.

2. The transfer of processed personal data to a non-EU Member State shall also be permitted if it is authorised by the Garante on the basis of adequate safeguards for data subjects' rights:

    - as determined via the decisions referred to in Articles 25(6) and 26(4) of Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, through which the European Commission may find that a non EU Member State affords an adequate level of protection, or else that certain contractual clauses afford sufficient safeguards.

Apart from the above exceptions defined in points 1. And 2. Above, it is prohibited to transfer personal data that is the subject of processing from the State's territory to countries outside the European Union, temporarily or not and in any form and by any means whatsoever, if the laws of the country of destination or transit of the data do not ensure an adequate level of protection of individuals.

Account shall also be taken of the methods used for the transfer and the envisaged processing operations, the relevant purposes, nature of the data and security measures.

2.2.1.8 Security

According to section 31, 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 minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorised access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B to the Privacy Code:

- computerised authentication;
- implementation of authentication credentials management procedures;
- use of an authorisation system;
- 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 electronic means;
- protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software;
- implementation of procedures for safekeeping backup copies and restoring data and system availability;
- keeping an up to date security policy document (exceptions to this duty are provided for by the Privacy Code);
- 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.

Processing personal data without electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B to the Privacy Code:

- regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of the processing and/or by the individual organisational departments;
- implementing procedures such as to ensure safekeeping of records and documents committed to the entities in charge of the processing for the latter to discharge the relevant tasks; or
- implementing procedures to keep certain records in restricted access filing systems and regulating access mechanisms with a view to enabling identification of the entities in charge of the processing.

2.2.1.9 Breach Notification

Legislative Decree No. 69/2012 amended the Privacy Code provisions in relation to breach notification by introducing (i) the definition of "personal data breach" (meaning "*a breach of security leading to the accidental destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service*" – Section 4, par. 3, let. g-*bis*) and (ii) new obligations in case of personal data breach.

In particular, in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the Garante. When the personal data breach is likely to adversely affect the personal data or privacy of a contracting party or other individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification shall not be required if the provider has demonstrated that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. The notification to the contracting party or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach.

The notification to the Garante shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach (Section 32-bis of the Privacy Code).

2.2.1.10 Enforcement

The Garante is authorised to investigate complaints and to impose sanctions. The Garante may also appoint experts, proceed with inspections, require to produce documents and to be granted access. In case of criminal actions, the Garante notifies the public prosecutor.

The Privacy Code provides for the following administrative sanctions:

- providing no or inadequate information to data subjects shall be punished by a fine consisting in payment of between six thousand and thirty six thousand Euro (Section 161 of the Privacy Code);
- processing personal data without the relevant data subject consent (if required) shall be punished by a fine consisting in payment of between ten thousand and one hundred and twenty thousand Euro (Section 162 of the Privacy Code);
- processing personal data without submitting the notification to the Privacy Commissioner (if required) shall be punished by a fine consisting in payment of between twenty thousand and one hundred and twenty thousand Euro (Section 163 of the Privacy Code).

2.2.1.11 Data subjects' rights

Title II of the Privacy code defines the following rights, which may be exercised by making a request (by registered letter, facsimile or e-mail) to the data controller or processor without formalities, also by the agency of a person in charge of the processing:

- the rights of access (which includes the right to be informed of the source of personal data, of the obligatory or voluntary nature of providing the requested data and the consequences if (s)he fails to reply, of the purposes and methods of the processing, of the logic applied to the processing, if the latter is carried out with the help of electronic means, of the identification data concerning data controller, data processors or their representative, of the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data…); the personal data requested will be provided by the data controller either verbally, on paper or magnetic media or else transmitted via electronic networks,
- the right of updating, rectification or, where interested therein, integration of the data,
- the right of erasure, anonymisation or blocking of data that have been processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed,
- the right to object, in whole or in part, on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection or where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of

market or commercial communication surveys.

It is important to note that, according to Section 84, "personal data disclosing health may be communicated by health care professionals and health care bodies either to the data subject or" their legal representative "only by the agency of a physician who must have been designated either by the data subject or by the data controller". Furthermore, "the data controller or processor may authorise, in writing, healthcare professionals other than physicians who, to fulfil their respective duties, have direct contacts with patients and are in charge of processing personal data disclosing health, to communicate said data either to data subjects" or their legal representative.

2.2.1.12 Termination of Processing Operations

This is regulated in Section 16 which establishes that when data processing is terminated (for whatever reasons) the data shall be:

- Destroyed;
- Assigned to another data controller, provided they are intended for processing under terms that are compatible with the purposes for which the data have been collected;
- Kept for exclusively personal purposes, without being intended for systematic communication or dissemination;
- Kept or assigned to another controller for historical, scientific or statistical purposes, in compliance with laws, regulations, Community legislation and the codes of conduct and professional practice.

A special note here, that in terms of DAPHNE, once data processing has terminated and personal sensitive data is no longer needed the regulation permits this data to be anonymised for historical, scientific or statistical purposes **without consent from the data subject**. Otherwise the subject must be explicitly informed of the dual purposes of the collection of his data by DAPHNE for personal health monitoring and also anonymised bulk data statistics (as per section 2.2.1.6.6).

2.2.1.13 Processing of Data in the Healthcare Sector

As covered in Title V, health professionals and public health care bodies may process personal data disclosing health, also within the framework of activities in the substantial public interest with the data subject's consent, also without being authorised by the Garante, if the processing concerns data and operations that are indispensable to safeguard the data subject's bodily integrity and health.

General practitioners and paediatricians shall inform data subjects of the processing of personal data in a clear manner. The information may be provided as regards the overall personal data processing operations that are required for prevention, diagnosis, treatment and rehabilitation as carried out by a general practitioner or a paediatrician to safeguard the data subject's health or bodily integrity, such activities being performed at the data subject's request or else being known to the data subject in that they are carried out in his/her interest.

The information provided shall highlight, in detail, processing operations concerning personal data that may entail specific risks for the data subject's rights and fundamental freedoms and dignity, in particular if the processing is carried out:

- For scientific purposes, including scientific research and controlled clinical drug testing, in compliance with laws and regulations, by especially pointing out that the consent, if necessary, is given freely,
- Within the framework of tele-aid or tele-medicine services,
- To supply other goods or services to the data subject via electronic communication networks.

2.2.1.14 Clinical Records

Where public and private health care bodies draw up and retain clinical records in compliance with the applicable legislation, suitable precautions shall be taken to ensure that the data are understandable as well as to keep the data concerning a patient separate from those concerning other data subjects — including the information related to unborn children.
Any request to inspect or obtain a copy of the clinical records and the attached patient discharge form as lodged by entities other than the data subject may only be granted, in whole or in part, if it is justified because of the proven need to:

- establish or defend a legal claim in pursuance of Section 26(4), letter c), such claim being equal in rank to the data subject's right or else consisting in a personal right or another fundamental, inviolable right or freedom,
- establish a legally relevant claim in pursuance of the legislation concerning access to administrative records, such claim being equal in rank to the data subject's right or else consisting in a personal right or another fundamental, inviolable right or freedom.

Patient rights to access their medical files in Italy is not clear as patient rights in Italy are regulated by the Code on Medical Ethics, which is not legally binding. On the other hand however it is described in section 2.2.1.11 that a patient is able to have their personal health data communicated to them by an authorised health care professional or body.

In the case of DAPHNE the users / patients will have access to their PHRs stored in DAPHNE DaaS, access to PHRs and will control authorised access to the PHRs from public and private care bodies for clinical and non-clinical applications.

Patient access to the EHRs and MDRs used by public and private care bodies will be subject to the rules applied by the clinic that is treating the patient.

2.2.1.15 Online Privacy

The Privacy Code as amended by Legislative Decree No. 69/2012 regulates the collection and processing of traffic data and location data by the provider of a public communications network or publicly available electronic communications service and the use of cookies.

According to Section 123 of the Privacy Code, traffic data shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication. However traffic data can be retained for a period not longer than 6 months for billing and interconnection payments purposes or, with the prior consent of the contracting party or user (which may be withdrawn at any time), for marketing electronic communications services or for the provision of value added services.
According to Section 126 of the Privacy Code, location data may only be processed if made anonymous or if the subscriber or user has been properly informed and (s)he has given her/ his prior consent (which can be withdrawn at any time).

According to Section 122 of the Privacy Code (which reflects recital 66 of the E-Cookies Directive 2009/136/EC and the amended Section 5, par. 3 of the Directive 2002/58/EC – as amended by Directive 2009/136/EC) the storing of information in the contracting party's or user's computer is only allowed if said contracting party or user has been properly informed and (s)he has given her/his consent.

The Privacy Code states that the Garante may determine certain simplified modalities to provide contracting parties or users with the information notice and to identify the most efficient and practical ways to implement the new obligations on cookies. For this purpose, the Garante has recently launched a consultation with which it has also provided some FAQs that shed some light on the Garante's general view on cookies. The Garante confirmed its current trend to subject the cookies regulations to opt-in requirements, with limited exceptions, including analytics, authentication, flash players, "shopping baskets". To better assess the

cookies issue under Italian Law, we therefore need to wait for the Garante's guidelines on cookies after the public consultation.

2.2.1.16 Cloud Computing Guidelines

The selection and appointment of the cloud service provider as a Data Processor means the client will need to obtain information on the reliability and business reputation of the provider, its experience in the sector, professional and technical skills, the quality and levels of services it provides, and procedures and policies that will be adopted to protect the integrity and confidentiality of the data processed and stored *via* the cloud services. The Data Controller is still, however, in principle liable for violations if it is found to have a lack of control or be negligent in entrusting its data processing to third parties and in supervising the Data Processor's activities.

The guidelines also warn that some services offered by the cloud provider are actually subcontracted from other service providers, which could pose significant issues as to availability and access to the data. Accessibility is key to being able to provide personal data to data subjects on demand. In this case, the Data Controller must obtain in advance detailed information on each participant company involved at each level (particularly in relation to storage and transfer of the data), in order to make a thorough and considered decision.

The guidelines recommend that adequate insurance coverage for damages is granted by the cloud service provider and indicated expressly in the service agreement. Alternative dispute resolution clauses and penalties should also be outlined clearly.

2.2.1.16.1 Check the Reliability of the Cloud Service Provider

Users should establish how experienced, skilled and reliable their provider is before moving their most valuable data to the cloud; they should take account of their business or institutional requirements, type and amount of the information to be allocated to the cloud, risks and security measures in place.
Depending on, among others, the type of service to be provided and the importance of the data, users should assess the provider's corporate structure; the provider's references; the legal safeguards afforded to ensure data confidentiality along with the measures in place to prevent service breakdowns following unexpected failures. Additionally, users should assess the quality of the connectivity services the provider relies upon in terms of their capacity and reliability. Users might also want to consider whether the provider employs skilled staff, how adequate the provider's IT and communications infrastructure is, and to what extent the provider accepts to be liable for damages – which should be set forth explicitly in the terms of service – in case of security breaches and/or service breakdowns.

The reliability concerns as identified here shall be analysed for DAPHNE DaaS service including if the service is run on a private cloud.

2.2.1.16.2 Data Portability Preference

Clients should prefer cloud computing services that rely on open formats and standards to facilitate migration between cloud systems managed by different providers. Data portability means you can withdraw from the service without incurring costs and inconveniences that are difficult to gauge in advance. Additionally, this will reduce the risk that a provider may change the terms of the cloud service contract unilaterally to the client's detriment by taking advantage of his stronger negotiating power.

The Data portability requirement should be included in all DAPHNE DaaS private and public scenarios.

2.2.1.16.3 Data Availability

Clients should request that their contract with the cloud provider includes clear-cut, adequate safeguards on availability and performance of cloud services. Choosing a service that does not afford adequate

confidentiality and continuity safeguards may impact substantially not only on the cloud client, but also on the data subjects – think of public administrative bodies or any company delivering services to third parties. This is why the data controller – who is usually the cloud client – will have to make sure that he can keep a copy of any data allocated to the cloud apart from any underlying cost-containment objective; this is especially appropriate if the loss and/or unavailability of such data might prove seriously harmful not only to the controller's finances and/or image: think of highly sensitive information such as health care or judicial data, or any data on taxation and personal income.

This details key data availability requirements for the DAPHNE DaaS Service. Data Controllers must have backup plans in case of system failures and the same applies to cloud service providers which must keep a backup (e.g. by redundant database or mirrored server). This is important to satisfy the legal requirement of making data available to data subjects and any request (which may include rectification or even deletion of data stored), must be fulfilled within a certain timeframe, not importing if the system is down.

2.2.1.16.4 Select which Data should be Moved to the Cloud

Some items of information require – by their very nature – specific security measures to be in place: this is the case of information protected by industrial secrecy rules as well as of sensitive data such as information relating to health, ethnic origin, political opinions or membership of trade unions. Since moving data to the cloud reduces, in all cases, the user's direct control over such data, which is exposed to the (at times hardly foreseeable) risk of being lost or accessed unlawfully, users should evaluate responsibly whether to rely on cloud computing services (particularly public cloud services) or have recourse to other types of outsourcing or even continue processing that data "in house".

This especially relates to DAPHNE DaaS to consider how to protect sensitive data in the cloud with other recommendations providing specific safeguards such as pseudonymisation, encryption and separation of identity management from sensitive data.

2.2.1.16.5 Transparency

Users should always carefully consider the type of service being offered and check whether the cloud provider that is party to the contract will be holding the data factually or else that provider is actually a broker of services or relies on technologies made available by a third party. This might occur, for instance, with a cloud-based application where the provider of the data processing service ultimately relies on a storage service purchased from a third party: this will entail that the client's data will he hosted factually in the physical systems owned by the third party in question. Thus, to gauge the quality of cloud-based services one should establish who does exactly what out of all the entities involved in providing those services.

It is an important requirement for DAPHNE DaaS that it is clear where the data is stored/processed and that the responsibilities of data processor(s) and sub-processor(s) are equally clearly defined in contractual terms. Ideally sub-processors should be avoided due to the sensitive nature of the data.

2.2.1.16.6 Data Location

It is important for users to know whether their data will be moved to and processed by servers in Italy, the EU, or a non-EU country. This information may be essential to determine jurisdiction and applicable law in case of disputes between users and service providers; above all, it is fundamental to check the protection afforded to the data. Transferring data to countries where no adequate safeguards are in place in terms of security and confidentiality might make the processing of personal data unlawful and cause irreparable damage to the institutional activities of a public body as well as to a company's business. Before uploading data to the cloud and allowing data transfers to non-EU countries, users should check that this transfer takes place in accordance with the safeguards laid down in Italy's and EU's legislation on personal data protection.

For instance, if the cloud provider is a US-based company, one should check that it is a member of the Safe Harbor scheme – which includes rules agreed upon with EU institutions to enable the processing of personal data. It is also helpful to check that any non-EU cloud service provider has subjected its security and data processing procedures to specific certification schemes such as those regulated by ISO security standards. Additionally, one should check whether the outsourcing contracts submitted by the provider include the "standard contractual clauses" approved specifically by the European Commission to transfer personal data to third countries.

For the DAPHNE DaaS trial it is not envisaged that data will be processed or stored outside the EU for EU citizens. Therefore it is not needed to consider data transfer to 3rd countries from the PHS or CSP perspective. Also as for the CSP it has already been recommended in section 2.1.2.2.2 point 7 that under analysis of the Article 29 Opinion that due to the sensitive data being handled the controller should assure that data for EU citizens is processed and stored by the CSP (and any subcontractors) within the EEA[15].

That said however, the Italian data protection legislation does provide for exceptions for data to be transferred to 3rd countries as per the DPD, including sensitive data (see section 2.2.1.7). For example, as long as the 3rd country is compliant with EU data protection laws and provides the same level of protection as the EU (as determined by the European Commission) or the patient has given written explicit consent.

2.2.1.16.7 Terms of Service and Liability

It is important to assess whether the terms of service laid down in the cloud contract are appropriate; this is true, in particular, for the obligations and liability applying to loss and/or unauthorised disclosure of the data kept on the cloud as well as for the mechanisms to withdraw from the service and shift to a different provider. Special emphasis should be put on the specification of clear-cut quality standards along with the respective penalties, so that the provider is made liable for non-performance as well as for the consequences of specific events such as unauthorised access, data loss, unavailability due to malfunctioning, etc. To be on the safe side, check whether sub-contractors are involved in delivering cloud-based services and/or processing the data.

The terms of service and liability conditions will be analysed for DAPHNE DaaS service including if the service is run on a private cloud.

2.2.1.16.8 Data Retention

Before relying on cloud-based services, one should probe into the provider's policies regarding data retention on the cloud and make sure that they are laid down contractually. If the law does not provide for the erasure of the controller's data immediately the cloud contract expires, one should establish the deadline for the provider (= the data processor) to erase any data that was committed to him. The provider must ensure that no data will be kept beyond such deadline or in breach of what was explicitly set out with the client. At all events, all data must be kept in compliance with the purposes and arrangements agreed upon.

DAPHNE DaaS is guided by the retention principle which requires personal data to be kept for no longer than is necessary for the purpose for which the data were collected or further processed. The Italian legislation provides for data retention periods for national statistics but this does not affect DAPHNE as Bulk Data for possible use by national statistics will be anonymised data and not personal.

2.2.1.16.9 Security Measures

In order to protect data confidentiality, one should also consider the security measures put in place by the cloud service provider. Generally speaking, preference should be given to providers that rely on secure data storage and transmission mechanisms as based on encryption – especially if highly sensitive information is to be processed – along with robust mechanisms to identify access-enabled entities.

[15] It should be noted that the data protection laws of the data Controller´s home jurisdiction would apply to the data processed and stored by the cloud service provider wherever it is being processed or stored.

Data confidentiality will be analysed for DAPHNE DaaS service including the use of encryption and authentication and authorisation access measures.

2.2.1.16.10 Trained Staff

Both the client's and the provider's staff should be trained appropriately if they are tasked with processing data via cloud computing services so as to reduce the risks of unauthorised access, data loss and – more generally – unlawful processing operations. Training should include the technical information to enable the knowledgeable selection of cloud technologies along with the practical steps of the processing such as uploading data to the cloud and processing such data. Data protection may be jeopardized not only if staff behave unfairly or fraudulently, but also if they make trivial mistakes or work sloppily or negligently.

Staff training will be analysed for DAPHNE DaaS service as well as logging of all staff operations and authorisation levels.

The DAPHNE Data Controller is ultimately required to check and ensure that adequate technical and organisational measures are in place to minimise the risk that data may be destroyed, lost or accessed by third parties.

2.2.2 Israel

Data protection and privacy principles are provided for in Israeli law, through the following Israel regulations:

- Section 7 in the Basic Law: Human Dignity and Liberty
- Israeli Data Protection law (1981)
- Patient's rights law (1996)

In general, the Israeli law and Ministry of Health procedures are in accordance with international procedures of ethical approvals and comply with European Directives.

The European Commission Decision (2011/61/EU) [17] has also ruled that the State of Israel provides adequate protection of personal data with regard to automated processing of personal data. Therefore for the purposes of Article 25(2) of the DPD, the State of Israel is considered as providing an adequate level of protection for personal data transferred from the European Union in relation to automated international transfers of personal data from the European Union or, where they are not automated, they are subject to further automated processing in the State of Israel.

The Opinion WP114 of Article 29 further clarifies that in the case of sending of personal sensitive data from the EU to third countries (such as Israel) under Article 26(1) of the DPD then the derogations of processing sensitive data as per Article 8 of the DPD are still needed (e.g. explicit consent is to be freely given from the data subject).

Some further clarifications on privacy and running a DAPHNE trial in Israel are included below.

1. When there is a request for research data, an application submitted to the Ethical Committee, which approve to get the relevant data under research question, go through the process of anonymity. These data are used only for research, and does request a signature on a consent form. The access to this data is limited to the authorized personnel, for example: GP has access for clinical data except Gynecology and psychiatry Gynecology and psychiatry has access to all data, and Social workers have partial information access.

A patient can "opt out" – no one will see his data- this option is currently used rarely.

Personal health data will not be transferred to any 3rd party.

Authorization to access health data to health care professionals is part of the routine work. If a patient opt out, the data will be saved and stored but will be marked in the system and no one can see it.

During a clinical trial the patient will sign a consent form and will permit the data obtained during the trial and additional data that is defined and approved by ethical committee. For the use of the specific research\trial

2. In case of clinical trial- A clinical trial involving human subjects shall not be conducted unless the Investigator has received informed consent from the clinical trial participant it shall be given in writing, on the informed consent form approved by the Ethics Committee for the specific trial. The informed consent form shall be signed by both the participant and the Investigator. In the consent form there is an explanation to the patient that the information in the patient file, including medical records, will be reviewed only by authorized individuals (e.g. the Ethics Committee, the audit panel of the hospital, the Ministry of Health, representatives of the company responsible for the trial and trial monitoring), while maintaining absolute confidence, and that the patient's identity shall not be disclosed to non-authorized individuals either verbally or in scientific / medical publications.

Clinical trial application

According to the Israeli Ministry of Health procedures, handling new applications for special clinical trial by the medical institution is done as follows:

- The Principal Investigator submits the scientific studies/ clinical trial application to the institutional Ethics Committee. The Ethics Committee review the scientific studies/ clinical trial application and decides whether to approve or reject the application. The Ethics Committee also decides, whether the director of the medical institution is authorized to approve the scientific studies, or whether additional approval by the Ministry of Health is required.
- The Ethics Committee shall forward to the director of the medical institution its decisions regarding applications for scientific studies which it has approved and which the Director is authorized to approve without additional approval by the Ministry of Health. The Director shall issue an approval for the scientific studies to the Principal Investigator, detailing the terms and conditions). The Investigator may initiate the scientific studies only after receipt of said approval.

2.3 Communications from the Commission to the European Parliament

2.3.1 eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century - COM(2012)736

This communication is dedicated to promoting use of modern Information and Communication Technologies (ICT) for health and healthcare systems to increase their efficiency, improve quality of life and unlock innovation in health markets.

The European Commission has been developing targeted policy initiatives aimed at fostering widespread adoption of eHealth throughout the EU since the first eHealth Action Plan3 was adopted in 2004.

Since then, major large scale pilot projects such as epSOS [9] have been succesfully implemented and the adoption in 2011 of the Directive on the Application of Patients' Rights in Cross Border Healthcare [4] and its Article 14 establishing the eHealth Network, set another milestione on eHealth, with the aim to maximise social and economic benefits through interoperability and the implementation of eHealth systems.

However, the communication identifies many barriers that continue to exist and prevent the deployment of eHealth systems in Europe, amongst which it identifies: "lack of legal clarity for health and wellbeing mobile applications and the lack of transparency regarding the utilisation of data collected by such applications".

Effective data protection is vital for building trust in eHealth. It is also a key driver for its successful cross-border deployment, in which harmonisation of rules concerning cross border exchange of health data is essential.

Very applicable to DAPHNE, the report stresses the empowerment of citizens and patients in eHealth and wellbeing applications requires greater transparency and effective data protection safeguards which would subsequently enable "the integration of user-generated data with official medical data so that care can be more integrated, personalised and useful for Patients".

Subsequent to this communication the EDPS issued its Opinion [6] concerning the matters raised on its data protection content and the relevant conclusions to DAPHNE are included below with important points underlined:

- Data protection requirements should be appropriately considered by industry, Member States and the Commission when implementing initiatives within the eHealth area. In particular:
    - that personal data processed in the context of eHealth and well-being ICT often relate to health data, which require a higher level of data protection and underlines the guidance already given to controllers and processors in the area;

- notes that the Communication does not refer to the current data protection legal framework set forth under Directive 95/46/EC and Directive 2002/58/EC, which contains the relevant data protection principles that are currently applicable and reminds the Commission that these rules are to be respected for any action to be taken in the short to medium term until the proposed revised Data Protection Regulation (see section 2.4) enters into force;

- notes that the importance of the data subject's rights of access and information in the context of eHealth has not been made clear in the Communication. He therefore encourages the Commission to draw the attention of controllers active in the field of eHealth on the necessity to provide clear information to individuals about the processing of their personal data in eHealth applications;

- notes that the Communication does not underline that any data mining using non-anonymous health data is only acceptable under very limited circumstances and provided that full account is taken of data protection rules and encourages the Commission to draw the attention of controllers to this fact;

- underlines that profiling should only be done in very limited circumstances and provided that strict data protection requirements must be met (e.g. as set forth in Article 20 of the proposed Data Protection Regulation) and encourages the Commission to remind controllers of this important obligation.

- urges the Commission, when examining the interoperability of health records, to look into possible legislative initiatives at EU level, as he believes that such interoperability would benefit from a strong legal basis, which would include specific data protection safeguards.

2.4 Future Data Protection Regulation Implications

On 25 January 2012, the European Commission unveiled a draft European General Data Protection Regulation (GPDR) that will supersede the Data Protection Directive.

A major goal of the commission is to harmonise data protection within the EU under a single law, the **GDPR**. The current EU Data Protection Directive 95/46/EC does not consider important aspects like globalization and technological developments like social networks and cloud computing sufficiently and therefore the commission determined that new guidelines for data protection and privacy were required.

A revised "Compromise Text" of the GPDR was approved by the European Parliament on October 21, 2013. The next stage is for Council of Ministers to agree on it and final considerations between the Parliament, Council and Commision will lead up to a vote on the GPDR expected before the parliamentary elections in May 2014.

To conclude, the adoption of the GPDR is aimed for in 2014 and the regulation is planned to take effect in 2016 after a transition period of 2 years.

Therefore in terms of DAPHNE the project must follow the national legislations pursuant to the DPD. As and when the GDPR is passed by Parliament in its final form, it is for the project to analyse if this will impact on DAPHNE i.e. on whether the new regulation is required to be included in DAPHNE.

An initial examination of applicable impacts of the GDPR is included in the following sections so to give an indication of the data protection and privacy principles that are proposed to be changed.

2.4.1 Single Set of Rules

The GDPR will create one single set of rules that applies to all EU member states.

However there may be provision for exceptions in the area of employment data and health that could still be subject to individual country regulations, and therefore DAPHNE may still have to refer to national legislation for guidance on processing of health data.

2.4.2 Responsibility & Accountability

The notice requirements remain and are expanded so that they must include the retention time for personal data and contact information for data controller and data protection officer has to be provided.

Privacy by Design and by Default require that data protection is designed into the development of business processes for products and services privacy settings are set at a high level by default.

Data Protection Impact Assessments have to be conducted when specific risks occur to the rights and freedoms of data subjects.

Data Protection Officers are to ensure compliance within organizations. They have to be appointed for all public authorities and for companies processing more than 5000 data subjects within 12 months.

2.4.3 Consent

Valid consent must be explicit for data collected and purposes data used.

Consent for children under 13 must be given by child’s parent or custodian, and should be verifiable.

Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn.

2.4.4 Data breaches

The data controller has to notify the DPA without undue delay and, where feasible, not later than 72 hours after having become aware of the data breach.

Individuals have to be notified if adverse impact is determined.

2.4.5 Right to be Forgotten

Personal data has to be deleted when the individual withdraws consent or the data is no longer necessary and there is no legitimate reason for an organization to keep it.

2.4.6 Data Portability

A user shall be able to request a copy of personal data being processed in a format usable by this person and be able to transmit it electronically to another processing system.

2.4.7 Pseudonymous data

This is defined as “personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution”.

Where the controller is unable to comply with the Draft Regulation because it is processing pseudonymous data, the controller is not obliged to comply with that particular provision of the Draft Regulation.

3 Classification of DAPHNE Data

3.1 Anonymous Bulk Data for Research Purposes

As seen from the above analysis of the EU data protection framework personal health data collected in DAPHNE may be made available for bulk data research purposes when anonymised pursuant to specific safeguards in national legislation including strict rules on its profiling.

For a concise definition of anonymous data please refer to section 2.1.1.2.

3.2 Private Data for Personal Health Services

The terms Electronic Health Record (EHR) and Electronic Medical Record (EMR) are often used interchangeably although differences between them can be defined. For example, an EMR can be defined as the patient record created in hospitals and which can serve as a data source for the EHR.

An EHR is generated and maintained within an institution, such as a hospital, clinic, or physician´s office to give patients, physicians and other health care providers access to a patient's medical records across facilities. In the main it is updated by the health provider but patients may also be able to input data.

A Personal Health Record (PHR) is similar to an EHR except that the individual patient usually owns and controls it. If a patient has access to their EHR they are able to copy this data into their own PHR, in which case they would now own and control this data, and be able to give to other practioners or 3rd parties as they see fit.

As the DAPHNE data model is yet to be defined it is unclear exactly how the user/patient data will be managed in DAPHNE and this may be through EHRs and/or PHRs or some other method. However for the purposes of capturing and classifying the relevant health data for DAPHNE it is assumed that this data will be captured in EHRs and/or PHRs.

Also it is not clear if medical device data should be part of the EHR/PHR or whether it would be kept separate in a new Medical Device Record (MDR), or indeed if it is needed to be stored at all. For now it is assumed to be kept separate in an MDR, and this too will be clarified later in the project.

- **Personal Data Record**
  - Data subject name
  - National Health Card Number
  - Address
  - Administrative Data
    -
  - Etc.
- **Electronic Health Record / Personal Health Record**
  - Doctor notes data module
    - …
  - Obesity data module
    - …
  - Dietary data module
    - …

  - Wellbeing data module
    - …
  - Patient input data module
    - …
  - 3rd party data module (data received from 3rd party sources)
    - …
  - Genetic data module
    - …
  - Medication data module
    - …
  - Etc.
- **Medical Device Record**
  - Clinical Medical Device Data (for medical PHS applications)
    - Heart rate module
    - Blood pressure level module
    - Glucose level module
    - Cholesterol level module
    - etc
  - Non-clinical Medical Device Data (for "wellbeing" applications)
    - Weight measurement module
    - Pedometer activity module
    - etc
  - etc

4 Privacy Level Agreement (PLA)

A PLA, as outlined by the Cloud Security Alliance (CSA), will be used to disclose the privacy and data protection that the cloud service provider (CSP) will maintain [11] for the DAPHNE Service. This will address the recommendations and guidance provided throughout 2012 by Article 29 Working party and several European data Protection Authorities.

"All cloud service providers (CSPs) offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the clients should be key drivers behind the offer of cloud computing services." Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing [12]. Further it is indicated in the same reference that CSP information should be made available so that a proper risk assessment exercise can be carried out: "a precondition for relying on cloud computing arrangements is for the controller [cloud client] to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective".

Additionally in accordance with [12] the PLA provides a tool for structured disclosure of the CSPs privacy and data protection practices. In summary the PLA enables the CSP to describe in detail their cloud service security information in a standard way and is structured as follows:

1. Identity of the CSP (and of Representative in the EU, as applicable), its role, and the contact information for the data protection officer and information security officer
2. Categories of personal data that the customer is prohibited from sending to or processing in the cloud
3. Ways in which the data will be processed
    a. Personal data location
    b. Subcontractors
    c. Installation of software on cloud customer's system
4. Data transfer
5. Data security measures
   Describe the concrete technical, physical, and organizational measures to ensure:
    - Availability
    - Integrity
    - Confidentiality
    - Transparency:
    - Isolation (purpose limitation)
    - Intervenability
    - Portability
    - Accountability

   As part of this exercise the security control framework employed by the CSP is specified e.g. ISO/IEC 27002. For DAPHNE it is recommended to employ the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) [13] as this is specifically designed to provide fundamental security principles to guide cloud providers, and also to assist cloud customers in assessing the overall security risk of a cloud provider. It is also based upon the aforementioned ISO/IEC control framework as well as industry standard security regulations and common practices.
6. Monitoring
7. Third-party audits
8. Personal data breach notification
9. Data portability, migration, and transfer-back assistance
10. Data retention, restitution, and deletion
    a. Data retention policy
    b. Data deletion
    c. Data retention for compliance with legal requirements
11. Accountability
12. Cooperation
13. Law enforcement access

14. Remedies
15. Complaint and dispute resolution
16. CSP insurance policy

For greater detail refer to the actual CSA PLA [11].

5 Conclusions

This deliverable D2.2 has produced a rotund analysis of the directives and regulations that pertain to data protection and privacy in the EU arena, in relation to the handling of personal health data in a DAPHNE DaaS service.

As such the key principles and rules that impact on DAPHNE have been highlighted and will serve as input to establishing requirements on the DAPHNE DaaS service.

It has been noted that the service scenarios are yet to be established, however some example scenarios have been included to demonstrate the variation in Data Controller and Processor models that can occur.

Also the data model is yet to be established, however from the understanding at this stage the deliverable identifies the need for Electronic Health Records as well as Personal Health Records and possibly Medical Device Records as described in the classification of data DAPHNE in section 3. In the same section the use of anonymous data is confirmed for bulk data research use with safeguards provided by national legislation.

A final note to make clear for the next phase of the project is that in order to fully clarify the application of the rules and regulation in terms of requirements for DAPHNE it is needed to:

- confirm the scenarios for the trial so to properly identify the data controllers;
- consult medical group partners on their actual data protection, privacy and ethical policies, which could apply further restrictions (where allowed by national legislation).

References

[1] http://www.DAPHNE-fp7.eu

[2] European Convention on Human Rights, http://www.echr.coe.int/Documents/Convention_ENG.pdf

[3] Data Protection Directive 95/46/EC,

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[4] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=EN&numdoc=32011L0024

[5] COM(2012) 736 - eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century,

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0736:EN:NOT

[6] Opinion of the EDPS on COM(2012) 736,
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-03-27_eHealth_Action_EN.pdf

[7] General Data Protection Regulation,

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

[8] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, included in "Data protection. Compilation of Council of Europe texts", Directorate General of Human Rights and Legal Affairs Strasbourg. 2010 November, pp.15-27.

[9] epSOS, http://www.epsos.eu/

[10] Charter of fundamental rights of the European Union,

http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[11] Cloud Security Alliance PLA Outline for the Sale of Cloud Services in the European Union, https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf

[12] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[13] CSA CCM https://cloudsecurityalliance.org/research/ccm/

[14] CSC Final Report, http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

[15] Italy National Legislation, http://www.garanteprivacy.it/

[16] Article 29 WP 169, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/

[17] Commission Decision on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (2011/61/EU),

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:en:PDF

[18] Article 29 WP114,

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:en:PDF