Grant agreement no. 211714

neuGRID

A GRID-BASED e-INFRASTRUCTURE FOR DATA ARCHIVING/ COMMUNICATION AND COMPUTATIONALLY INTENSIVE APPLICATIONS IN THE MEDICAL SCIENCES

Combination of Collaborative Project and Coordination and Support Action

Objective INFRA-2007-1.2.2 - Deployment of e-Infrastructures for scientific communities

Deliverable reference number and title: D2.1 Review document on data protection (legal and procedural issues)

Due date of deliverable: month 6

Actual submission date: 30th July 2008

Start date of project: February 1st 2008 Duration: 36 months

Organisation name of lead contractor for this deliverable: PROVINCIA LOMBARDO-VENETA - ORDINE OSPEDALIERO DI SAN GIOVANNI DI DIO FATEBENEFRATELLI

Revision: Version 1

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	PU
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of contents

Executive summary 3
1 Introduction 3
2 Methodological approach 5
3 Activity carried out and results 6
3.1 The respect of privacy as a human right 6
3.2 Directive 95/46/EC: an overview.....8
3.3 Data Protection Directive and biomedical research.....18
3.4 Implementation of the Data Protection Directive 95/46/EC in the European Union member states.....22
3.4.1 Austria.....22
3.4.2 Belgium.....25
3.4.3 Bulgaria.....27
3.4.4 Cyprus.....28
4.4.5 Czech Republic.....30
3.4.6 Denmark.....31
3.4.7 Estonia.....33
3.4.8 Finland.....35
3.4.9 France.....37
3.4.10 Germany.....40
3.4.11 Greece..... 42
3.4.12 Hungary.....44
3.4.13 Ireland.....45
3.4.14 Italy.....47
3.4.15 Latvia.....49
3.4.16 Lithuania.....50
3.4.17 Luxembourg.....52
3.4.18 Malta.....53
3.4.19 the Netherlands.....55
3.4.20 Norway.....57
3.4.21 Poland.....59
3.4.22 Portugal.....61
3.4.23 Romania.....63
3.4.24 Slovakia.....65
3.4.25 Slovenia.....66
3.4.26 Spain.....68
3.4.27 Sweden.....69
3.4.28 United Kingdom.....72
3.5 European projects using health infrastructure and health grid.....75
3.5.1 SHARE.....76
3.5.2 ACGT..... 78
3.5.3 ARTEMIS.....79
3.5.4 @neurIST.....80
3.5.5 HEALTH-E-CHILD.....81
3.5.6 LHP.....82
4 Conclusion 83
Bibliography.....84
APPENDIX A: table 87

EXECUTIVE SUMMARY

The present deliverable aims to review privacy and data protection issues in Europe, with regard to medical research and particularly to research using health infrastructures and healthgrids.
In the first part we analyzed the *Directive 95/46/EC* and its implementation in the Member States. In the second part we performed a search within recent European projects dealing with infrastructures and grids in the health field in order to survey data protection policies. The deliverable will be the basis for the development of the data protection protocol and procedures to be used within the neuGRID project.

1. INTRODUCTION

The present deliverable deals with privacy and data protection issues in the context of medical research, and particularly of research using health infrastructures and healthgrids and will be the basis for the development of the data protection protocol and procedures to be used within the neuGRID project. The importance of the matter is based on the acknowledgment of privacy as a fundamental human right, as stated by all major international treaties and agreements on human rights.

The protection of privacy of personal medical data is important in any use of such data, but it becomes even more important in the context of research. In fact, while the right to the privacy can be overcome in the best interest of the person concerned – i.e. for better diagnosis and treatment – incomplete privacy protection for research purposes is questionable, such that in the research field it is necessary to enforce all the possible means to guarantee personal data protection.

In context of health Grids, the protection of privacy deserves specific regard for the technical specificity of the tool. In fact, the distributed nature of Grids and the many players involved in Grid computing could make the control of sensitive information presents specific issues. For these reasons, as early as the planning phase of the project, the consortium decided to develop a specific and unified protocol for privacy and data protection to manage personal data in a way mindful of the needs of both science and the individual's rights. To this avail, a review of the European and Member States regulations as well as of previous results of European projects on data protection had to be performed. The present deliverable is the result of the review performed in the first six months of the neuGRID project.

Assuming that privacy of own health information is a basic human right, we analyzed the *Directive 95/46/EC of the European Parliament and of the Council of 24.10.95 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* that sets a milestone in the European history of the protection of personal data. After an overview of the full Directive aiming to provide a general framework for the discussion, we focused on the aspects of the Directive related to the core of our interest, i.e. medical research.

Although all Member States have now adopted the Directive, the Communication from the Commission to the European Parliament and the Council (Brussels, 7.3.2007), highlights that some Member States have sometimes failed to incorporate a number of important Directive provisions and at other times translation to practice has not been compliant with the Directive or has fallen outside the bounds of manoeuvre that Member States are allowed. Furthermore, the Directive includes a number of broadly formulated provisions that, either explicitly or implicitly, leave Member States considerable latitude in its adoption into national legislation. Thus, seeing as differences across national legislations may arise, we have analyzed the implementation of the Directive in each Member State in order to spot analogies and differences in the implementation.

In the analysis of both the aspects of the Directive related to medical research and the national data protection legislations, we gave special regard to the following issues: definition of personal data as opposed to anonymization; special exemptions from/to the data protection provisions for medical research; the notion of consent and its relation with the other conditions that may remove the prohibition to process personal data (sensitive and no sensitive data); the content and extent of the duty to inform subject about the processing of his/her personal data; the national provisions concerning the obligation of notification and prior checking; the provisions regarding the transferring of personal data to foreign countries outside the European Union and the European Economic Area. Finally, we performed a search within recent European projects dealing with infrastructures and grids in the health field in order to survey data protection policies.

2. METHODOLOGICAL APPROACH

For the first part of the work, consisting in the analysis of the *Directive 95/46/EC* and of the implementation of the Directive in the Members States, we accessed in particular the website of the European Commission http://ec.europa.eu/justice_home/fsj/privacy and the websites of the National Data Protection Commissioners http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm that report the national legislations. National legislations have been accessed in the official English version or in the non-official English version in case official English translation was not available.

In particular for the studying of the aspects of the Directive and of its implementation related to medical research, the results and recommendations of the European project PRIVIREAL – Privacy in Research Ethics and Law (http://www.privireal.org) have been taken into consideration. The two PRIVIREAL publications D. Beyleveld, D. Townend, S. Rouillé-Mirza, J. Wright (ed.) "The data Protection Directive and Medical Research Across Europe" (2005) and D. Beyleveld, D. Townend, S. Rouillé-Mirza, J. Wright (ed.) "Implementation of the Data Protection Directive in Relation to Medical Research in Europe" (2004) have been carefully considered.

For the part of the deliverable related to European projects using infrastructures and grids in the health field, we performed a search in the CORDIS Information and Communication Technologies website http://cordis.europa.eu/fp7/ict/projects/home_en.html . We searched projects funded in FP7, FP6 and FP5 using several enter search terms such as health grid, heath infrastructure, biomedical grid, biomedical infrastructure, grid imaging and brain imaging, and then we accessed the ad hoc projects website.

3. ACTIVITY CARRIED OUT AND RESULTS

3.1 THE RESPECT OF PRIVACY AS A HUMAN RIGHT

Privacy is recognized as a fundamental human right in all major international treaties and agreements on human rights. Nearly every Country in the world recognizes privacy as a fundamental human right in their constitution, either explicitly or implicitly.
The **Universal Declaration of Human Rights** *(Paris, 1948) states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". (Article 12).*
At European level, the **European Convention for the Protection of Human Rights and Fundamental Freedoms** *(Rome, 1950) at Article 8 – Right to respect for private and family life affirms that "1.Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*
Similarly, the **Charter of Fundamental Rights of the European Union** *(2000/C 364/01) states the respect for private and family life (Article 7) and the protection of personal data (Article 8): "Everyone has the right to respect for his or her private and family life, home and communications"; "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.3. Compliance with these rules shall be subject to control by an independent authority".*

With specific regard to the field of health, the ***Convention for the Protection of Human Rights And Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*** (*Oviedo, 1997*) affirms the right to the protection on Private life at Chapter III – Private life and right to information, Article 10 – Private life and right to information: " 1.Everyone has the right to respect for private life in relation to information about his or her health; 2. Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed; 3. In

exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient".

The additional protocol to the Convention on Human Rights and Biomedicine, concerning biomedical research *(Strasbourg, 2005) deals with the issue of privacy at CHAPTER VIII on Confidentiality and right to information. Article 25 on Confidentiality states that "1. Any information of a personal nature collected during biomedical research shall be considered as confidential and treated according to the rules relating to the protection of private life".*

At Article 26 – Right to information "1. Research participants shall be entitled to know any information collected on their health in conformity with the provisions of Article 10 of the Convention; and 2. Other personal information collected for a research project will be accessible to them in conformity with the law on the protection of individuals with regard to processing of personal data".

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is in Europe the specific legal tool aimed to give common rules to member states on privacy issue.

3.2 DIRECTIVE 95/46/EC: AN OVERVIEW

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Data Protection Directive) was adopted as a legislative provision in October 1995.
The Data Protection Directive aims to establish an equivalent level of protection of personal data in all Member States in order to facilitate the transfer of personal data across national boundaries within the European Union.
Article 1.2 states that "*Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection* …[of personal data]" .
This implies that the correct implementation of the principles stated in the Directive should ensure an adequate protection of rights and freedoms of individuals.
Therefore Data protection Directive has two main purposes: a) to allow the free flow of data within Europe in order to prevent the Member States from blocking inter European Union data transferring on data protection grounds, and b) to reach a harmonized minimum level of data protection throughout Europe.

Definitions
Article 2 of the Directive sets out important definitions.
Firstly according to Article 2: *'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*

The Directive does not clarify the meaning of the expression "natural person", therefore it is necessary referring to national legislation. Indeed, in certain EU Member States the data of legal person are also covered by the data protection law.
Another open question is whether the data protection principles apply to deceased persons.

According to Article 2(b): " *'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;*
The Data Protection Directive applies to personal data processed wholly or partly by automatic means and to manual data held in filing system structured by reference to

individuals, but it does not apply to activities outside the scope of European Union Law. Areas within Titles V and VI of the Treaty on European Union such as public safety, defence, State security are excluded.

Moreover, according Article 2(d): *'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;*

The data controller must process personal data in compliance with the principles on data protection stated in the Directive and he/she is responsible for the breaching of data subject's rights.

Directive sets out the conditions under which the processing of personal data is lawful, the rights of the data subject and the standards of data quality.

Principles relating to data quality

Article 6 establishes fundamental principles that have to be respected when personal data are processed: "...*personal data 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*."

Criteria for making data processing legitimate

Article 7 sets out a number of conditions that must be satisfied before data can be processed. Data processing must be undertaken only with the data subject's consent except when: *"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).

Sensitive data

The Data Protection Directive created a category of data called "sensitive personal data". The processing of sensitive data - that is data revealing racial or ethnic origin, political opinions, philosophical or religious beliefs, trade-union membership, as well as data concerning health and sex life – is in principle forbidden. A controller who processes sensitive data can only do so if he/she meets one of a set of conditions. Some of these conditions are laid down in Article 8 of the Directive. Moreover, Member States are permitted to create their own conditions that allow the processing of sensitive data where adequate safeguards are established.

According to Article 8.2 of the Directive the prohibition to process sensitive data does not apply where: " *(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 referred to in paragraph 1 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".
Directive does not introduce an order of priority with respect of the conditions that may legitimate the processing of sensitive data, thus it is not clear if consent must be preferred to the other conditions.

In the case M.S. v. Sweden, 28 EHRR 313 [1997], the European Court of Human Rights stated that the processing of sensitive data without the data subject's consent constitutes a violation of privacy according to Article 8.1 of the European Conventions on Human Rights (ECHR). A derogation from this rule is allowed only if it is so provided by the law and under certain circumstances. According to Article 8.2 of the ECHR
The aforementioned decision is not binding for the European Union, however, the European Court of Justice, the jurisdictional body of the European Union, assigns great value to the former judge's decisions.
If to the consent is given the priority, the controller will have to obtain the data subject's consent and only where consent is impossible or impracticable he/she may refer to another condition legitimate the processing.

Moreover, according to Article 8.3 the prohibition to process sensitive data does not apply 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*".

Finally, Articles 8.4 states that: "*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*".

Information to be given to the data subject

The data subject has the right to be informed either in the case that the data are collected from the data subject him/herself or from a third party. Articles 10 and 11 of the Directive are formulated as duties for data controller rather than rights of the data subject. This seems to imply that information must be provided without an explicit request from the data subject.

In particular, Article 10 of the Directive states that: "*the controller or his representative 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 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*".

When the data are not obtained from the data subject, Articles 11 states 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 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;(c) any further information such as - the categories of data concerned, - the recipients or categories of recipients, - the existence of the right of access to and the right to rectify the data concerning him, in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.*
2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards".

The aforementioned provisions are strictly connected with Article 6 of the Directive in order to ensure a fair and lawful processing of personal data and they have a central role in the Directive since they allow the data subject to give an informed consent.

Data subject's right of access of data and to object

Article 12 sets out the data subject's right to obtain from the controller information about the processing of his/her data.
According to Article 13.1 g) this right can be restricted for the protection of the data subject or of the rights and freedoms of others. The restriction of the right to access needs the adoption of a legislative measure.

According to Article 14.a the data subject, at least in the cases referred to in Article 7 e) and f), can object at any time on compelling legitimate grounds to the processing of data relating to him/her, unless otherwise provided by national legislation. If the objection is justified the processing can no longer involve those data.
Article 14.b grants the right to object to the processing for the purposes of direct marketing.
While in the former case the data subject's right may be removed by the national legislator, in the latter may not and the data subject must be informed of this right.

Exemptions and restrictions

Article 13 permits Member States to restrict the scope of obligations and rights provided for in Articles 6, 10, 11, 12 and 21 (publicizing..) by means of a legislative measure when it is necessary to: " *a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;*
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others.

Moreover according to Article 12.2: "*Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.*"

Confidentiality and security of processing

According to Articles 16 and 17 data security must ensure that personal data are protected against accidental and unlawful destruction or accidental lost. Data must also be protected against unauthorized alteration, disclosure or access and all other forms of unlawful processing. The level of security must be appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of technology and cost.

Notification – Prior checking – Publicizing of processing operations
Article 18 requires the data controller to notify the Supervisory Authority before carrying out any automatic or partly automatic processing.
Article 18(2) and (3) allows Member States to provide for exemptions or simplifications from the duty of notification if some conditions are met:
" - *where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or*

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular: - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.
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".
Article 19 specifies the content of notification that, among other things, must contain information about the identity of the data controller, the purposes of the processing, data subjects, categories of data processed and recipients of the data.

According to Article 20 Member States must determine which processing operations are likely to present specific risks to the rights and freedoms of data subject in order to provide for a prior checking of them by the Supervisory Authority or a Data Protection Official.

Article 21 requires Member States to take measure to publicize all processing operations. If the processing needs to be notify according to Article 18, a register must be kept by the Supervisory Authority containing all the information laid down in Article 19(1).
Even though notification is not necessary, Member States must guarantee that this same information is available on request.

Judicial remedies, liability and sanctions

Articles 22, 23 and 24 require Member States to provide for: a judicial remedy for any breach of the rights guaranteed to the data subject by the national law of implementation; compensation from controller for damages suffered as a result of an unlawful processing operation; suitable measures to ensure full implementation of the provisions of the Directive which must include sanctions for infringing these provisions.

Transfer of personal data to third countries

The Data protection Directive sets out the conditions under which personal data can be transferred to countries outside the European Economic Area. In general, a transfer can only take place if the third country ensures an adequate level of protection for the rights and freedoms of data subject. Indeed, Article 25 of the Directive states that: " *1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without*

prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision".

However, Article 26 of the Directive sets out some exemptions to the general principle: "*By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:*
(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from 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 who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.
If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).
Member States shall take the necessary measures to comply with the Commission's decision.
4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision".

Codes of conduct

Article 27 requires Member States and the Commission to encourage the adoption of codes of conduct to assist with the implementation of the Directive in specific sectors of processing.

Supervisory Authority
Each Member State is required to set up a Supervisory Authority to oversee the application of data protection provisions. The powers and responsibilities of the Supervisory Authority are specified in Article 28 (3):

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing

the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts."

According to Article 28 (4): "*Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.*
Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place."

According to Article 28 (5) the national Supervisory Authority must draw up a regular report on its activities, which must be made public.
The Supervisory Authority may be asked to exercise its powers by the Authority of another Member State and must cooperate with the Supervisory Authorities in other Member States.
Finally, according to Article 28 (7) the staff of the Supervisory Authority must be subject to a duty of professional secrecy with regard to confidential information. This obligation must continue after the cessation of the employment.

Working Party

Article 29 sets up an advisory, independent Working Party on the Protection of Individuals with respect to the Processing of Personal Data and specifies the composition and functioning of the Working Party.
Moreover, Article 30 clarifies the role of the Working Party:
(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level".

According to Article 29.2 the Working Party must inform the Commission of any lack of harmonization in the implementation of the Directive that may affect the equivalence of protection. Moreover, the Working Party may make recommendations, forwarded to the Commission and Article 31 committee, on the protection of persons in the processing of personal data in the Community. The Commission must inform with a report the Working Party of actions taken in response to its recommendations. The report must be public and also be forwarded to the Parliament and the Council.
Finally, according to Article 29.5 the Working party every year must draw up a public report to the European Parliament and the Council on the level of protection in Member States and third countries.

Committee

Article 31 provides that the Commission is to be assisted by a committee composed of representatives of Member States when it proposes to take Community measures. If the committee agrees, by the majority laid down in Article 148 (2) of the Treaty, to the proposed measures, they apply immediately. Otherwise, the measures must be submitted to the Council.

Final Provisions

Article 31 requires Member States to have implemented the Directive within three years of its adoption, hence by 24 October 1998. Moreover by 24 October 2001, all processing already underway by 24 October 1998 must comply with the provisions of the Directive. Member States may delay conformity with Articles 6, 7 and 8 until 24 October 2007 in case of processing of data already held in manual filing system on 24 October 1998.
According Article 33 the Commission has to report to the Council and European Parliament on implementation of the Directive at regular intervals.

3.3 DATA PROTECTION DIRECTIVE AND BIOMEDICAL RESEARCH

Directive 95/46/EC does not contain explicit reference to medical research. However, certain useful elements may be found in several provisions of the Directive.
As seen above, the Directive states two kind of provisions that have been interpreted as provisions that to some extent could be applied to medical research even in absence of a specific appeal: - Article 8 of the Directive concerning the processing sensitive data in which data concerning health are included; - provisions regarding the processing of data for scientific research purposes.
In particular, the present paragraph will be focused on: - the conditions that can legitimate the processing of sensitive data according to Article 8 of the Directive that involves or could involve medical research, that is consent of the data subject, preventive medicine and substantial public interest, and the possible hierarchy between these conditions; - the duty of information and the possible exemption from this obligation where the further processing of data is for the purpose of scientific research; - other exemptions from the data processing principles where data are processed for scientific purposes

Before analyzing the aforementioned provisions, the notions of personal data and anonymization will be taken into consideration.

Personal data and anonymization

Since data protection principles apply only to personal data, it is crucial to determine when data can be considered personal, thus falling under the scope of the Directive.
As seen above, Article 1 of the Directive defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Directive as well as the majority of national legislations does not contain express reference to the subject that can make the identification.
While for direct identification it is generally meant that this can be performed by anyone, it is more difficult to ascertain who can make an indirect identification. The implications to consider that anyone can indirectly identify the data subject are significant. In fact, in this perspective, also coded or pseudonymized data have to be considered as personal data because the person who holds the key to the coded data is able to make the identification.
Anyway, it is difficult to know what direct or indirect identification means in the Directive context and when a data can be considered not personal.

According to Recital 26: "*to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible*".
Recital 26 seems to introduce a limit on the means needed to identify a person. The identification has to be considered possible using "reasonable means".

The national laws differ in the implementation of the definition of personal data. While certain States have used the same or similar wording to the Directive without reference to the reasonable means of Recital 26), other States, even giving the same interpretation of the Directive of who can identify the data subject, have introduced a limit (cap) on indirect identification as outlined by recital 26). Finally, some States have used different wording to the Directive giving their own interpretation of Article 2a and Recital 26).

As far as anonymization is concerned, the only reference to it in the Directive is contained in the aforementioned Recital 26) and in Article 6 where it states that data must be 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.
Also in the majority of the implementation laws there is no definition of anonymization.

An open question is whether the processing of making the data anonymous (anonymization) can be considered as a processing according to Article 2b of the Directive.
There is no a common interpretation neither among scholars nor in the national legislations.

Medical Research and Article 8 of the Directive

Consent
According to Article 8.2 of the Directive, the prohibition to process sensitive data may be removed with the data subject's explicit consent.
Article 2 h) of the Directive states that: '*the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*
Directive 95/46/EC does not contain any reference to the form of the "explicit consent", thus, it is necessary to refer to requirements provided by the national legislators in the implementation laws.

Indubitably, the data concerning health may be used for the purposes of medical research if the data subject's consent to the processing has been obtained, unless a Member State provides that the prohibition to process sensitive may not be lifted by the data subject's consent.

Preventive medicine and medical diagnosis

As seen above, Article 8.3 of the Directive permits the processing of sensitive data where the 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.

The medical research is not explicitly included in this provision, however it is controversial whether medical research can be considered as a subcategory of "preventive medicine and medical diagnosis" so covered by the exemption of Article 8.3.

Moreover, it is disputable whether in the hypothesis of Article 8.3 the data subject's consent is not requested even if it is not impossible or impracticable to obtain.

Substantial public interest

Article 8.4 permits to derogate from the prohibition on processing sensitive data for reasons of substantial public interest where suitable safeguards are provided for by the national legislation.

Recital 34) of the Directive identifies public health and scientific research as areas that can justify the exemption on important public interest grounds.

The derogations based on substantial public interest must be provided for by a national law or by a decision of the Supervisory Authority and must be communicated to the European Commission.

Duty of information and exemption for scientific research

As pointed out before, Articles 10 and 11 of the Directive play a key role in stipulating the information that must be given to the data subject.

Since information constitutes an essential requirement to the release of a valid consent, the importance of these provisions is manifest.

While Article 10 takes in consideration the case where the data are collected directly from the data subject, Article 11 sets out the event of collection of the data from a source other than the data subject. The content of the information is the same but it is different the moment in which the controller is subject to the duty to inform. In the first case information must be given at the time of the collection of the data, in the second case, instead, the information will be subsequent: at the time of recording or disclosure of the data.

Article 11.2 provides for a derogation from the duty to inform the data subject where the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. Moreover, Articles 11.2 points out that this provision applies in particular for processing of statistical purposes or for the purposes of historical and scientific research.
This implies that, when data are not collected from the data subject and the processing is for the purpose of scientific research the duty to inform the data subject is removed if impossible or involving a disproportionate effort.
According to the Directive the implementation of this exemption from the informative obligation must be balanced by the provision of appropriate safeguards.

Exemption for scientific research

According to Article 6, the further processing of data for historical, statistical or scientific purposes is not considered incompatible with the purpose of the collection on condition that States provide adequate safeguards. Moreover, Article 6 (e) states that is possible to store personal data for longer periods for historical, statistical or scientific purposes but even in this case adequate safeguards must be provided.

According to Article 13, when data are processed only for purposes of scientific research, and there is clearly no risk of breaching the privacy of the data, Member subject States may restrict by a legislative measure the rights provided by Article 12 of the Directive (data subject's right of access to data). Also in this case the exemption must be balanced with adequate legal safeguards.

In conclusion, Directive lays down some exemptions from the principles of data protection when the data are processed for the purpose of scientific research but the derogation must always be counterbalanced by the provision of adequate safeguards.

In the following paragraph, the implementation, State by State, of the Directive 95/46/EC into the national systems will be analyzed.

3.4 IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE 95/46/EC IN THE EUROPEAN UNION MEMBER STATES

In the present paragraph the implementation, State by State, of the Directive 95/46/EC into the national systems will be analyzed.
As known, while the European Union Regulations are directly applicable in the Member States, Directives require an *ad hoc* national law of implementation to produce their effects. Therefore, Directive, giving a certain degree of autonomy to national legislators, is an instrument of harmonization rather than unification. This implies that normally the different national laws of implementation are not perfectly homogeneous. Moreover, the national law often deviate from the provisions stated in the Directive itself and it is not always clear if the State has simply exercised its discretionary power or even violated the principles of the Directive.

The analysis of the national data protection legislations will be focused on:
- the definition of personal data as opposite to anonymization;
- whether exists special exemptions from/to the data protection provisions for medical research;
- the notion of consent and its relation with the other conditions that may remove the prohibition to process personal data (sensitive and no sensitive data);
- the content and extent of the duty to inform the data subject about the processing of his/her personal data;
- the national provisions concerning the obligation of notification and prior checking;
- the provisions regarding the transfer of personal data to foreign countries outside the European Union and the European Economic Area.

3.4.1 AUSTRIA

In order to implement Directive 95/46/EC the Austrian legislator enacted the Datenschutzgesetz 2000 (DGS). The DGS is a federal Act that provides for both constitutional and ordinary law provisions.
When the processing of data is automated the competence to regulate the processing is federal, therefore the DGS applies. On the contrary, if the processing of data is manual (non-automated) the competence to legislate is of the single states.
It is not completely clear the borderline between federal and state competence; moreover not every state has provided for an adequate system of data protection. Currently there are seven Acts on data protection that apply where federal jurisdiction lacks. As far as medical

sector is concerned, the applicability of state law is contained since manual processing of medical files in hospitals is of minor importance today.
The English version of the Datenschutzgesetz 2000 is available at:
http://www.dsk.gv.at/dsg2000e.htm

1. Personal Data and Anonymization

The DGS does not provide for an explicit definition of personal data and anonymous data. Therefore, in accordance with the Directive a data may be considered personal where it is possible to identify, directly or indirectly, the person which the data refers to. Whereas it is not possible to determine the link between the data and the data subject, the data may be considered anonymous.
However, DGS introduces the notion of data that are "only indirectly personal" for a controller, a processor or recipient of a transmission when the data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Section 9, 11 of the DGS permits the processing of sensitive data for preventive medicine and medical diagnosis purposes but medical research is not included in this exemption to the general prohibition of processing sensitive data.

2.2 substantial public interest

According to Section 9, 3 of the DGS the derogation from the prohibition to process sensitive data on substantial public interest grounds requires a specific law provision.

2.3 other exemptions

A further exemption from the prohibition to process personal data is laid down in Section 9, 10 of the DGS as far as the processing is carried out for research or statistical purposes in compliance with Section 46 of the DGS.
It is necessary to operate a distinction between two situations: 1) researches where the goal is to obtain data there are not in a form relating to a specific data subject; and 2) researches where the goal is to obtain data that are in a form relating to a specific data subject or where there is not a specific goal. In the former case, the use of data is allowed if the data are publicly accessible, the controller has lawfully collected the data for another research project or the data are only indirectly personal for the controller. In the second case the stricter regulation of Section 26 paragraph 2 applies: the use of data is only legitimate pursuant to specific legal provisions with the consent of the data subject or with an authorization from the Data Protection Commission (DPC). The authorization must be granted if consent of the data subject is impossible or unreasonable to obtain, there is public interest -

important public interest if research involves sensitive data - and the professional qualities of the applicant have been demonstrated.
The data must be coded immediately if the goal can be pursued with indirectly personal data and, unless expressly provide otherwise by law, the data must be rendered anonymous as soon as the personal link is no longer needed.
According to Section 46 paragraph 1 Z2 if the research is carried out on medical records it is presumed that the data were legitimately collected for another purpose.

3. Consent

Section 9 of the DGS prohibits in principle the processing of sensitive data. The use of this kind of data is permitted only where one of the thirteen conditions set out in the same Section 9 is met. In the medical sector are particularly significant the following conditions: - the data subject has obviously made public his/her data; - the data are used only in indirectly personal form; - the obligation or authorization to use the data is stipulated by laws, insofar as these serve an important public interest; - the data subject has unambiguously given his consent; - the processing or transmission is in the vital interest of the data subject and his consent cannot be obtained in time or the use is in the vital interest of a third party; - data are used for scientific research or statistics pursuant to sect. 46.
The DGS does not state the same provision of Article 8.2c of the Directive that requires the data subject is physically or legally incapable of giving his/her consent, but permits the use of data also when obtaining consent is time consuming.
The consent is one of the conditions that can legitimate the processing of personal data but has not priority with respect to the other conditions. Consent can be revoked at any time and revocation makes any further use of data illegal.

4. Duty of Information

The data subject has the right to receive information to the controller, or his/her representative, about the processing of his/her personal data.
According to Section 26 of the DGS, the duty to inform covers all data, the origin, the purposes, the recipient and the legal justification for the processing.
Section 26 also provides for the procedure that the data subject has to follow in order to obtain information for the controller. The data subject may satisfy his/her right by reference to the Data Protection Commission.

5. Notification and Prior Checking

Substantially all automated data processing requires the notification to the DPC. Section 17 paragraphs 2 and 3 lays down some exceptions of little relevance in the medical sector.
The only exception may be the derogation of standard application. The federal Chancellor defines standard applications by ordinance: it consists of applications or transmission that are

carried out by a large number of controllers in a similar fashion, while the risk for the interests deserving protection must be unlikely due to purpose and kind of data used.
However, applications that contain health data cannot be considered standard application.
In some case the obligation to notify is simplified: the single physician has no the same duty of notification to the DIC than the hospital.
According to Section 20 of the DGS, if the processing refers to sensitive data and there is no exemption to notification, before starting the processing the authorization from the DIP is required.

6. Transfer of Personal Data to Third Countries

The transferring of personal data to third countries is permitted only if the country in question ensures an adequate level of protection. Countries that meet this requirement must be indicated in a Federal Chancellor's Ordinance.
The transferring is also admitted in cases listed by Section 12 paragraphs 2 and 3 that substantially copy Article 26 of the Directive.

3.4.2 BELGIUM

In Belgium the personal data protection regulation is provided for by Law 8 December 1992 as amended by Law 11 December 1998 enforced by the Royal Decree 13 February 2001 (RD) in order to implement the Directive 95/46/EC.
The unofficial English translation of the Belgian Data Protection Act (DPA) is available website at: http://www.law.kuleuven.ac.be/icri/itl/12privacylaw.php
The original version in French and in Dutch is available on the website of the Privacy Commission at: http://www.privacycommission.be

1. Personal Data and Anonymization

Article 1 Section 1 of the Belgian data protection law defines personal data in the same terms of Directive: information directly or indirectly relating to a natural person. In specular way, the data must be considered anonymous when nobody, neither the controller nor someone else, may identify the data subject.
If data are used for scientific research purposes they must be rendered anonymous; if it is not possible the data must be encoded. Finally, if also codification is not available, then personal data may be used.

2. Medical Research

2.1 implementation of Article 8.3 of the Directive

According to Article 7 §2, d) of the RD, the prohibition to process health data does not apply if processing is necessary for the promotion and protection of public health, including the screening of the population. In the report to the King preceding the RD it is stated the population screening in order to protect and promote public health has to be considered as scientific research. However, it is not clear if this provision can be considered as implementation of Article 8.3 (preventive medicine) or of Article 8.4 (substantial public interest) of the Directive.

2.2 other derogations (substantial public interest)

According to Article 7 §4, k) of the RD it is allowed to process sensitive data if it is necessary for scientific research and the processing is carried out under the conditions established by the King in a Decree. The decree constitutes a necessary condition for the processing since represents the suitable safeguard required by Article 8.4 of the Directive.

The Decree 13 February 2001 applies only to further use of health data for scientific research purposes but not to the primary processing of this kind of data. Therefore at present Article 7 §4 k may not be applied.

3. Consent

The processing of sensitive data concerning health requires the written consent of the data subject.

According to Article 20 of the RD, consent seems to have priority with respect to the other conditions that can legitimate the processing of sensitive data, therefore the controller must to seek the consent of the data subject unless it reveals impossible or impracticable to obtain.

4. Duty of Information

According to Article 9 of the RD the controller has a duty to inform the data subject both if the data are obtained directly from the data subject and if data are collected from another source.

The controller can be exempt from the obligation to inform only in the latter case if, in particular for statistical purposes or for the purposes of historical or scientific research, the provision of such information appears to be impossible or involves disproportionate effort.

5. Notification and Prior Checking

The RD provides for a general obligation to notify the Commission for the Protection of Privacy before carrying out any wholly or partially automatic processing of data.

This provision does not apply to the processing for the sole purpose of keeping a register that is intended by law to provide information to the public.

By Order of the King and previous communication to the Supervisory Authority it is possible to introduce an exemption to notification for some categories of data. According to Article 17 of the RD medical research is not covered by the exemption.

6. Transfer of Personal Data to Third Countries

Article 22 of the RD copies the Directive provision relating to the transferring of data to third countries. This Article has not been implemented by the King yet.

3.4.3 BULGARIA

The Directive 95/46/EC has been implemented in Bulgaria by the Data Protection Act of 21 December 2001 (DPA).
The English version of the Act integrated with the *amend. SG. 70/10 Aug 2004, amend. SG.93/19 Oct 2004, amend. SG. 43/20 May 2005, amend. SG. 103/23 Dec 2005, amend. SG. 30/11 Apr 2006, amend. SG. 91/10 Nov 2006, amend. SG. 57/13 July 2007* is available on the website at:

http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/bg_data_protection_law_en.pdf

1. Personal Data and Anonymization

Article 2 of the DPA defines personal data as any information able to disclose the physical, psychological, mental, familial, economic, cultural and social identity of a natural person.
In the Bulgarian system anonymization is not viewed as a process covered by the Data Protection regulation.

2. Medical Research

2.1 implementation of Article 8.3 of the Directive

According to Article 5 paragraph 2, 6) of the DPA it is allowed to process sensitive data if "the processing is needed for the purposes of the preventive medicine; the medical diagnostics, the providing and management of medical services, under the condition that the data is processed by a medical expert, obliged by a law to keep the professional secret or by another person, bound with a similar obligation to keep secret".

However, medical research is not included in this provision.

2.2 substantial public interest

The Bulgarian law on Data Protection does not take into consideration the exemption to the sensitive data processing general prohibition based on public interest.

3. Consent

According to Article 5 paragraph 2 of DPA the explicit consent of the data subject is one of the conditions that permits the sensitive data processing. In particular, consent must be given in a written form.

Consent has not priority with respect to the other requirements for the lawful processing of sensitive data set out in Article 5 paragraph 2, therefore it is possible to choose an alternative to consent even if obtaining it is not impossible or impracticable.

Other than the case of preventive medicine seen above (*supra* paragraph 2.1) and consent, processing of sensitive data is allowed when: the procession is needed for the purposes of the execution of specific rights and obligations of the administrator in the field of the labour legislation;- the procession is needed for the protection of live and health of the natural person whom the data refers to, or to another person and the status of the natural person does not allow to give consent or legal obstacles exist for this; - the procession is performed by a non-profit organization, including religious, philosophical, political or trade-union purpose, within its lawful activity and with appropriate protection; - the processing is related to data, publicly announced by the natural person or this is needed for the finding, exercising and the protection of rights under court procedure; - the processing is performed only for the purposes of journalistic, literature or artistic expression, as far as this procession does not violate the right of private live of the person whom the data refers to.

4.Duty of Information

According to Articles 20 and 21 of DPA, before the beginning of the processing, the controller, or his/her representative, must inform the data subject about: - the data which identifies the administrator and his/her representative; - the purpose and the resources for their processing; - the recipients or the categories of recipients to whom the data can be submitted and the sphere of their using; - the obligatory or voluntary nature of submission of the data and the consequences

from a refusal of submission; - the right to access and to correction of the gathered data.

This kind of information must be given where the data are collected from the person whom they refer to as well as in case of original collection from a person different from the data subject. In the latter hypothesis the controller is exempted from the duty of information when the processing is for statistical, historical or scientific purpose and the provision of such information is impossible or requires excessive efforts.

5.Notification and Prior Checking

The Bulgarian Data Protection Act does not require neither the obligation to notify the Supervisory Authority nor prior checking in relation to medical research.

6.Transfer of Personal Data to Third Countries

According to Article 36a of the DPA transferring personal data to a third country is admitted only if the said country provides an adequate level of protection. The Commission for Protection or the Personal Data (CPPD) has to assess the adequateness of protection taking into account the nature of the data, the purpose and duration of processing, legal regulation and safeguard measures adopted in the third countries. The CCPD must notify the European Commission and the Member States about the permissions granted as well as about the refusal to provide such permissions (Article 36b)

The DPA allows the transfer of data to a third country that does not ensure an adequate level of protection at the same conditions set out in article 26 of the Directive.

3.4.4 CYPRUS

Cyprus has enacted the Processing of Personal Data Law 2001 (PPDL), amended with the Law 37(I)/2003, in order to comply with Directive 95/46/EC.

The English version of the PPDL is available at:

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/138(I)-2001_en.pdf

1.Personal Data and Anonymization

According to Article 2 of the PPDL "personal data" means any information relating to a living data subject in contrast with "consolidated data of a statistical nature", from which the data subject cannot be identified, that are not deemed to be personal data.

There is no reference to the notion of anonymous data.

2. Medical Research

2.1 implementation of Article 8.3 of the Directive

According to Article 6(2)(f) of the PPD the prohibition to process sensitive data does not apply when the processing relates to medical data and is performed by a person providing health services by profession and has a duty of confidentiality or is subject to relevant codes of conduct, on condition that the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or the management of health-care services..

Medical research does not fall under the scope of this provision.

2.2 other exemptions

Article 6(2)(h) of the PPD states that he ban to process sensitive data is also removed if data are processed solely for statistical, research, scientific and historical purposes, on condition that all the necessary measures are taken for the protection of the data subjects.

3. Consent

According to Article 2 of the PPD consent means "*any freely given, express and specific indication of his wishes, clearly expressed and informed, by which the data subject, having been previously informed, consents to the processing of personal data concerning him*".

As far as sensitive data is concerned, an explicit written consent signed by the data subject is required by Article 6(2) of the PPD.

Consent is not the only condition that can remove the prohibition to processing sensitive data and has not priority over the alternatives to consent.

4. Duty of Information

The controller has an obligation to inform the data subject either when data are collected directly from the data subject or when they are obtained from another source at least about: the identity of the controller; the purpose of the processing; the recipients of the data; the right to access and rectify the data.

According to Article 11(3)(b) when the data are not obtained from the data subject, the duty to inform does not apply "*especially in cases where the processing is performed for statistical and historical purposes or for purposes of scientific research if it is impossible to inform the data subject or where disproportionate effort is necessary in order to inform him, or if the communication of data is provided by another law, provided that in each case a license is issued by the Commissioner*"

5. Notification and Prior Checking

According to Article 7(1) the controller has a duty to notify the Commissioner for Personal Data Protection in writing about the establishment and operation of a filing system or the commencement of processing.

The controller is exempted from the duty to notify where the processing is performed by doctors or other persons who provide health services and concerns medical data, provided that the controller is bound by medical confidentiality or other kind of confidentiality required by law or code of conduct and the data are neither transferred nor communicated to third parties.

6. Transfer of Personal Data to Third Countries

The transfer of data to third countries is regulated by Article 9 of the PPD that translates into the Cyprian legal system the provisions of Articles 25 and 26 of the Directive.

3.4.5 CZECH REPUBLIC

The Data Protection Act n. 101 of 2000 (DPA), amended by the Acts n. 227/2000, n. 177/2001, n. 450/2001 and n. 107/2002, implemented the Directive 95/46/EC.
The English version of the DPA is available on the website at:
http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/czech_republic_act_101_en.pdf

1.Personal Data and Anonymization
According to Article 4 paragraph A of the DPA personal data means any information relating to an identified or identifiable person. The identification may be made/happened directly or indirectly by reference to one or more factors. However, the data cannot be considered personal where an inadequate quantity of time, effort or resources is required to identify the data subject.

2. Medical Research
The DPA does not stipulate specific provisions, as well as exemptions to the data protection principles, relating to medical research.

3. Consent
The consent must specify the purpose for which it has been given and may be revoked at any time, unless there is a different agreement between the data subject and the controller.
As far as sensitive data is concerned, an explicit written consent signed by the data subject is required by the DPA.
According to DPA 2000 the consent is not the only condition that can remove the prohibition to processing personal data.
Articles 5-9 of the DPA substantially implement the exemptions set out in Articles 7 and 8 of the Directive.

4. Duty of Information
The controller has an obligation to inform the data subject either when data are collected directly from the data subject or when they are obtained from another source.
If the controller wishes to process the data for further purposes not foreseen at the time of collection, data subject's consent is required. Nevertheless, according to Article 11 paragraph 5 of the DPA the controller is not obliged to give information where: - the processing is exclusively for statistical, scientific, or archival purposes; - the processing of personal data is imposed by the law; - the processing involve exclusively published data; - the data subject gave his/her previous consent.

5. Notification and Prior Checking

The DPA provides a general obligation to notify the Supervisory Authority the beginning of data processing.
Article 18 of DPA lays down the exceptions to the aforementioned rule but medical research is not included in those exceptions.
There are also no special provisions concerning the prior checking of processing operation in medical research field.

6. Transfer of Personal Data to Third Countries
The transfer of data to countries that do not guarantee an adequate level of data protection is regulated by Article 27 of DPA that copies Article 26 of the Directive.

3.4.6 DENMARK

The Directive 95/46/EC has been implemented into the Danish system by the Act on Processing of Personal Data n. 429 of 2001 (APPD).
The English version of the APPD is available at: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/

1. Personal Data and Anonymization
Section 3.1 of the APPD defines personal data as any information relating to an identified or identifiable person. During the preparatory works the opportunity of interpreting the term "identifiable person" in compliance with Article 2 of the Directive has been pointed-out.
According to Danish law, in order to operate the identification, it does no matter if the information is commonly known or available just for few persons. Indeed, also coded or encrypted data is considered personal if someone has access to the code. Therefore, only processing of data rendered completely anonymous is not covered by the APPD.
As seen above, the interpretation of personal data acknowledged in the Danish system is very broad.
If making data anonymous has to be considered processing covered by the APPD provisions is an open question. According to an authoritative scholar as long as anonymization aims to exclude the data from the scope of the APPD, it would be too bureaucratic if the Act should apply in this situation.
On the contrary for other scholars it is better to consider anonymization as processing of data according to the APPD. [See M. HARTLEV, *The Implementation of Data Protection Directive 95/46/EC in Denmark*, in D. Beyleveld et al. (ed.) *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. 2004: 60-61]

2. Medical Research

2.1 implementation Article 8.3 of Directive

Section 7.5 of the APPD allows processing of sensitive data concerning health 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 law to the obligation of professional secrecy.
Even if biomedical research could be considered as "preventive medicine or medical diagnosis", processing of health data exclusively for research purpose in not covered by section 7.5.

2.2 substantial public interest

According to section 7.7 of the APPD processing of sensitive data is allowed on substantial public interest grounds. The Datatilsynet (Danish Supervisory Authority) may authorize a processing based on public interest if specific requirements are met.
Any exemption to the prohibition of processing sensitive data based on public interest must be communicated by the Datatilsynet to the European Commission.
It is not clear if medical research may be covered by this exemption.

2.3 other exemptions for research

Section 10.1 allows the processing of sensitive data where the processing takes place for the sole purpose of carrying out statistical or scientific studies of significant public importance and where such processing is necessary in order to carry out these studies.
The APPD does not clarify the meaning of "significant public importance" and who is qualified to decide over it.
The data covered by section 10.1 may only be disclosed to a third party with prior authorization from the supervisory authority. The supervisory authority may lay down specific conditions concerning the disclosure.

3. Consent

Section 3.8 of the APPD defines consent as any freely given, specific and informed indication of the data subject wish by which he/she signifies agreement to the processing of his/her personal data.
Consent must be explicit but not necessarily written: in fact also oral consent is considered explicit. However, in order to prove the existence of consent the written form may be preferable.
Consent is not the only condition that permits the processing of data (sensitive and no sensitive) and the APPD does not assign priority to consent: all conditions are treated as open alternatives.

4. Duty of Information

Sections 28 and 29 of the APPD implement Articles 10 and 11 of the Directive concerning the controller's obligation to inform the data subjects about the identity of the controller and of his representative, the purposes of the processing for which the data are intended and any

further information which is necessary, having regard to the specific circumstances in which the personal data are collected.
If the data is obtained directly from the data subject and at the time of collection there is an intention to use the data for research purposes, the data subject should be informed about it. On the contrary, if the need to use the data for research emerges after the collection, the data subject should be informed only where the new purpose is incompatible with the original one.
However, according to section 5 of the APPD, the further processing of data for research purposes is presumed to be compatible with the collection purpose.

5. Notification and Prior Checking

In Danish data protection system it exists a general obligation to notify the Datatilsynet of the processing of personal data and this duty is laid down in sections 43 and 48 of the APPD.
Even thought there are some exemptions to the notification duty, medical research is not exempted.
According to section 50 of the APPD when the processing operations present specific risks to the rights or freedoms of the data subject, like the processing of sensitive data, a previous authorization from the Datatilsynet is required.
However, if the medical research is carried out in the public sector instead of the aforementioned authorization the Datatilsynet has to provide an opinion before the beginning of the processing. It is not clear the nature, binding or not, of this opinion.

6. Transfer of Personal Data to Third Countries

The rule is that transfer of data to a third country may take place only if the third country in question ensures an adequate level of protection. Nevertheless, sections 27.3 and 27.4 of the APPD set out the exceptions to the rule.
While in section 27.3 are enumerated the same conditions as Article 26 of the Directive, according to section 27.4 the Datatilsynet may authorize a transfer of personal data to a third country which does not ensure an adequate level of protection where the controller adduces adequate safeguards with respect to the protection of the rights of the data subject. Specific conditions may be laid down for the transfer. The Datatilsynet shall inform the European Commission and the other Member States of the authorizations granted pursuant to this provision.

3.4.7 ESTONIA

In Estonia personal data protection is currently regulated by the law of the 1 October 2003 as amended in 2004.
The English version of the Estonian Personal Data Protection Act (PDPA) is available at:

http://www.legaltext.ee/text/en/X70030.htm

1. Personal Data and Anonymization

According to Article 4(1) of the PDPA personal data means any information relating to an identified or identifiable natural person. The information may refer to physical, mental, psychological, economic, cultural and social characteristics of the data subject.

Although according to the PDPA anonymization can be considered as a data processing, some scholars stated that for this kind of processing the data subject's consent should not be required. [See A. Nomper, *Personal Data Protection Regulation in Estonia and Directive 95/46/EC*, in D. Beyleveld et al. (ed.) *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. 2004: 78]

2. Medical Research

The PDPA does not lay down specific provisions regarding medical research. Neither Article 8.3 nor Article 8.4 of the Directive have been implemented, therefore there is no debate whether medical research may be considered to be part of "preventive medicine or medical diagnosis" or in the substantial public interest.

3. Consent

Consent is the main condition able to legitimate the processing of sensitive data. Indeed, according to Article 14 of the PDPA the processing of sensitive data without consent may occur only in two circumstances: - for performance of an obligation prescribed by law or international agreements; - for protection of the life, health or freedom of the data subject or other person.

Article 12(1) of the PDPA requires a "freely given, specific and informed" consent not necessarily in a written form.

4. Duty of Information

According to Article 15 of the PDPA the data subject must be informed about: - the purpose of processing of the personal data; - the categories and sources of the personal data; - persons or categories thereof to whom transmission of the personal data is permitted; - the name of the chief processor or a representative thereof and the address of the place of business of the chief processor;- the cases when the data subject has the right to demand termination of processing of the personal data and rectification, blocking or erasure of the personal data; - the cases when the data subject has the right to obtain access to the personal data pertaining to him or her.

These information must be supplied either when data are collected directly from the data subject or from a third person.

5. Notification and Prior Checking

According to Article 21 of the PDPA the controller must notify the Data Protection Inspectorate (DPI Estonian Supervisory Authority) the processing of personal data. The unique exception to the rule does not cover medical research.
Moreover, Article 24 lays down an obligation to register processing of sensitive data with the DPI that may refuse the registration if there is no legal basis for the processing or the conditions for processing do not comply with the requirements of the PDPA
The difference between notification and prior check is not very clear.

6. Transfer of Personal Data to Third Countries

In order to comply with the standards imposed by the Estonia's accession to the European Union, the PDPA permits the transfer of data to Member States, European Economic Area States, as well as to a State, the personal data protection level of which has been deemed adequate by the European Commission.
Transfer of personal data to countries that not ensure an adequate level of protection is normally forbidden, but according to Article 28(4) of the PDPA with the permission of the Data Protection is possible to overcome the prohibition if: in the specific case the chief processor guarantees the protection of the rights and private life of the data subject in the state; in the specific case of transmission of personal data, the sufficient level of data protection is ensured in the state.
Moreover according to Article 28(6), even without the permission of the DPI, personal data may be transmitted to a foreign state where the sufficient level of data protection is not ensured if the data subject has given his/her consent or if the data are transmitted to the foreign state in cryptographic form and the data necessary for decoding is not communicated to the foreign state.

3.4.8 FINLAND

In Finland the legislation on the protection of personal data is provided by the Law n. 471/1987 as amended in 1999 by the Law n. 523/1999, on the basis of Directive 95/46/EC.
The Finnish Personal Data Act (PDA) has to be integrated with other Acts dealing with medical research: Patient's Rights Act 795/1995, Act on Health Care Professionals 559/1994, Medical Research Act 488/1999 and Act on the Medical use of Tissues and Organs 101/2001.
The English version of the PDA is available at: http://www.tietosuoja.fi/uploads/hopxtvf.HTM

1. Personal Data and Anonymization

According to Section 3 of the PDA personal data means "any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household".

If the data are made anonymous the data protection principles do not apply and the data can be used for any purpose. However, if someone is able to make the identification, even though the user of the data could not do it, the data are not considered completely anonymous: therefore the processing of this kind of data should comply with PDA principles.
In practice, where the identification of the data subject requires unreasonable effort the data are considered *de facto* anonymous.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

According to Section 12(10) of the PDA the general prohibition to process sensitive data does not prevent "a health care unit or a health care professional from processing data collected in the course of their operations and relating to the state of health, illness or handicap of the data subject or the treatment or other measures directed at the data subject, or other data which are indispensable in the treatment of the data subject.
Even though, Finnish formulation of the exemption does not mach exactly the Directive provision, medical research does not seem to be covered by the derogation in question.

2.2 substantial public interest

The PDA does not provide for an exemption to the prohibition to process sensitive data on public interest grounds.
There is also no explanation of "substantial public interest" meaning.

2.3 derogation for scientific research via Article 13 of the Directive

Article 14 of the PDA sets out a derogation from the data processing requirements for scientific research. However, for the exemption to apply, strict conditions must be met. First of all, it must be necessary to use personal data in the research and it must be impossible to obtain the data subject's consent due to the large amount of data or to their old age. Secondly, the research must be based on a specific plan, the data must be used only for scientific purposes and then destroyed or rendered anonymous.

3. Consent

In the PDA there are no specific provisions regarding the characteristics of the consent, however, some information may be found in the Supervisory Authority guidelines. Indeed, according to the Supervisory Authority consent must be specific to certain data and to certain purposes of data processing.

4. Duty of Information

Section 24 of the PDA provides for the duty of information in the same terms of the Directive Articles 10 and 11, therefore, the controller should inform the data subject about the purposes of the processing, the recipients of the data, the identity of the controller of his/her representative and the existence of the right of access to the data concerning him/her.

According to paragraph (2) of Section 24 the controller is exempted from the aforementioned obligation: - if the data subject already has the relevant information; - if this is necessary for the protection of national security, defence or public order or security, for the prevention or investigation of crime; - where the data are collected from elsewhere than the data subject, if the provision of the information to the data subject is impossible or unreasonably difficult, or if it significantly damages or inconveniences the data subject or the purpose of the processing of the data and the data are not used when making decisions relating to the data subject, or if there are specific provisions in an Act on the collection, recording or disclosure of the data.

5. Notification and Prior Checking

According to Section 26 of the PDA when the processing of data is for scientific research purposes the notification to the Supervisory Authority is not required. However, the Supervisory Authority stated that the derogation does not apply if in the research are used sensitive data.
The PDA does not provide for a prior checking of data processing operations for medical research. The task to check the compliance of the research with the data protection principles is assigned to the Ethics Committees when they approve the research.

6. Transfer of Personal Data to Third Countries

According to Section 22a, issued with the amendment 986/2000 to the PDA, personal data shall not be transferred out of the territory of the member states of the European Union nor out of the European Economic Area in so far as the Commission has found, pursuant to Articles 3 and 25(4) of the Data Protection Directive, that the country in question does not guarantee an adequate level of data protection.
Section 23 of the PDA allows a derogation to the said rule at the some conditions provided for in Article 26 of the Directive.

3.4.9 FRANCE

France has implemented Directive 96/46/EC with/by the law n. 801/2004, however even before there was a regulation for privacy protection (law n. 17/1978).
The original version in French of the Law 801 is available at:
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676&dateTexte=

1. Personal Data and Anonymization

Law 801/2004, Article 2 paragraph 2, defines personal data as any information related to an individual identified or who can be identify directly or indirectly by reference to an identification number or to one or more factors and then introduces the criteria of

reasonableness and proportionality of the means used by the controller or anybody else in the identification.
The notions of "anonymous data" and "identifiable person" are not absolute; they depend more on the knowledge and ability of the recipient than on the data itself considered. Therefore, a data could be regarded as anonymous where the identification of the data subject involves an exceptional effort.
The *Commissione Nationale de l'Informatique et de Libertés* (CNIL, France Supervisory Authority), in accordance with the provisions of Article 2, had considered the quality of "identifier" to qualify some data as personal or not.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Article 8.II. 6 of the law 801/2004 sets out an exemption from the general prohibition to process sensitive data where the processing is necessary for the purposes of preventive medicine and medical diagnosis and the processing is carried out by a health professional or another person that by reason of his/her functions is subjected to the obligation of professional secrecy in accordance with Article 226-13 of French Penal Code. Medical Research is not covered by this provision.

2.2 substantial public interest

Law 801/2004 states a generic exemption from the prohibition to process sensitive data on substantial public interest grounds, but neither the notion of substantial public interest nor the possibility to include medical research in this derogation are specified.

2.3 derogation for scientific research in the health sector

Articles 8.II.8 of the law 801/2004 permits the processing of sensitive data when it is carried out for the purposes of scientific research in the health sector. The processing is subjected to an authorisation procedure according to Chapter IX of the law 801/2004 itself. Each request must be submitted to a "consultative committee on the processing of information for research in the health sector" established by the Minister for Research and composed by experts in the field of medical research (epidemiology, genetic, biostatistic).
Before submission to the CNIL the committee provides an opinion on the methodology of the research in relation to data protection law and on the necessity to use personal data in comparison the goal of the research.
The committee has to deliver its opinion in one month from the request. If no decision is taken during this period, the opinion is presumed to be in favour of the requester. After that, the request is submitted to the CNIL that has two months to come to a decision. Even in this case the lack of decision is considered as assent at the beginning of the processing.

3. Consent

Consent, that must be express where sensitive data are used, is one of the conditions that can legitimate the processing of personal data but it does not seem to have priority with respect to the other conditions listed in Article 8. Indeed, Article 8 of the law 801/2002 has implemented the exemptions to the prohibition to process sensitive data stated in Article 8 of the Directive.
Moreover, as seen above, the French law introduced a specific derogation for scientific research in the health sector.
Even if there is no specific legal provision, according to the indications of the CNIL "express consent" must be meant as "consent in written form".

4. Duty of Information

In relation to the duty to inform, law 801/2003 essentially follows the wording of Article 10 and 11 of the Directive.
If data are collected to be rendered anonymous in a short time the only information to provide are those relating to the identity of the controller and the purpose of the processing.
According to Article 32-III-3 where data are not obtained from the data subject the duty to inform is removed if: the processing is necessary for the storage of data for historical, statistical or scientific purposes and data were initially collected for another purpose; - providing information to the data subject proves to be impossible or requires disproportionate effort.

5. Notification and Prior Checking

The processing of no sensitive data requires the prior notification to the CNIL even if many exemptions to this rule are set out in Article 23 of the law 801/2004.
As far as medical research is concerned, the duty to notify the CNIL is removed when the controller has appointed an official. The latter must ensure the respect of data protection principles and must keep a register of processing operations accessible to any person who request to see it.
The appointment of the official must be notified to the CNIL.
Otherwise, when sensitive data are processed or the processing could present risks for the rights and freedoms of the data subject, the controller must obtain a prior authorisation through one of the several procedures provided by the law 801/2004.

6. Transfer of Personal Data to Third Countries

Chapter XII of the law 801/2004 states that personal data may be transferred to a third country only if the country in question guarantees an adequate level of protection. This principle suffers many exceptions that, even if with a different order, match with the exemptions listed in Article 26 of the Directive.

CNIL and the Council of the State have the power to provide for further derogation on condition that the third country ensures a "sufficient protection", however it is not clear how has to interpret the expression "sufficient protection".
Regarding the transfer of data concerning health, the CNIL in a recommendation of 1997 has considered the duty of secrecy of the recipients as adequate safeguards.

3.4.10 GERMANY

In 2001 the German legislator enacted a new version of the Federal Act on personal data protection in order to implement Directive 95/46/EC. The German Constitution provides for a sharing of competence to legislate in certain areas between the federation and the single states and this situation prevents that data protection regulation had/has a unique source.
The main legislation on data protection is contained in the aforementioned Federal Act 2001 (Bundesdatenschutzgesetz- BDSG) and in the data protection acts of the sixteen German states.
The English version of the BDSG is available at:
http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf

1. Personal Data and Anonymization

German legislator has introduced a very broad notion of personal data: not only information strictly connected to the person but also other circumstances in some way referable to the data subject. Aware of the possible consequences of a so wide interpretation of personal data, German legislators, both federal and statal, set up a "two-tier" system in various provisions regarding data protection: one distinct entity makes personal data anonymous and then passes the data to an other entity which will process the data. This implies that the same data are anonymous for who processes them (ex. the researcher that has not the key code) and personal for who may link the data with the person to which they refers to.
Therefore the notion of personal data is quite relative in the German system: what is personal data for a controller may be anonymous data for another.

2. Medical Research – Scientific Research

In Germany scientific research receives constitutional protection and it is necessary to balance the interest of person to privacy with the interest to the research.
Section 40.2 of the BDSG states that personal data collected for the purpose of scientific research must be rendered anonymous as soon as possible in view of the goals of the

research. Until that moment the controller must pseudonymized data, if possible, ensuring that information which permits the re-identification of the data subject are kept separately from the data used by the researches.
If data are lawfully collected, once rendered anonymous the may be freely supplied to other researchers.

2.1 special provisions for scientific research

According to Section 13.2 n.8 of the BDSG the collection of sensitive data ("special types of personal data" in the wording of BDSG) is permitted only in so far as "*such collection is necessary for the purposes of scientific research, where the scientific interest in carrying out the research project substantially outweighs the data subject's interest in excluding collection and the purpose of the research cannot be achieved in any other way or would otherwise necessitate disproportionate effort*".
Therefore, sensitive data can be collected without the data subject's consent where the conditions point out above are met.
Moreover, Section 14.5 n.2 stipulates the legitimacy of "storage, modification and use of special types of personal data for other purpose" if the following conditions are satisfied:
–this is necessary to carry out the scientific research;
–scientific interest in conduct of the research project substantially outweighs the interest of the data subject in excluding the change of purpose;
–the research purpose cannot be attained by other means or can be attained thus only with disproportionate effort.
According to the aforementioned provisions a careful balance among the competing interests is required.

2.2 implementation of Article 8.3 of the Directive

Section 13.2 n.7 of the BDGS allows the collection of sensitive data where it is necessary for the purposes of preventive medicine, medical diagnosis, health care or the administration of health services and the processing of these data is carried out by medical personnel or other persons who are subject to an obligation to maintain secrecy.
The collection of data for medical research is not covered by the scope of the provision.

3. Consent

Processing of personal data requires the data subject's consent or the satisfaction of one of the conditions set out in Section 13 of the BDGS that substantially implements Articles 7 and 8 of the Directive. Consent does not seem to have priority with respect to the other conditions.
Consent must be given in writing, otherwise it is invalid. With reference to scientific research an exception to the written consent principle is set out in Section 4a.2 where the defined purpose of research would be impaired considerably if consent were obtained in writing.
Therefore, other forms of consent are permitted but the controller must keep records of any consent given.

Moreover, consent must be informed on the purposes of collection, processing and on the use of data.

4. Duty of Information

According to Sections 19 and 19a of the BDGS the controller must inform the data subject either when the data are collected from the data subject or in case of collection from someone else. However, in the latter hypothesis are provided certain exemptions from the duty to inform.

The breach of the duty does not make the collection and the subsequent processing of the data necessarily unlawful. Information may be supplied afterwards but if the controller, at the time of the collection, failed to inform the data subject about the nature mandatory or voluntary of the collection the processing could be unlawful whereas the data subject would not have provided the data if adequately informed.

5. Notification and Prior Checking

Section 4 of the BDGS states a general duty for the controller to notify the Supervisory Authority about the processing of personal data.

Even if there is no special derogation from the duty to notify regarding medical research, Section 4d.2 provides for an exemption when an official for the protection of personal data has been appointed. Many hospitals and research institutions have provided for the appointment of an official but a very small numbers of them fall into this category since the aforementioned provision, of federal nature, does not apply to hospitals and research institutions under the state jurisdiction.

As far as state legislation is concerned, there are essentially two different systems: 1) some states follow the federal provision creating a duty to notify the Supervisory Authority unless local data protection officials are appointed; 2) in other states the appointment of data protection officials is legally binding and by consequence there is no additional duty to notify.

Under federal law the prior checking is required for the processing of sensitive data unless: - data subject has given his/her explicit consent; - there is a legal obligation to process or the processing corresponds to the purpose of a contract or a quasi-contractual fiduciary relationship with the data subject.

Also state Acts on data protection have introduced the prior checking where automated procedures are used.

6. Transfer of Personal Data to Third Countries

Articles 25 and 26 of the Directive have been implemented by Section 4b of the BDGS concerning the transfer of personal data abroad and to supranational or international bodies.

3.4.11 GREECE

The Directive 95/46/EC has been implemented in Greece with the Law n. 2472/1997. Before that moment personal data protection was not provided for by Greek legislation.
The English version of the Greek law of implementation is available at:
http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL

1. Personal Data and Anonymization

According to Article 2.c of the Law 2472/97 the identity or the data subject may be determined directly or indirectly by reference to an identity card number or to one or more factors. The law does not specify who is able to make the identification, thus a subject may be considered identifiable, and a data personal, if somebody, not only the controller, may perform the identification.
Law 2472/97 does clarify neither when personal data must be rendered anonymous, nor what is the exact meaning of the term "anonymization".
Probably, according to Greek law, the data is considered anonymous when the data subject can no longer be identified; however, the notion of "person identifiable" is not provided too.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Article 7.d allows the processing of sensitive data for preventive medicine or medical diagnosis without the consent of the data subject, but medical research cannot be included in this exemption.

2.2 substantial public interest

According to Article 7.d the collection and processing of sensitive data is permitted when " *processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained and all necessary measures for the protection of the persons involved are taken*".
This derogation is considered by the Greek implementation law as a public interest exemption.

3. Consent

Consent is defined as a freely given, explicit, specific and informed indication of will. The data subject can withdraw his/her consent in any time but with no retroactive effect.

Regarding the relation between consent and the other conditions that legitimate the processing of sensitive data, the former seems prevail over the latter. Therefore consent must be searched unless it reveals impossible or impracticable to obtain.

4. Duty of Information

According to Article 11.2 of Law 2472/1997 the controller has an obligation to inform the data subject, specifically and in writing, about the purposes of the processing, the identity of the controller, the nature of the data and whether is mandatory or not cooperate at the data collection.

The Greek Law on data protection does not take into account the case where the controller wishes to use the data for a new purpose different from the original and does not implement Article 11 of the Directive concerning the duty of information in the situation where the data have not been obtained from the data subject.

5. Notification and Prior Checking

According to Article 6 of Law 2472/97, the controller has a duty to notify in writing the Data Protection Authority (DPA) the establishment of a personal data file or the beginning of the processing.

Moreover, in the Greek system the processing of sensitive data requires a special permission by the DPA.

6. Transfer of Personal Data to Third Countries

Article 9 of Law 2472/97 permits the transmission of personal data to foreign countries which do not guarantee an adequate level of protection in accordance with Article 26 of the Directive.

3.4. 12 HUNGARY

Data protection of personal data is provided for by the Act n. LXIII 1992 on Protection of Personal Data and Disclosure of Data of Public Interest as amended by Act n. XIX 2005 (DPA). The English version of the DPA is available at:
http://abiweb.obh.hu/dpc/index.php?menu=gyoker/relevant/national/1992_LXIII

1.Personal Data and Anonymization

Article 2 of the Hungarian DPA defines personal data as "*any data relating to a specific (identified or identifiable) natural person as well as any conclusion with respect to the data subject which can be inferred from such data. In the course of data processing such data shall be considered to remain personal as long as their relation to the data subject can be restored. An identifiable person is in particular one who can be identified, directly or*

indirectly, by reference to his name, identification code or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

2. Medical Research

The DPA does not stipulate specific provisions, as well as exemptions to the data protection principles, relating to medical research.

3. Consent

According to Article 2.6 of the DPA consent is any freely given, specific and informed indication of the wish of the data subject by which he/she signifies his unmistakable agreement to the processing of personal data relating to him/her.

The processing of sensitive data requires the data subject's written consent.

Even though conditions other than consent may legitimate the processing of sensitive data, consent seems prevail over the alternatives, therefore consent must be obtained when it is not impossible or impracticable.

According to DPA 2000 the consent is not the only condition that can overcome/overrule the prohibition to processing personal data.

Articles 5-9 of the DPA substantially implement the exemptions set out in articles 7 and 8 of the Directive.

4. Duty of Information

According to Article 6 (2) of the DPA the controller has a duty to give the data subject unambiguous and detailed information about: the purposes and legal basis of the data processing; the identity of the person authorised to carry out the data processing and the technical data processing; the duration of data processing and who is authorised to have access to the data.

Article 6 (4) states that "*If it is impossible to inform each data subject or if it would entail disproportionate expenses, particularly in the case of processing data for statistical or scientific (including historical research) purposes, information may be given by making public, in a way that it will be accessible to all, the fact of data collection, the data subjects concerned, the purpose of the data collection, the duration of the data processing, and the accessibility of the data*".

5. Notification and Prior Checking

Article 28 of the DPA states that the controller has a duty to notify the Data Protection Commissioner (DPC) before the beginning to process personal data.

Exemption from the afore mention rule are provided by Article 30: the duty to notify the DPC is removed where, among other hypothesis, data processing operation involve personal data relating to the diseases or state of health of persons receiving medical care, for purposes of

medical treatment or preservation of health or for social insurance claims or serve the purposes of scientific research, provided that the data are not made public
According to Article 31 of the DPA the Data Protection Commissioner may perform prior checking before the technical processing of new data files or the application of new technical data processing technologies.

6. Transfer of Personal Data to Third Countries
The transfer of personal data to third countries is regulated by Article 9 of the Hungarian DPA that substantially copies the provisions of Articles 25 and 26 of the Directive.

3.4.13 IRLAND

The Data Protection Act 2003 has implemented Directive 95/46/EC amending the previous regulation on data protection.
The Irish Data Protection Act (DPA) is available at:
http://www.dataprotection.ie/images/Act2003.pdf

1. Personal Data and Anonymization
According the DPA 2003 personal data is any information relating to an individual that alone or combined with other factors permits the identification of the subject to whom it refers to.
It does not matter who can make the identification.
The DPA 2003 does not contain any express provision on the anonymization, however where the data subject is no longer identifiable the data has to be considered anonymous and, thus, outside the scope of the DPA.
If the data are used for a purpose not disclose at the time of the collection this does not necessary mean that the data have been obtained unfairly, provided that the data are not used in such a way that damage or distress is, or it likely to be, caused to any data subject.

2. Medical Research
2.1 implementation Article 8.3 of the Directive
Section 2b of the DPA provides for an exemption from the prohibition to process personal data where: "the processing is necessary for medical purposes and is undertaken by (I) a health professional, or (II) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which that would exist if that person were a heath professional".
The term "medical purpose" receives a wide interpretation in the DPA including not only preventive medicine and medical diagnosis but also medical research.

2.2 substantial public interest

Section 2B (1)(b)(iii) states an hypothesis of exemption from the general ban to process sensitive data for medical research on public interest grounds were: "*the processing is necessary to prevent injury or other damage to the health of the data subject or another person or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where: (I) consent to the processing cannot be given by or on behalf of the data subject; or (II) the data controller cannot reasonably be expected to obtain such consent; or (III) the processing is necessary to prevent injury or other damage to the health of another person or serious loss in respect of, or damage to, property of another person, in a case where consent has been unreasonably withheld*".

Section 2B (1)(b)(iii) provisions go far beyond the scope of Article 8(2)(c) of the Directive where the exemption applies when the processing is necessary to protect the vital interest of the data subject or of another person and the data subject is physically or legally incapable of giving a valid consent.

3. Consent

Explicit consent of the data subject is one of the condition that may legitimate the processing of sensitive data, even if the DPA does not clarify the meaning of the term "explicit consent".

Consent is not considered prevalent with respect to the other conditions enumerated in Sections 2A and 2B legitimating respectively the processing of normal data and sensitive data.

It is therefore acceptable to rely on non-consent alternatives even if consent would be practicable.

4.Duty of Information

Section 2D of the DPA listed the information that must be given to the data subject. When the data are collected from the data subject the duty to inform involves: identity of the controller or of his/her representative; - purpose or purposes of the processing operations; - any other information needed, taking in consideration the specific circumstances of the processing, to guarantee a fair and lawful processing.

Where data are not obtained from the data subject together with the above mentioned information, the following additional information must be supplied: - the categories of data concerned, and – the name of the original data controller.

In case of further processing for the purpose of scientific research it is permitted to derogate from the duty to inform when information reveals impossible or would involve a disproportionate effort.

5. Notification and Prior Checking

The unique exemption from the duty to notify the Supervisory Authority for medical research related to the manual processing of data. Nowadays this regulation is not yet applicable, therefore all processing operations require to be notified.
Even though Section 12A of the DPA provides for prior checking of processing that is likely to cause substantial damage or distress to the data subject, no regulations clarify the type of processing covered by this provision.

6. Transfer of Personal Data to Third Countries

Section 11 of the DPA permits the transfer of personal data to third countries that do not ensure an adequate level of protection at the same conditions provided by Article 26 of the Directive.

3.4.14 ITALY

Personal Data Protection is currently regulated by the Personal Data Protection Code 2003 (PDPC) issued with the Legislative Decree n. 196 of 30 June 2003.
The English version of the PDPC is available at: http://www.garanteprivacy.it/garante/doc.jsp?ID=311113

1. Personal Data and Anonymization

According to Section 4 of the PDPC 'personal data' means any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number.
Moreover, 'anonymous data' means 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. Medical Research

2.1 implementation Article 8.3 of the Directive

The PDPC does not contain a direct implementation of Article 8.3 of the Directive. Indeed, according to Section 85.2 of the PDPC "the processing of data disclosing health that is carried out either by health care professionals or by public health care bodies for the purpose of protecting health or bodily integrity of a data subject, a third party or the community as a whole" requires the data subject's consent or the authorisation by the Garante (the Italian Supervisory Authority).

2.2 substantial public interest

The PDPC in Sections 85 and 86 provides for numerous exemptions from the prohibition to process sensitive data based on the substantial public interest.

Medical research is not included in the above mentioned derogations.

3. Consent

According to Section 26 of the PDPC sensitive data may only be processed "with the data subject's written consent and the Garante's prior authorisation, by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations".

The Garante must communicate its decision concerning the request for authorisation within forty-five days and if the communication is not given in the said term, the request must be regarded as dismissed. Along with the authorisation the Garante may provide for measures and precautions in order to safeguard the data subject, which the data controller must apply.

Part II, Title V, Sections 75 and 76 of the PDPC provides for specific rules for the processing of personal data in heath care sector: "*Health professionals and public health care bodies may process personal data disclosing health: a) 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, or b) also without the data subject's consent, based on the Garante's prior authorisation, if the purposes referred to under a) concern either a third party or the community as a whole*".

The Garante's authorisation shall be granted after seeking the opinion of the Higher Health Care Council except for emergencies.

4. Duty of Information

According to Section 13 of the PDPC the controller has a duty to inform the data subject about: - the purposes and modalities of the processing for which the data are intended; - the obligatory or voluntary nature of providing the requested data; - the consequences if he/she fails to reply; - 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 identification data concerning the data controller or his/her representative.

According to Section 13 paragraph 4 if the personal data are not collected from the data subject, the information, also including the categories of processed data, has been provided to the data subject at the time of recording such data or, if their communication is envisaged, no later than when the data are first communicated.

The latter paragraph does not apply if the provision of information to the data subject involves an effort that is declared by the Garante to be manifestly disproportionate compared with the right to be protected. In this case the Garante must lay down suitable measures.

5. Notification and Prior Checking

According to Section 37 of the PDPC "*the notification of processing operations has to be submitted to the Garante in advance of the processing and once only, regardless of the number of operations to be performed and the duration of the processing, and may concern one or more processing operations for related purposes*".

According to Section 40 of the PDPC the provisions of Personal Data Protection Code "*referring to an authorisation to be granted by the Garante shall also be implemented by issuing authorisations applying to specific categories of data controller or processing, which shall be published in the Official Journal of the Italian Republic*".

Therefore if the data controller or the processing fall under the above mentioned provision Garante authorization is not required.

6. Transfer of Personal Data to Third Countries

Title VII, Sections 42, 43, 44 and 45, implements the provisions of Articles 25 and 26 of the Directive concerning the transfer of personal data to third countries outside EU and EEA.

3.4.15 LATVIA

Directive 95/46/EC has been implemented in Latvia with the Personal Data Protection Law 2000 (PDPL) subsequently amended in 2002 and 2006.

The English version of the PDPL is available at: http://www.dvi.gov.lv/eng/legislation/pdp/

1. Personal Data and Anonymization

Personal data means any information relating to a person that permits the identification of the person itself. Generally it does not matter who can make the identification.

The procedure to render anonymous data is considered as processing covered by the PDPL.

It is possible to process the data for a purpose other then the original one (the purpose of the collection) only if there is not breaching of the data subject's rights and the processing is carried out for the needs of scientific research or statistic. The data controller must inform the data subject of the new processing purpose.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Section 11 of the PDPL permits the processing of sensitive data if it is necessary for the purpose of medical treatment and it is carried out by a medical practitioner and an adequate level of protection of personal data is guaranteed.
Law on Medical Treatment states that "information regarding a patient may be used in scientific research if the anonymity of the patient is guaranteed or his/her consent has been received".

3. Consent

The PDPL defines consent as a freely given expressed affirmation of wishes of the data subject by which the data subject allows his or her personal data to be processed.
Certain legislative acts require that the express consent must be given in written for in order to legitimate the processing of the data (e.g. the Human Genome Research Law).
Section 16 of the PDPL states the conditions alternative to consent that can legitimate the processing of sensitive data. It is probably possible to use alternatives to consent even when it is not impossible or impracticable to obtain it

4. Duty of Information

According to Section 15 of the PDPL the controller must inform the data subject about the identity of the controller, the purpose of the processing, the possible recipients of the data and the data subject's right to access the data and to rectify them. The obligation to inform the data subject exists either when the data are collected from the data subject or when are obtained from another source.
According to Section 17 of the PDPL the duty to inform the data subject is removed if the processed data are used only for the needs of scientific and statistical research.

5. Notification and Prior Checking

PDPL does not provide for any derogation or simplification to the duty to notify the Supervisory Authority.
The notification is always required before starting the data processing in compliance with prescriptions of the PDPL. The person who wishes to carry out the processing of personal data must submit an application to the State Data Inspection.
Regarding the prior checking, certain specific rules for medical research are set out in the Human Genome Research Law: the controller must immediately give each tissue sample, DNA profile, health profile and genealogy a unique code in order to replace all data that enable the identification of the gene donor. This unique code must be indicated in the written informed consent form. The State Data Inspection must approve the method of generating these codes.

6. Transfer of Personal Data to Third Countries

Generally, the transfer of personal data to a third country is permitted only if the state in question ensures an adequate level of data protection an a written permission has been obtained from the SDI. It is possible to derogate from the above mentioned principle at the conditions laid down in Section 28 of the PDPL copying the provisions of Article 26 of the Directive.

3.4.16 LITHUANIA

Directive 95/46/EC has been implemented in the Lithuanian legal system with the Law on the Legal Protection of Personal Data 2003 (LLPPD).
The English version of the LLPPD is available at:
http://www.ada.lt/images/cms/File/pers.data.prot.law.pdf

1. Personal Data and Anonymization

Article 2.1 defines "personal data" as any information relating to a natural person whose identity is known or can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

According to Article 10 of the LLPPD personal health data may be processed by an authorized health care worker. This provision does not cover medical research.
In the Lithuanian system personal data for the purpose of medical research must be processed in compliance with the Law on Ethics of Biomedical Research. Article 4 of the latter law states that in the medical research the researcher must ensure the protection of the data subject as well as the confidentiality of information about him/her.

2.2 substantial public interest

There is no in the LLPPD an explicit derogation from the ban to process sensitive data for the purposes of medical research based on public interest.

3. Consent

Even if usually it does not seem that consent prevails over the other conditions legitimating the processing of sensitive data, consent is given a priority in case of medical/scientific research.
According to Article 12.1 of the LLPPD if data are processed for the purpose of scientific research, the data subject's consent is required. The processing of personal data without the

consent of the data subject is possible only after reporting to the State Data Protection Inspectorate (SDPI).
The LLPPD does not contain a definition of "explicit consent" needed for the processing of sensitive data.

4. Duty of Information

According to Article 18 of the LLPPD the controller must inform the data subject about the identity of the controller, the purpose of the processing, the possible recipients of the data and the data subject's right to access the data and to rectify them. The obligation to inform the data subject exists either when the data are collected from the data subject or when are obtained from another source. In the latter case the duty to inform is removed when data are processed for statistical, historical or research purposes and the provision of such information proves impossible or would involve disproportionate effort.

5. Notification and Prior Checking

Article 25 of the LLPPD states a general obligation to notify the Supervisory Authority about the automated processing of personal data. There are some exemptions from the duty to notify but medical research is not included in them.
According to Article 26 of the LLPPD the prior checking of the SDPI is not required when the controller processes data for health care or medical research purposes.

6. Transfer of Personal Data to Third Countries

Article 28 of the LLPPD corresponds to Articles 25 and 26 of the Directive.

3.4.17 LUXEMBOURG

Directive 95/46/EC has been implemented in Luxembourg with the new Data Protection Law 2002 (DPL) amended in 2007.
The English version and the French version of the DPL are both available at:
http://www.cnpd.lu/fr/legislation/legis_nationale/index.html

1. Personal Data and Anonymization

According to Article 2 of the DPL personal data means any information concerning an identified or identifiable person. The identification can be made directly or indirectly especially by reference to an identification number or one or several elements.

The DPL does not contain reference to the anonymization question, however coded data are still considered as personal data if anybody can create a link between the data and the data subject.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Article 8.3 of the Directive has been implemented by Article 7 of the DPL where it is stated that the prohibition to process sensitive data does not apply if the processing is necessary for preventive medicine, medical diagnosis, administration of care and treatment, management of health services, and scientific research in biological and medical field. Therefore medical research falls under the scope of the exemption.

2.2 substantial public interest

Article 6(2)(g) stipulates that the ban to process sensitive data does not apply where the processing is necessary for reasons of public interest, especially for historical, statistical or scientific purposes. In this case the processing must receive a prior authorization from the National Commission.

3. Consent

Article 2(c) of the DPL defines the data subject's consent as any expression of express, non-equivocal, free, specific, and informed willingness.

Article 5 provides the conditions that can legitimate the processing of sensitive data: the alternatives to consent are similar to those mentioned in Article 8 of the Directive. It seems that is sufficient to comply with one of the condition to render the processing legitimate, therefore consent is not given priority.

4. Duty of Information

Article 26 of the DPL set out the duty to inform the data subject while Article 27 provides the exemptions to this duty.

The information to be provided to the data subject is the same as that of the Directive. Moreover the controller must supply information about the length of time the data will be kept.

It is not considered in the DPL context the case where the controller, having collected the data from the data subject decides to change the purpose.

5. Notification and Prior Checking

According to Article 12 of the DPL the duty to notify the National Commission does not apply to certain processing of the data. The only exemption that may refer to medical research is that for the further processing for historical, scientific, or statistical purposes.

In the aforementioned case the notification is replaced by the prior checking. In fact, the

controller must obtain prior authorization from the National Commission.

6. Transfer of Personal Data to Third Countries

Article 19(3) implements Article 26 of the Directive. The transfer of personal data to a third country that not ensure an adequate level of protection can be authorized by the National Commission at the same conditions stated in the Directive.

3.4.18 MALTA

Data Protection Act 2001 (DPA) has been introduced in order to render Maltese legislation compatible with Directive 95/46/EC.
The English version of the DPA is available at:
http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/malta_en.pdf

1. Personal Data and Anonymization

Article 2 of the DPA defines personal data with the same wording of the Directive. Therefore, "personal data means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".
There is no reference to the anonymization.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Article 15 of the DPA states that sensitive data may be processed for health and hospital care purposes and the processing is carried out by a health professional or other person subject to the obligation of professional secrecy.
Medical research is not covered by this provision.

2.2 substantial public interest

According to Article 16 of the DPA sensitive personal data may be processed for research and statistics purposes, where the processing is necessary for the performance of an activity that is carried out in the public interest. If this processing has been approved by the Commissioner on the
advice of a research ethics committee the requirement of the public interest is deemed satisfied.

3. Consent

Consent is defined as a freely given, explicit, specific and informed indication of will. A particular form for consent is not required by the DPA.

According to Article 12 of the DPA explicit consent of the data subject is one of the conditions that can legitimate the processing of sensitive data. These conditions alternative to consent are listed in Articles 13-16.

4. Duty of Information

According to Article 19 of the DPA the controller has a duty to inform the data subject about the purposes of the processing, the identity of the controller, the nature of the data and whether is mandatory or not cooperate at the data collection.
Article 20 states that where data are not collected from the data subject the duty to inform must also cover the data concerned and the identity of the recipient.
In this second hypothesis the duty to inform does not apply if the data are processed for purposes of historical or scientific research and the provision of such information proves impossible or would involve a disproportionate effort.

5. Notification and Prior Checking

According to Article 29 of the DPA the controller is obliged to notify the Data Protection Commissioner (DPC) before carrying out any automated processing operations.
Exemptions or simplification to the above mentioned rule may be introduced by the DPC.
According to Article 34 the data controller may ask for the prior checking when there are risks for the data subject's rights and freedoms.

6. Transfer of Personal Data to Third Countries

Articles 27 and 28 of the DPA allow the transmission of personal data to foreign countries which do not guarantee an adequate level of protection in accordance with Article 26 of the Directive.

3.4.19 THE NETHERLANDS

Directive 95/46/EC has been implemented with the Wet Bescherming Persoonsgegevens (WBP) adopted by the Dutch Parliament on 3 July 2000. The WBP incorporated the previous legislation on data protection.
The English version of the WBP is available at:
http://www.dutchdpa.nl/downloads_wetten/wbp.pdf?refer=true&theme=purple

1. Personal Data and Anonymization

According to the WBP any data that may provide information about an identifiable natural person is considered personal data.
The person who can make the identification is not only the controller but also someone else.

Where data have been rendered completely anonymous the WBP does not apply in case of processing for a new purpose incompatible with the original one. Moreover the principles of the WBP do not apply when encryption or agreements about access to the data "reasonably" excludes the identification of the data subject.

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Article 23 of the WBP states the possibility to derogate from the general ban of processing sensitive data on scientific research grounds. This seems imply that preventive medicine and medical diagnosis should be interpreted in broad way in order to include also medical research. Nevertheless, the exemption is not formulated in this manner and certain conditions must be satisfied: a) the research serves a public interest; b) the processing is necessary for the research or statistics concerned; c) obtaining consent appears impossible or would involve a disproportionate effort; d) adequate measures have been adopted to ensure that the processing dose not adversely affect the individual privacy of the data subject to a disproportionate extent.

2.2 substantial public interest

According to Article 23.1 (e) of the WBP the prohibition to process sensitive data does not apply where the processing is necessary with a view of an important public interest, where appropriate guarantees have been adopted to protect individual privacy and this is provided by law or the Data Protection Commission (DPC) has granted an exemption. When the DPC provides for an exemption it may imposed particular rules or restriction on the data processing.

The WBP provides for various exemptions from the prohibition to process sensitive data based on public interest, not explicitly contained in the Directive, that must be notify to the European Commission.

Those exemptions on public interest grounds are contained in Articles 21.1, 21.3 and 21.4 of the WBP including, among other things, the processing of information for insurance companies when assessing risks, for schools when it is necessary to provide special support for pupils, for the Minister of Justice in relation to prison sentences.

3. Consent

Article 23.1(a) of the WPB requires the express consent of the data subject for the processing of sensitive data. Consent means any freely given, specific and informed expression of will whereby data subject agrees to the processing of data relating to him/her. Express consent does not necessary requires to be given in written form, an affirmative action could be enough.

The conditions listed in Article 8 of the Directive in order to allow the processing of sensitive are contained in different Articles of the WPB. Therefore, consent is not the only condition that

can legitimate the processing of sensitive data and the various conditions are considered open alternatives under the WBP.
However, according to the Medical Treatment Contracts Act, consent is always required to use medical information in research unless there are exceptional circumstances. The consent requirement is removed in two hypothesis: - where obtaining consent is not reasonably possible and if, with respect to the performance of the research, appropriate guarantees have been given that the privacy of the patient is not disproportionate affected; - where obtaining consent, having regard to the nature and object of the research, cannot be reasonable required and if the provider of the care has ensured that the information is given in such a manner to prevent the tracing of the patient.

4. Duty of Information

Articles 10 and 11 of the Directive concerning the duty to inform have been implemented by Articles 33 and 34 of the WBP.
In case of further processing for a purpose not anticipated at the time of the collection Article 9.2(6) applies. If the controller wishes to use the data for a purpose different than the original one, he/she must inform the data subject who has the opportunity of objection to the processing.

5. Notification and Prior Checking

The Exemption Decree 2001 provides derogation and simplification to the duty to notify the Supervisory Authority for certain categories of data. According to Article 30 of the Exemption Decree dealing with scientific research and statistics, the duty to notify is removed when obtaining, processing and controlling of the data needed for certain researches or for certain statistics.

6. Transfer of Personal Data to Third Countries

According to Article 77.2 of the WBP the DPC may authorize the transfer of data to a country which does not have adequate safeguards attaching to the authorization detailed rules in order to protect individual privacy and fundamental freedoms of persons.
Article 44 of the Exemption Decree stipulates that is mandatory the notification of data processing involving international transfers.

3.4.20 NORWAY

The Norwegian Personal Data Act, which came into force on 1 January 2001, has implemented the Directive 95/46/EC.
The English version of the PDA is available on the website at:
http://www.datatilsynet.no.htest.osl.basefarm.net/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf

1. Personal Data and Anonymyzation

The PDA defines "personal data" in terms very similar to the Directive: "any information and assessment that may be linked to a natural person". Neither the Directive nor the PDA clarify how to apply the said definition in order to decide when data are considered anonymous. The key variations in national regulations is whether the time, expense and labour needed to re-identify a data subject are crucial when deciding if the data are anonymous or not. According to Norwegian legislation data that could be linked, directly or indirectly or in whatever way and by whoever, to a natural person is always regarded as personal data.

2. Medical Research

2.1 implementation of Article8.3 of the Directive

The exemption from the ban to process sensitive data set out in Article 8.3 of the Directive has not been implemented in the Norwegian PDA:

2.2 substantial public interest

The preliminary works to the PDA mention research as an example of a task that can be in the public interest. In order to allow the processing on public interest basis the researcher must establish: the impossibility to obtain the data subject's consent without seriously damaging the research; the research is serving an important public interest; the risk involved is minimal. The Data Inspectorate (DI), the Norwegian Supervisory Authority, seems to apply the condition of necessity and public interest strictly: non-consent alternatives are rarely acceptable if to obtain consent is possible and not inappropriate.

Secondary processing of sensitive data for research without the consent of the data subject is allowed if strict legal and procedural safeguards are met. The interest in the processing must exceed the disadvantages it may entail for the natural persons. The DI has the power to decide if a specific research project complies with the requirements of the PDA, balancing the interests in research against the rights and freedoms of the data subjects.

The appropriate safeguards are: prior checking and licence from the DI before processing sensitive data.

3. Consent

Consent is "any freely given, specific and informed declaration by the data subject to the effect that he or she agrees to the processing of personal data relating to him or her".

Passive consent is not admitted. How specific the information should be for consent to be regarded as informed is crucial.

The PDA, as well as the Directive, prohibits the processing of sensitive data unless it satisfies one of the conditions set out on section 9. As far as the research is concerned, the most relevant criteria are: consent; the processing for statistical, historical and scientific purposes if the public interest overweights the disadvantages for the data subjects.

The Data Inspectorate is given the power to decide when sensitive data can be processed

beyond the cases laid down in Section 9 if: this is warranted by important public interest and measures are taken to protect data subject's interest.

4. Duty of Information

The PDA Section 19 implements and is in line with the provisions of Article 10 of the Directive. No explicit exemption from the duty to inform if the person who obtained the data wishes to use the data for a new purpose. According to the DI guidance any re-use of existing data should comply with the duty to inform as required by Article 11 of the Directive as implemented by Section 20of the PDA.

Section 20 lays down further information that must always be provided to the data subject without taking into account the "necessity test" foreseen by the Directive.

The duty to inform is applied very strictly and it is used like an argument to avoid processing without consent. DI translated the duty to inform into a requirement of consent if it possible and not inappropriate to inform data subject.

Consent is regarded as the main rule for processing personal data therefore the DI is reluctant to allow researches based on non-consent alternatives.

5. Notification and Prior Checking

Section 31 specifies the type of processing subject to the duty of notification while section 32 specifies the list of information to be notified.

In addition, Article 19 requires notification of the legal basis (consent or law) for collecting data and when the processing starts.

The Directive offers the Member States the opportunity to provide for exemptions from notification when the data controller has appointed a Data Protection Official in accordance with Article 18(2).

The DPO has an important role in the research field. It is responsible for ensuring compliance with the PDA and the Act on Personal health Data Filing Systems and the Processing of Personal Health Data, and for keeping a record of processing operations carried out by the data controller. DPO's functions are, inter alia: promote notification, verify the accuracy and adequateness of the information, keep a systematic public record of every processing operations, inform of possible breaches of the privacy and so on.

The appointment of DPO does not replace the legal responsibility of the data controller or the duties of the DI.

Data Protection Official for Research

The DPO for research was created on February 2003 with the Director of NSD appointed as the Ombudsman for Privacy in Research. Most medical research projects are subject to notification of and pre-evaluation by DPO for Research at NSD (in this case exemption from the duty to inform/contact the DI). DPO for Research's competence also covers projects that

need authorisation: in these cases DPO acts like a mandatory intermediary, assessing the project and making recommendations to the DI.
The institution of Data Protection Official for Research is seen as an important step (adequate, appropriate and suitable safeguard) towards effective implementation of the law with regard to research.

DI authorisation is needed when processing operations are likely to present a specific risk (involving sensitive data). Hence, the majority of medical and health research projects are subject to this kind of preventive control, even if the data subject gave his/her consent.
However, there are exceptions for certain types of processing considered less risky (e.g. the collected material is rendered anonymous or deleted on completion of the project). In these cases authorisation is replaced by notification.

6. Transfer of Data to Third Countries
According to Section 29 of DPA personal data may be transferred only to countries that guarantee an adequate level of protection. This adequateness is presumed in the States that implemented Directive 95/46/EC.
In evaluating the level of protection it shall be take into account, among other things, the nature of the data, the purpose and duration of the processing, the rules of law, the professional rules and the security measures which apply in the country in question.
However, even if an adequate level of protection is not guaranteed, the transfer of data to a third country is allowed when the requirements set out in section 30 of DPA are met or the DI gave its authorisation.
The conditions of Section 30 are the same enumerated in Article 29 of Directive 95/46/EC.

3.4.21 POLAND

Protection of citizen's privacy is firstly guaranteed at constitutional level (Article 47). Details of privacy protection are contained in the Act on the Protection of Personal Data of 1997 (APPD) amended in 2004 in order to meet the requirements of Directive 95/46/EC.
The English version of the APPD is available at:
http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/poland_en.pdf

1. Personal Data and Anonymyzation
According to the APPD personal data is defined as any information relating to a an identified or identifiable person"; it is not specified if it matters who can identify the data subject. The Act protects personal data of natural (living) person and it does not apply to dead person.
The main rule in polish legislation on data protection is not anonymization but authorisation to process data for certain purposes.

Protection of privacy of the data subject by means of anonymization applies only to the data that are made public. In fact Article 27 of the APPD specifies that data used for research purpose must not make identification of persons possible in publishing the results of the research.

2. Medical Research

2.1 implementation of Article8.3 of the Directive

According to Article 27 7) of the APPD it is possible to overcome the ban to process sensitive data where the processing is required for the purposes of preventive medicine, the provision of care or treatment, where the data are processed by a health professional subject involved in treatment, other health care services, or the management of health care services and subject to providing appropriate safeguards.

This provision does not include medical research.

2.2 substantial public interest

The exemption for the public interest is not implemented in the APPD.

2.3 other exemptions

According to Article 27 9) of the APPD the processing of sensitive data does not constitute a breach of the data protection principles if "i*t is necessary to conduct scientific researches including preparations of a thesis required for graduating from university or receiving a degree; any results of scientific researches shall not be published in a way which allows identifying data subjects*".

3. Consent

Article 5) of the APPD defines the data subject's consent as " a declaration of will by which the data subject signifies his/her agreement to personal data relating to him/her being processed; the consent cannot be alleged or presumed on the basis of the declaration of will of other content".

When data processing refers to sensitive data a written consent is required under Article 27 of PPDA.

In the same terms as Article 8 of Directive the consent is not the only condition that can legitimate the processing of sensitive data and consent does not seem to have priority with respect to the alternatives.

5.Duty of Information

Articles 24 and 25 of the APPD set out the duty to inform the data subject about the processing of the data referring to him/her. In particular Article 24 takes into consideration the case where personal data are collected from the data subject. In this event the controller is obliged to provide a data subject from whom the data are collected with the following information:

a) the address of its seat and its full name, and in case the controller is a natural person about the address of his/her residence and his/her full name,
b) the purpose of data collection, and, in particular, about the data recipients or categories of recipients, if known at the date of collecting,
c) the existence of the data subject's right of access to his/her data and the right to rectify these data,
d) whether the replies to the questions are obligatory or voluntary, and in case of existence of the obligation about its legal basis.
If data are not collected from the data subject according to Article 25 the controller has also to provide the source of the data.
However, if the data are necessary for scientific, didactic, historical, statistic or public opinion research, the processing of such data does not violate the rights or freedoms of the data subject, and the provision of information would involve disproportionate efforts or endanger the success of the research, the duty to inform is removed.

5. Notification and Prior Checking

According to Article 40 of the APPD the controller must notify the Inspector General the automated processing of personal data in order to obtain the registration. The application for registration must meet the requirements of Article 41: purpose of processing, identity of the controller and so on.
Article 43 of the APPD provides for certain exemptions from the obligation to notify but medical research is not included.

6. Transfer of Data to Third Countries

According to Article 47T of the APPD the transfer of personal data to a third country may take place only, if the country of destination ensures at least the same level of personal data protection in its territory as that in force in the territory of the Republic of Poland.
However, some exemptions are provided for in compliance with Article 26 of the Directive.

3.4.22 PORTUGAL

The Data Protection Directive 95/46/EC was implemented into the Portuguese system by the Law n. 67 of 26th October 1998 (hereinafter DPA).
The English version of DPA is available on the website at:
http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM

1. Personal Data and Anonymyzation

According to article 3a of the Portuguese DPA personal data is "any information of any type, irrespective of the type of medium involved, including sound and image, relating to an

identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".
The DPA does not contain reference to the potential identifier; therefore if someone, the controller or anybody else, could make the identification the data is considered personal.

2. Medical Research

2.1 implementation of Article8.3 of the Directive

The processing of data relating to health and sex life, including genetic data, shall be permitted if it is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided those data are processed by a health professional bound by professional secrecy or by another person also subject to an equivalent obligation of secrecy and are notified to the National Data Protection Commission (NDPC) and where suitable safeguards are provided.
Medical research is not included in this provision.

2.2 substantial public interest

The Portuguese DPA does not contain an explicit derogation to the prohibition of processing sensitive data on substantial public interest grounds.

3. Consent

Consent is one of the conditions able to permit the processing of sensitive data (as well as no sensitive data). The consent must be explicit but in the DPA is not clarify if the written form is required.
Article 7 of the DPA states in which cases the processing of sensitive data is permitted. Among other: a) when it 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; c) when it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations; when it is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose.
It is not clear if consent has priority with respect to the other conditions legitimating the process of sensitive data.

4. Duty of Information

The data subject's right to be informed about the processing of data referring to him/her is set out in Article 10 of DPA. It deals both with the case of collection from the data subject and where data have not been obtained from the data subject.
The information should cover: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing; (c) other information such as: the recipients or categories

of recipients and whether replies are obligatory or voluntary, as well as the possible consequences of failure to reply.
Article 10.1.b) requires the controller to inform the data subject about the purposes of the processing, thus anytime there is a change of purpose the renewal of information is due.
According to Article 28 of the DPA if the controller wishes to use data for purposes not anticipated at the time of the collection it is necessary the authorisation of the NDPC.
Article 10.5 provides for an exception from the duty of information in case of statistical processing for the purposes of historical or scientific research, when the provision of such information proves impossible or would involve a disproportionate effort.

5. Notification and Prior Checking

According to Article 27 of the DPA the controller or his /her representative must notify the NDPC 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.
There are no exemptions or simplification relating to medical research.
The processing of sensitive data as medical data is also subject to the prior authorisation from the NDPC.

6. Transfer of Data to Third Countries

The Portuguese DPA transposes the Directive provisions relating to the flow of Personal Data: the transfer is allowed if the third country guarantees an adequate level of protection.
In the Portuguese data protection system the NDPC is responsible in evaluating the so-called "adequate level of protection" and determine which measures should be considered adequate safeguards.

3.4.23 ROMANIA

The Directive 95/46/EC was implemented by the Law n. 677 of the 21 November 2001.
In 2005 Romanian Parliament passed the Law n. 102 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing
The English version of the Law n. 677/2001 is available on the website at:
http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/ro_law_677_2001_en_unofficial.pdf

1. Personal Data and Anonymyzation

Article 3 of the Law 677/2001 gives the same notion of personal data provided for Article 2 of the Directive and defines anonymous data as the data that, due to its specific origin or specific manner of processing, cannot be associated to an identified or identifiable person.

2. Medical Research

2.1 implementation of Article8.3 of the Directive

Article 7.2 g) of the Law 677/2001 states that the ban to process sensitive data is removed when: " *the processing is required for preventive medical care, to establish a medical diagnosis, to provide medical care or treatment in the interest of the data subject, or to manage health services that are in the best interest of the data subject, on the condition that the processing of that data is performed by, or under the supervision of medical staff pledged to professional secrecy or by or under the supervision of another person subject to a similar obligation regarding the secrecy*".

The above mentioned provision does not cover medical research.

3. Consent

According to Law 677/2001 the data subject's consent is one of the conditions that can legitimate the processing of personal data, sensitive and non-sensitive. In the former case the consent must be explicit even if the Law 677/2001 does not require a particular form.

It does not seem to be necessary to obtain consent when an alternative, another conditions stated in Articles 7 and 8 of the Law, is available.

4. Duty of Information

Article 12(1) of the Law 677/2001 stipulates that it is mandatory to inform the data subject at least about: the identity of the controller or of his/her representative; the purpose of the data processing and any further information such as the categories of data concerned, the right of access and of intervention to rectify the data, and all other information that have to be delivered by the Supervisory Authority.

The controller must provide the data subject with the aforementioned information even if the data have not been obtained from the data subject.

However, in the latter hypothesis the duty to inform the data subject does not apply when the processing of data is carried out for statistical, historical or scientific research, or in any other situations if providing such information proves to be impossible or would involve a disproportional effort versus the legitimate interest that might be damaged, as well as in the situations in which recording or disclosure of the data is expressly stated by law.

5. Notification and Prior Checking

According to Article 22(1) of the Law 677/2001, before carrying out any processing operation, the controller is obliged to notify the Supervisory Authority. The processing of personal data for medical researcher is included in this provision but in fact it is not yet respected.

The law 677/2001 does not provide for a the prior checking of processing that involves medical research.

6. Transfer of Data to Third Countries

Article 27 of the Law 677/2001 allows the transfer of personal data to third Countries (outside EU) if there is an authorisation of the Supervisory Authority (Ombudsman) and the recipient State guarantees the same level of data protection.

3.4.24 SLOVAKIA

Directive 95/46/EC has been implemented in the Slovakian legal system with the Protection of Personal Data Act n. 428/2002 (PPDA) as amended by the Act n. 602/2003, Act n. 576/2004 and the Act n. 90/2005.

The English version of the PPDA is available at:

http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/slovakia_428_02_en.pdf

1. Personal Data and Anonymyzation

According to Section 3 of the PPDA personal data means "*any information relating to an identified or identifiable natural person, while such person is one who can be identified, directly or indirectly, in particular by reference to a identifier of general application or by reference to one or more factors specific to his physical, physiological, psychic, mental, economic, cultural or social identity*".

Moreover, Section 4 k) defines anonymous data as a data "*adjusted in such manner that it cannot be matched with the concerned data subject*".

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Section 9 e) of the PPDA states that the prohibition to process sensitive data does not apply where "*the processing is performed for the purposes of providing medical care and effecting public health insurance, provided that these data are processed by a provider of the medical care, a health insurance company or the Office for Internal Supervision over Health Care*".

This provision does not cover medical research.

2.2 substantial public interest

The PPDA does not contain any express exemption from the ban to process sensitive data for medical research by reference to the public interest.

3. Consent

According to Section 8 of the PPDA sensitive data may be processed only with the written consent of the data subject or when another condition stated in same Section applied.

Consent does not seem to have priority over other conditions.

However, according Section 7(4) of the PPDA " *Biometrical data may only be processed under conditions stipulated by a special Act, provided that a) it expressly results for the controller from the Act; or b) the data subject gave a written consent to the processing*".

4. Duty of Information

According to Section 10 of the PPDA, the data controller is obliged to inform the data subject about: the identity of the controller and of his/her representative if any; the purpose of the personal data processing; additional information to the extent necessary for safeguarding the rights and legitimate interests of the data subject with regard to all circumstances of the processing of personal data (e.g. Whether replies to the questions is mandatory or voluntary).
The same information must be supplied also if personal data were not collected directly from the individual to whom they relate no later than on the recording or disclosure of personal data to the data recipient.
In the latter case the duty to inform is removed when the processing of the data is for historical, statistical or scientific-research purposes and provides the information proves to be impossible or would involve disproportionate costs and effort.

5. Notification and Prior Checking

Section 26 of the PPDA states that before commencement of the processing of personal data the controller must notify the Office (Slovakian Supervisory Authority) for registration.
According to Section 27 the processing of sensitive data, included data relating to health, requires a special registration.

6.Transfer of Data to Third Countries

According to Sections 23 and 24 of the PPDA the transfer of data to third countries is subject to the same conditions listed in Article 25 and 26 of the Directive.

3.4.25 SLOVENIA

Personal data protection in Slovenia is currently regulated by the Personal Data Protection Act 2004 (PDPA) enacted in order to put the Slovenian legislation in accordance with the Directive 95/46/EC.
The English version of the PDPA is available at:
http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf

1. Personal Data and Anonymyzation

According to Article 6 of the PDPA personal data is any data relating to an individual, irrespective of the form in which it is expressed. Moreover, individual is an identified or

identifiable natural person to whom personal data relates The identification may be effectuated directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, where the method of identification does not incur large costs or disproportionate effort or require a large amount of time.
The Slovenian PDPA contain express reference to the anonymization as an alteration to the form of personal data such that they can no longer be linked to the individual or where such link can only be made with disproportionate efforts, expense or use of time.
Therefore, the PDPA introduces the limit of the "reasonable means".

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Article 13.6 of the PDPA states that prohibition to process sensitive data does not apply where the data are processed by health-care workers and health-care staff in compliance with statute for the purposes of protecting the health of the public and individuals and the management or operation of health services.
This provision does not seem to cover medical research.

2.2 substantial public interest

The PDPA does not contain any express exemption from the ban to process sensitive data by reference to the public interest.

3. Consent

The data subject explicit consent in written form is one of the condition that may legitimate the processing of sensitive data.
However, Article 13 of the PDPA set out some alternatives to consent that seems to be equivalent.

4. Duty of Information

According to Article 19 of the PDPA if personal data are collected directly from the individual to whom they relate, the data controller or his representative must communicate to the individual the following information: identity of the controller and his/her possible representative and the purpose of the processing of personal data.
The same information must be supplied also if personal data were not collected directly from the individual to whom they relate no later than on the recording or disclosure of personal data to the data recipient.
In the latter case the duty to inform is removed when the processing of the data is for historical, statistical or scientific-research purposes and to provide the information proves to be impossible or would incur large costs or disproportionate effort or would require a large amount of time, or if the recording or supply of personal data is expressly provided by statute.

5. Notification and Prior Checking

Article 27 of the PDPA provides for a general obligation to notify the National Supervisory Body for Personal Data Protection at least 15 days prior to the establishing of a filing system or prior to the entry of a new type of personal data.

According to Article 60 of the Health Activity Law 1992 a medical-ethics commission has been established in order to study and give an authorization to any medical research.

No specific rules on the prior checking are provided by the PDPA.

6. Transfer of Data to Third Countries

According to Article 62 of the PDPA the transfer of data to third countries is subject to the same conditions listed in Article 25 and 26 of the Directive.

3.4.26 SPAIN

Spain has implemented the Directive 95/46/EC amending the Ley Organica n. 5/1992 (LO). Hence, currently the personal data protection regulation is provided for by the Ley Organica n. 15/1999.

The English version of the LO is available at: https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf

1. Personal Data and Anonymyzation

According to Article 3 of the LO personal data is any information concerning an identified or identifiable natural persons.

Once the data have been rendered anonymous they cannot be considered personal, therefore the LO does not apply.

Article 3(f) of the Ley Organica defines the dissociation procedure (anonymization) as "*any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person*".

2. Medical Research

2.1 implementation Article 8.3 of the Directive

Article 7.6 of the Ley Organica implements Article 8.3 of the Directive and the medical research is not included in "preventive medicine and diagnosis".

Indeed, Act n. 41/2000 distinguishes as different interventions in the heath sector the preventive, diagnostic, therapeutic, rehabilitate, or research activities.

2.2 substantial public interest

The Spanish regulation on data protection does not stipulate an exemption to the prohibition of processing sensitive data based on substantial public interest grounds.

3. Consent

According to Article 7 of the LO personal data concerning health may be collected and processed " *only when, for reasons of general interest, this is so provided for by law or the data subject has given his/her explicit consent*".

However, it is allowed to process medical data without consent if: - it is necessary to protect the vital interests of the data subject or another person whereas the data subject is physically or legally incapable to give his/her consent; or, as seen above, - it is necessary for preventive medicine and diagnosis purposes and the processing is undertaken by a health professional subject to professional secrecy or by another person subject to equivalent obligation of secrecy.

LO does not explain the meaning of explicit consent, anyway, if the processing refers to sensitive data a written consent is required.

4. Duty of Information

The data subject must be informed about the purpose of the processing both where the data are obtained directly from the data subject than where the data are collected elsewhere.

According to Article 4.1 the data cannot be used in a way incompatible with the purpose of the collection. Since the further processing for the purpose of scientific research is not considered to be incompatible with the original purpose in such a case the duty to inform the data subject is removed.

Moreover, according to the LO when the data are processed for statistical, historical or scientific purposes the controller is not obliged to inform the data subject even though the information is not impossible nor requires a disproportionate effort.

This seems in contrast with Article 11 of the Directive.

5. Notification and Prior Checking

LO at Article 39 states an obligation to register the processing of personal data in the General Data Protection Register that is a body incorporated into the Data Protection Agency (Spanish Supervisory Authority). There are no special provisions concerning medical research.

No prior checking is provided for by the Ley Organica.

6. Transfer of Data to Third Countries

Transferring of personal data to a third country is not permitted if the country in question does not ensure an adequate level of protection. The Data Protection Agency must verify the adequateness of protection taking into account the nature of data and the other circumstances regarding the transfer.

Articles 34 of the LO stipulates some derogation to the prohibition substantially in the same terms of Article 26 of the Directive.

3.4.27 SWEDEN

The Directive 95/46/EC has been implemented in Sweden with the Personal Data Act n. 201/1998.
In the Swedish system the provisions of the DPA are not applicable where there are diverging provisions in another Act or Ordinance. Considering the significant number of Acts or Ordinances concerning data protection the coordination between different provisions is often difficult.
The English version of the DPA is available at:
http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf

1. Personal Data and Anonymyzation
According to Section 3 of Swedish DPA, every kind of information directly of indirectly referring to a living person is considered personal data. It does not matter if the person who processes the data has no access to the necessary information for the identification nor if the process of identification requires a considerable amount of time, money and other resources. Thus, the Swedish notion of personal data is very broad: also encoded data have to be considered personal data as long as someone retains the code key.
The process of anonymization constitutes processing covered by the DPA. This does not necessarily imply that: the data controller must obtain the consent of the data subject for an anonymization procedure not foreseen at the collection time or even to inform the data subject of such processing, unless the anonymization and the further processing is incompatible with the original purpose for which data were collected.

2. Medical Research
According to Section 18 of the DPA "sensitive personal data may be processed for health and hospital care purposes, provided the processing is necessary for a) preventive medicine and health care, b) medical diagnosis, c) health care or treatment, or d) management of health and hospital care services". Moreover Section 18 states that "A person who is professionally operational within the health care sector and is subject to a duty of confidentiality may also process sensitive personal data that is subject to the duty of confidentiality. This also applies to the person who is subject to a similar duty of confidentiality and who has received sensitive personal data from the operation within the health care sector".
While Article 8.3 of the Directive allows the processing of sensitive data where it is required for the purpose of preventive medicine or medical diagnosis and the processing is carried out by

a health professional subject to the obligation of professional secrecy, in the Swedish version the conjunction "and" has been transformed in "or". This seems imply that the processing of sensitive data for clinical purposes could be undertaken not only by health professional or other persons under an obligation of secrecy but also by persons not subject to a duty of secrecy.
The wrong interpretation of the Directive does not seem to have produced important consequences.
Even though Section 18 of the DPA does not explicitly cover medical research, some scholars take the view that medical research is included in Section 18 exemption. [E. Rynning, *Processing of Personal Data in Swedish Health Care and Biomedical Research*, in D. Beyleveld et al. (ed.) *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*, 2004: 389 ss].

2.2 substantial public interest

Section 19 paragraph 1 permits the processing of sensitive personal data for research and statistics purposes, if the processing is necessary and the interest of society in the research or statistics project is manifestly greater than the risk of improper violation of the personal integrity of the individual that the processing may involve.
This derogation to the prohibition to process sensitive data that refers to research as a whole and not only to medical research is based on substantial public interest grounds.
According to Section 19 paragraph 2, if the processing has been approved by a research ethics committee, the prerequisites under the first paragraph shall be deemed satisfied. Otherwise, if the controller wishes to operate the balance between different interests involved, he/she must notify the processing to the Data Inspection Board (DIB) for a prior checking under Section 10 of the Protection Data Ordinance.

3. Consent

In principle, personal data may be processed only with the data subject' informed consent. However, Swedish DPA provides for alternative conditions able to legitimate the processing of data without consent, even if consent would be practicable and not inappropriate.
The DPA does not requires consent to be given in writing, but the DIB recommends the data controller to prove that consent has been obtained.
There is a debate in Swedish legal literature over the possible different interpretation of "consent" and "explicit consent" as used in the Directive.

4. Duty of Information

Sections 23 and 24 of the PDA state that, the controller of personal data must provide the registered person with information about the processing of the data.
However, according to Section 24, where personal data has been collected from another source than the registered person, the information need not be provided if: - there are

provisions concerning the registration or disclosure of personal data in an act or some other enactment; - it proves to be impossible or would involve a disproportionate effort.
According to Section 27 of the PDA, a general derogation from the controller's duty to inform is provided for situations where it is specifically prescribed by a statute or other enactment or by a decision that has been issued under an enactment that information may not be provided to the data subject. Even if cases where personal data cannot be disclosed to the data subject are uncommon , one example can be found in the Secrecy Act. According to Chapter 7, Section 3 of the Secrecy Act information concerning a patient's state of health must not be disclosed to the patient if it is particularly important, with regard to the purpose of the care, that this information is withheld from the patient.
According to Section 9(d) of the PDA personal data may not be processed for any purpose that is incompatible with purpose of the data collection. When deciding the compatibility between the new purpose and the original one it is necessary to consider how the average data subject would typically regard the situation. If the data subject could reasonably be expected to anticipate the data being processed also for the new purpose, then this purpose cannot be considered incompatible with the original purpose.
Whereas the new purpose is not incompatible with the original purpose, of which the data subject has been duly informed, no further information or consent is required.

Where the data are not obtained directly from the data subject, the researcher may be interested to access information from individual medical records or from national health data registers
In such cases the access may be granted only in compliance with rules on secrecy and confidentiality (see Secrecy Act). Moreover, information about the state of health must not be disclosed unless it is clear that the disclosure will not cause any harm to the person concerned, or to his/her relatives.
There are some exceptions to the principle stated above but a general derogation regarding medical research does not exist.
The person or agency that parts with the information is responsible to verify that the necessary requirements are satisfied. The notion of harm must be considered from the data subject point of view. Determining whether or not disclosure for the intended research will clearly cause no harm may be required consultation with the patient.
Normally the disclosure of depersonalised data is not considered to be harmful and the data subject can waive the right of secrecy.

5. Notification and Prior Checking

The PDA provides for a general obligation to notify the data processing to the Data Inspection Board. However such notification is not required if: - the controller has appointed a data representative giving notice of this to the DIP; - the data subject has given his/her

consent to the processing; - the processing of personal data is within the health care sector in accordance with Section 18 of the PDA.
The aforementioned exemptions do not apply where a mandatory prior notice to the DIP is prescribed by the law. According to Section 41 of the PDA , Government may issue regulation concerning notification for prior checking of processing operations likely to present particularly risks to the personal integrity of the data subject. The notification for the prior checking must be given to the DIP no later than three weeks before the beginning of the processing.
Section 10 of the Data Protection Ordinance lays down two hypothesis of prior checking: - the processing of sensitive data for research purposes without the consent of the data subject and without the approval of an ethical committee; - the processing of personal data concerning hereditary disposition derived from genetic investigation.

6. Transfer of Data to Third Countries
Sections 33, 34 and 35 of the PDA substantially reproduce what is provided for by Articles 25 and 26 of the Directive for transferring personal data to a foreign country.

3.4.28 UNITED KINGDOM

The United Kingdom has implemented Directive 95/46/EC with the Data Protection Act 1998 (DPA). Some modifications have been introduced by the Freedom of Information Act 2000.
The Data Protection Act 1998 is available at:
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

1. Personal Data and Anonymyzation
According to Section 1(1) of the DPA personal data are "*data which relate to a living person who can be identified from those data or from those data and other information which is in the possession of, or it is likely to come into the possession of, the controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual*".
Whereas the data subject can be identified only indirectly from the data, the data are personal – thus covered by the DPA – only if the controller can do the identification.
Under this aspect the DPA is not completely in accordance with Directive that does not make a distinction on the basis of who can identify the data subject. Indeed, Directive seems to state that data remain personal if anybody can identify the data subject from it, directly or indirectly.
The DPA does not take explicitly into consideration the anonymization issue and currently in UK there is a debate whether it can be considered as processing of data falling under the scope of the Act. While the prevailing assumption is that DPA does not cover the

anonymization of data, the Information Commissioner (IC is the UK Supervisory Authority) has a different opinion/comes to different conclusions. Indeed, IC stated that: "in anonymising personal data the data controller will be processing such data and, in respect of such processing, will still need to comply with the provisions of the Act".
This contrast will have to be resolved in the Courts.

2. Medical Research

2.1 implementation of Article8.3 of the Directive

Schedule 3 paragraph of the DPA, like Article 8.3 of the Directive, removes the prohibition on the processing of sensitive data where the processing is for medical purposes and is undertaken by a heath professional or someone else operating under an equivalent duty of confidence. However, the DPA explicitly considers medical research as a medical purpose, unlike the Directive.

2.2 substantial public interest

Schedule 3 paragraph 10 empowers the Secretary of the State to specify by order the circumstances under which the prohibition on the processing of sensitive data is overcome.
The Data Protection (Processing of Sensitive Personal Data) Order 2000 n. 417 stipulates that the prohibition does not operate where processing is necessary for research purposes that are in substantial public interest and the "relevant conditions" of Section 33 of the DPA are satisfied, that is: - the data are not processed to support measures or decisions with respect to particular individuals, and - the processing is not likely to cause substantial damage or distress to any data subject.
Anyway, it is not clear what is in the "substantial public interest" and who can determine it.

3. Consent

According to Schedule 3 and Schedules 7 the DPA consent is one of the conditions that can remove the prohibition to process personal data (sensitive or no sensitive) but it does not seem to have priority with respect to the other conditions.
However, the Human Rights Act 1998 requires all UK legislation to be interpreted in compliance with the European Convention on Human Rights (ECHR) and according to Article 8(1) of the ECHR consent must be obtain for processing sensitive data.
The Information Commissioner stipulated that even though according to the DPA consent is not a necessary condition for the processing of medical data, the Act imposes the controller a duty to process the data lawfully.
This implies that health care information has to be subject to requirements of common law confidentiality. Moreover, consent has to be informed, freely given and an indication the individual has given his/her consent is required.

4. Duty of Information

Schedule 1, part 2, paragraphs 2 and 3 lays down the information that must be given to the

data subject in order to render the processing fair and lawful: - the identity of the data controller, or of his/her representative if any; - the purpose or purposes for which the data are intended to be processed; and – any further information which is necessary, having regard to the specific circumstances, to enable processing in respect of the data subject to be fair.
The information must be provided where data are obtained from the data subject as well as the data are obtained elsewhere. While the Directive provides for a derogation, whereas the information reveals impossible or would involve disproportionate effort, only in the second situation (collection of the data from a subject other than the data subject), according to the DPA also where data are obtained from the data subject the information must be provided only in so far as is practicable.
Therefore, under this aspect the UK regulation on data protection seems to be in contrast with the Directive.
Finally, the obligation to inform is removed where: information reveals impracticable; - the controller is legally bound to register or to disclose the data; there is a Secretary of the State order.

5. Notification and Prior Checking

If the data used for the medical research are "non-automated accessible records" there is no need to notify the processing to the Information Commissioner, otherwise, notification is required.
According to Section 22(2) of the DPA a prior checking is required for such processing specified by an order of the Secretary of the State to be particularly likely to cause substantial harm or distress to the data or otherwise significantly to prejudice the rights and freedom of data subject. However, no order has been issued yet.

6. Transfer of Data to Third Countries

According to Schedule 4 paragraphs 8 and 9, the rule that prohibits the transferring of data to a third country that does not provide for an adequate level of protection can be derogated if the transfer is made on terms or in such a manner that the IC approves or authorizes as ensuring adequate safeguards (generally contractual clauses).
The IC must inform the European Commission and other EEA States of authorizations/approvals granted.

3.5 EUROPEAN PROJECTS USING HEALTH INFRASTRUCTURE AND HEALTH GRID

In our revision on data protection aspects, that has the final aim to be the starting point for the development of a specific protocol on data protection for, it appeared useful to consider how other European projects, dealing with infrastructure and grid in the field of health, have treated privacy issues.
The protection of privacy in the context of health grid deserves a very specific regard for the technical specificity of the tool: the distributed nature of Grids and the fact that various actors are involved in Grid computing make the situation more complicated than in common data processing with regard to the treatment and control of personal identifiable information of the subjects.

In order to verify if issues related to data protection were taken into consideration and, eventually, to analyse the adopted politics and policies related to data protection issues in the recent projects funded by the European Commission, we performed a search in the CORDIS Information and Communication Technologies website http://cordis.europa.eu/fp7/ict/projects/home_en.html
We tried to access all the projects using grids and infrastructures in the field of health, with particular regard to the projects dealing with brain imaging.
We searched projects funded in FP7, FP6 and FP5 using the following enter search terms: health grid, heath infrastructure, biomedical grid, biomedical infrastructure, grid imaging and brain imaging.

In total we found 7 projects funded in FP7 and 31 projects funded in FP6. We didn't find any project within FP5 using the above mentioned key words.
We succeeded in finding the project website for the large majority (33) of the projects; for two projects funded in FP7 and one project funded in FP6 it was possible to have access only to the project abstracts through CORDIS website.
We found brief references to privacy in two projects (HEALTH-E-CHILD and LHP), one publication in another project (@neurIST) and a full consideration of data protection issues in three research projects (SHARE, ACGT, ARTEMIS) which also produced public deliverables on privacy issues. Among the five mentioned projects, SHARE has a theorical approach to healthgrid, while the other four projects aim to the development of concrete infrastructures.
We found only a very quickly reference to the specificity of the use of brain imaging in relation with data protection in @neurIST project, but without a proposal for solution.

At least through the reading of the projects website, it seems therefore that very few projects took into consideration data protection issues, even if privacy issues seems to be pertinent to many research projects. Nevertheless it is obviously possible that some projects dealt with data protection issues without quoted them in the web description of the research.
Probably for the majority of projects the solution of questions related to confidentiality and privacy of medical data were left to each project partner, instead of developing a common policy for the whole project.
This is the case of the two projects which are the basis for the development of neuGRID, i.e. ***MammoGrid/Health-E-Child*** and ***AddNeuroMed/InnoMed*** in which the rules for data protection of clinical data and imaging are ruled individually by every partner, according to the legal regulation of each country.
With regard to ethical aspects and confidentiality, the recent MammoGrid document "CREATING A NETWORK OF COLLABORATORS -Criteria for collaboration with the MammoGrid Consortium (MG)" states that "issues containing ethical implications, aspects related to confidentiality and to protection of sensitive information, shall be dealt with by the medical organizations of the MG, according to their respective legislations."

We will report below the CORDIS projects for which we found some references to privacy and protection of medical data in the project website, starting from the theorical approach of SHARE.

3.5.1 SHARE

Supporting and structuring Healthgrid Activities and Research in Europe

http://www.eu-share.org/

The SHARE project aims to define a roadmap for future healthgrid research across Europe.
Starting from the observations contained in the HealthGrid White Paper (2004), SHARE project has as main objectives: to set up a roadmap for research and technology to permit a wide deployment and adoption of healthgrids and to create a "complementary and integrated roadmap for e-Health research and technology development (RTD) policy relating to grid deployment, as a basis for improving coordination amongst funding bodies, health policy makers and leaders of grid initiatives, avoiding legislative barriers and other foreseeable obstacles."

Privacy

Within the SHARE project three of the deliverables currently available on the website take in consideration the data protection issue, in particular: deliverable D4.1 "Baseline on legal, ethical, social, and economic aspects of healthgrids"; deliverable D4.2 "Bottlenecks & challenges and RTD responses for legal, ethical, social, and economic aspects of healthgrids

roadmap I" and deliverable D4.3 "Legal, social & economic challenges component roadmap II".
Since the goal of the present work is to supply a review document on data protection - in the light of Data protection Directive, national acts of implementation and previous European researches dealing with the data protection question - the other legal aspects such as product liability and IP rights protection as well as ethical and socio-economic issues analysed by SHARE project will not be taken into account.

The Share project analysis on confidentiality and data protection issues connected with the use of healthgrids starts from a Directive 95/46/EC overview focusing on the most crucial provisions: personal data notion, data controller's duties, different treatment of personal data (sensitive and no sensitive), data subject's rights and transfer of data towards other countries (inside and outside the European Union and European Economic Area).
From the point of view of the Share project, Directive imposes certain heavy burdens on the data controller hardly compatible with research needs and development of heathgrids. To meet the requirements of the Directive may prevent the use/share of data concerning health using grid technology.
According to SHARE, taken into account the specificity of the grid tool an *ad hoc* regulation concerning the healthgrid context in order to balance the individual interest to data protection with the medical research interest is needed.
The legal instrument could be, in the European context, the adoption of national legislation providing for a derogation to the strictly obligations imposed by the Directive in favour to the research.
The link between the data protection principles set out in the Directive and their application to a E-Infrastructure is in deep explored in Deliverable 4.2 (in particular in Annex I: data protection, confidentiality and security issues). In particular, the major risks for the data subject's rights and liberties due to the establishment of a telematic network are investigated.
As seen above, according to the Directive 95/46/EC the controller has to perform a set of duties in order to ensure the fair and lawful processing of the data, therefore the networks hosting data processing must be adapted in terms of confidentiality and security.
Finally, in the third deliverable (D4.3) the data protection issues are considered with reference to two different use case scenarios pointing out the problems which may arise in connection with the application of data protection principles.
The first use case taken into account is epidemiology defined as "the scientific study of factors affecting the heath and illness of populations". According to the SHARE project in the epidemiological field the data subject's consent is not the best way to legitimate the processing of his/her data. Indeed, consent is subject to strict conditions for its validity and may be revoked at any time. Since a valid consent needs to be given for a specific purpose probably it would not be the preferable solution for epidemiological researches in order to comply with requirements.

From the point of view of the Share project, the legitimization to process data related to health in the epidemiological study context would be found in "the substantial public interest" in accordance with Article 8.4 of the Directive. However, the processing of sensitive data on public interest grounds requires to be included in a specific provision/ regulation enacted by the national legislator.
The further use case considered is that one of innovative medicine defined as "treatment or therapy of empirical benefit that is still outside of the mainstream of conventional medicine".
Since the SHARE focus in this case is at the *in silico* phase of drug development, no personal data referring to a specific subject are processed. Therefore, the data protection issues were not deemed appropriate.
SHARE conclusion on data protection topic is that: "EU-level legislation on data protection is adequate but not ideal for promoting healthgrids. When healthgrids are used for treating patient or planning care, the requirements of the legislation provide that, if the data are collected and processed by medical professionals, the balance of rights weights in favour of data collection.
The current legislation is not, however, adequate to support most of the longer running initiatives around which healthgrids are based".

3.5.2 ACGT

Advancing Clinico-Genomic Trials on Cancer

http://www.eu-acgt.org/

The ACGT project aims to develop open-source, semantic and grid-based technologies in support of post genomic clinical trials in cancer research.

Privacy

As far as data protection issue is concerned, the deliverable 10.2 "the ACGT ethical and legal requirements" partly deals with the legitimate processing of data, in particular genetic data.
After a brief overview on Data Protection Directive 95/46/EC the deliverable provides for specific rules for the protection of the data within ACGT project in order to ensure the fair and lawful collection and storage of patients' data as well as the exchange of these data among the researchers participating in the project.
AGCT project proposes its own "Data Protection Architecture" to guarantee the compliance of AGCT with the data protection regulation.
First of all, AGCT suggests the set up of one central controller for the whole project who would be responsible for the compliance of ACGT with the data protection principles stated in Directive 95/46/EC, instead of several data controllers. The other participants would have to be regarded as data processors who actually processed the data. The AGCT suggestion is to

establish a Data Protection Board as a legal body: it should be the central data controller also competent to sign binding agreements and contracts regarding data protection issues. Moreover, the ACGT proposal includes an independent Trustee Third Party (TTP) that would support the central controller and be responsible for the second pseudonymization of the data and the protection of the links.
Indeed, in the ACGT system patients' data are collected in local hospitals which provide for the first pseudonymization, then it is a duty of the Trustee Third Party to anonymize de facto these data. In particular, the TTP has to render the data anonymous for the ACGT researcher but at the same time it has to enable the de-anonymization of the data in order to identify the concerned patient so that he/she can benefit from the research results.
In AGCT view the TTP must be the only party able to link the second pseudonym with the first one given by the hospital. According the AGCT project the TTP should provide a software tool which could perform the second pseudonymization and the sending of data from the hospitals to the TTP.
Moreover, since the data used in ACGT research are genetic data containing information about the patient but also of his/her relatives the possibility that the privacy of the latter may be affected by the processing of the data of the former has been considered. The conclusion on this issue is that only when additional information regarding patient's relatives is collected together with the genetic data of the patient, consent of relatives is needed but just of first-grade relatives as long as only their data sets contain enough similarities to the data set of the patient.

3.5.3 ARTEMIS

A Semantic Web Service-based P2P Infrastructure for the Interoperability of Medical Information Systems

http://www.srdc.metu.edu.tr/webpage/projects/artemis/

Considering that the inability to share patient records across enterprises is a key problem in healthcare informatics , one of the main objectives of ARTEMIS project is to develop the infrastructure necessary to make medical information systems interoperable based on the Web services.

Privacy

Because of resolving non-functional service requirements such as security and privacy are considered essential for interoperation, ARTEMIS proposes a specific technical approach for mediating between security and privacy policies.
The ARTEMIS global approach starts from the awareness that for the communication to occur between data controller (a healthcare provider who maintains personal data on its patients and is therefore responsible for protecting that data against unauthorised use) and data processor (a healthcare provider who wants to access personal data within another

organization) a consent must be obtained from the patient and a contract between the two parties must exist that defines conditions such as the type of data processing and how long the data can be stored by the data processor. ARTEMIS approach also considers that in most cases healthcare providers have different security policies that state a diverse set of security requirements and capabilities, and that authentication and authorisation mechanisms for healthcare professions may also be different.

ARTEMIS technical architecture starts after the out-of-bound legislative conditions for data processing (patient's consent and contract between the parties) have been agreed, considering that there are still technical challenges in terms of security and privacy mechanisms that need to be resolved before electronic healthcare records can be automatically shared between healthcare information systems.

The core requirement in ARTEMIS – as it is stated in the project publications - is for very robust, but highly flexible approach to security and privacy: an approach has been developed for mediating between different organizations security and privacy policies using a combination of industry supported web service standards and reasoning over semantics web service descriptions. The approach supported by ARTEMIS allows healthcare providers to codify their particular preferences and requirements for data security (confidentiality, integrity) and privacy (authorisation and anonymization) in accordance with overarching organisational security policies. Based on these, Artemis enables the communication of medical data across healthcare provider boundaries through mediation between semantic security and privacy policies on the condition that out-of-bound contracts and patient consent has been agreed. The initial authorisation infrastructure allows access control based on mediation between clinical roles defined by different organisations. In fact, in ARTEMIS, healthcare providers define privacy policies that state which healthcare professionals are able to access specific medical data.

The technical details of the ARTEMIS architecture for security and privacy, is available in the Artemis publication: Mike Boniface, Paul Wilken, "ARTEMIS: Towards a Secure Interoperability Infrastructure for Healthcare Information Systems", Stud Health Technol Inform. 2005; 112:181-9; and in the Artemis Deliverable 4.4.1 "Security and Privacy mechanisms for Web services".

3.5.4 @neurIST

Integrated Biomedical Informatics for the Management of Cerebral Aneurysms

http://www.cilab.upf.edu/aneurist1/index.php?option=com_frontpage&Itemid=1

@neurIST is focused on cerebral aneurysms and intends to provide an integrated decision support system to assess the risk of aneurysm rupture in patients and to optimize their treatments. @neurIST aims to provide an IT infrastructure for the management, integration and processing of data associated with the diagnosis and treatment of cerebral aneurysm and subarachnoid haemorrhage.

Privacy

The project website reports one publication dealing with security and privacy issues: J. Fingberg, M. Hansen, M. Hansen, H. Krasemann, L. Lo Iacono, T. Probst, and J. Wright (2006). *Integrating Data Custodians in eHealth Grids - A Digest of Security and Privacy Aspects*. Proceedings of Informatik 2006 - Informatik für Menschen, Lecture Notes in Informatics, vol. P-93, pp. 695-701.

As the authors speak in general terms about grids security and privacy aspects, it is not really clear if the proposed solution for the protection of privacy is the one adopted in the project itself.

The background of the document is the awareness that medical practitioners sending information to the Grid have a duty of confidentiality towards their patients and that the patients have the right to informational privacy so that patients should be informed about and allowed control over the processing of their own information.

The authors believe that, in the context of GRIDs, the solution of getting the consent of the subject to process his/her personal identifiable information is questionable (in the sense that it is not enough), because this would require that the subject really fully understands the risks related to the realization of the health grid. While the understanding of a single research project or of a short-term research project can be quite easy realized, it is difficult for the subject to understand the impact of the new Grid technologies and the possible future uses of his/her data, despite them being known at the time of the collection. It is also questionable how it can be assured that the subject personal data are used solely for the agreed purposes and that the subject does not lose the control of their data in the Grid context.

Starting from these considerations and to overcome these problems the main suggestion for the protection of privacy is the identification of a third party as a custodian.

The custodian is understood "as an independent and trustworthy third party taking care of provided data (possibly including software and configuration data), processing them in an agreed-upon manner, ensuring that provided data are used only for the agreed-upon purpose in the agreed-upon time period, are not forwarded to unauthorised parties, and are protected from external and internal attacks".

Several tasks have been identified for the custodian. Such as to (reversibly) detach personal identifiable information from the data for the duration of the processing (through: pseudoanonymization; segmenting of the computational tasks and processes and dispatching them in a way that the tasks reveal no personal information; pre and post-processing of computational tasks in a way that the remaining data cannot reveal personal identifiable information). Another task for the custodian is to offer a trustworthy archive for the huge data amounts which may occur in Grid computing. Even if the mentioned tasks can be executed also by the hospital itself or by a data processor on behalf of the hospital, the custodian is considered a better solution because the custodian would be a security and privacy expert and so could guarantee a better service, would be independent and so

could help to overcome possible internal conflict in the hospital. Furthermore a custodian serving multiple hospitals can simplify and thereby cheapen the transmission of pseudoanonymized or anonymized data for research purposes among research institutions.
As we said, the paper contains a quickly reference to the specificity of the use of brain imaging data, even if it is not reported a solution of the problem: "while reliably removing the link from personal identifiable information to the related patient is relatively easy with most alphanumeric data, it is impossible with, e.g., biometric data such as a tomographic scan of a head, where the whole set of "slices" allows for computation of a 3D model making the person identifiable", so that just removing the name from the data does not make them anonymous.

3.5.5 HEALTH-E-CHILD

An integrated platform for European paediatrics based on a Grid-enabled network of leading clinical centres

http://www.health-e-child.org

The Health-e-Child project aims at developing an integrated healthcare platform for European paediatrics, providing seamless integration of traditional and emerging sources of biomedical information. The long-term goal of the project is to provide uninhibited access to universal biomedical knowledge repositories for personalised and preventive healthcare, large-scale information-based biomedical research and training, and informed policy making.

Privacy

The annual report on ethical and legal issues (deliverable D3.2) declares attention to privacy issues particularly in the elaboration of the informed consent forms developed for the project, in which together with the description of design, purpose and additional risk of the study, privacy issues related to data management and the modalities to guarantee the patients privacy have been explained. Informed consent forms are not available on line.
All the measures to protect the privacy of the patients involved in the study are assured by the local sites in accordance with national and local regulations.
For the collection of biological samples, it is reported that samples are anonymized in order to allow sample and information sharing for research purpose using standardized anonymization techniques, and demographic and clinical data attached to anonymized samples are coded with international nomenclature.

3.5.6 LHP

Living Human Project

www.livinghuman.org/

Living Human Project (LHP) aims to develop a worldwide, distributed repository of anatomo-functional data and of simulation algorithms, fully integrated into a seamless simulation environment and directly accessible by any researcher in the world.

Privacy

A very brief reference to privacy is present in the Consensus Document of the Workgroup BioNet_VRLab linked to LHP. The document states that "the most important [challenge] is probably, as in any community, the need for establishing a body of rules for the management of the community itself. Again, for each specific aspect (quality control, sharing policies, the respect of general rules such as patient's privacy, etc.) the challenge will be to strike the proper balance between control and openness".

Taking this statement seriously, we have to suppose that unified strict rules for data protection have been developed or will be developed for the project. Nevertheless, it was not possible to find something more on the topic in the project website.

4. CONCLUSIONS

The present revision will be the basis for the development of the data protection protocol and procedures to be used within the neuGRID project. We performed a revision of privacy and data protection issues in the European context. The revision was aimed to the development of a specific and unified protocol for data protection that needs both to be in line with local and national regulations and to comply with health Grid data protection requirements. We took into consideration the *Directive 95/46/EC* and its implementation in the Member States, with particular regard to the previsions related to biomedical research.

The two major questionable points in the implementation of the Directive by Member States was related to the priority of the informed consent of the person concerned over other conditions in view of the treatment of his/her sensitive data and to the concept of anonymization. Anyway, differences among national legislations on data protection are not such to prevent the possibility of a common protocol on privacy issues. We also took into consideration the research projects funded by the European Commission in the last three Framework Programmes dealing with infrastructures and grids in the field of health. Only for two projects the procedures adopted for data protection were clearly described in the official project website.

BIBLIOGRAPHY

International sources:

- Charter of Fundamental Rights of the European Union (2000/C 364/01)
- Convention for the Protection of Human Rights And Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo, 1997); Additional protocol to the Convention on Human Rights and Biomedicine, concerning biomedical research (Strasbourg, 2005)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is in Europe the specific legal tool aimed to give common rules to member states on privacy issue
- European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 1950)
- Universal Declaration of Human Rights (Paris, 1948)

National legislations (in alphabetical order):

- Austria: Datenschutzgesetz 2000; http://www.dsk.gv.at/dsg2000e.htm
- Belgium: Royal Decree 13 February 2001; http://www.law.kuleuven.ac.be/icri/itl/12privacylaw.php
- Bulgaria: Data Protection Act of 21 December 2001; http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/bg_data_protection_law_en.pdf
- Cyprus: Processing of Personal Data Law 2001; http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/138(I)-2001_en.pdf
- Czech Republic: Data Protection Act n. 101 of 2000; http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/czech_republic_act_101_en.pdf
- Denmark: Act on Processing of Personal Data n. 429 of 2001; http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/
- Estonia: Personal Data Protection Act 2001; http://www.legaltext.ee/text/en/X70030.htm
- Finland: Personal Data Act (Law 471/1987 as amended by Law 523/1999); : http://www.tietosuoja.fi/uploads/hopxtvf.HTM
- France: Law n. 801/2004; http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676&dateTexte=
- Germany: Bundesdatenschutzgesetz 2001; http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf

- Greece: Law n. 2472/1997; http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL
- Hungary: Act n. LXIII 1992 on Protection of Personal Data and Disclosure of Data of Public Interest as amended by Act n. XIX 2005; http://abiweb.obh.hu/dpc/index.php?menu=gyoker/relevant/national/1992_LXIII
- Ireland: Data Protection Act 2003; http://www.dataprotection.ie/images/Act2003.pdf
- Italy: Personal Data Protection Code 2003; : http://www.garanteprivacy.it/garante/doc.jsp?ID=311113
- Latvia: Personal Data Protection Law 2000 (as amended in 2002 and 2006); http://www.dvi.gov.lv/eng/legislation/pdp/
- Lithuania: Law on the Legal Protection of Personal Data 2003; http://www.ada.lt/images/cms/File/pers.data.prot.law.pdf
- Luxembourg: Data Protection Law 2002 (as amended in 2007); http://www.cnpd.lu/fr/legislation/legis_nationale/index.html
- Malta: Data Protection Act 2001; http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/malta_en.pdf
- The Netherlands: Wet Bescherming Persoonsgegevens 2000; http://www.dutchdpa.nl/downloads_wetten/wbp.pdf?refer=true&theme=purple
- Norway: Personal Data Act 2001; http://www.datatilsynet.no.htest.osl.basefarm.net/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf
- Poland: Act on the Protection of Personal Data of 1997 (as amended in 2004); http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/poland_en.pdf
- Portugal: Law n. 67 /1998; http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM
- Romania: Law n. 677 /2001; http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/ro_law_677_2001_en_unofficial.pdf
- Slovakia: Protection of Personal Data Act n. 428/2002 (as amended in 2003, 2004 and 2005); http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/slovakia_428_02_en.pdf
- Slovenia: Personal Data Protection Act 2004; http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf
- Spain: Ley Organica n. 15/1999; https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf
- Sweden: Personal Data Act n. 201/1998; http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf
- United Kingdom: Data Protection Act 1998; http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

European Commission websites:

- http://ec.europa.eu/justice_home/fsj/privacy
- http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm
- http://cordis.europa.eu/fp7/ict/projects/home_en.html

European Research Projects (in alphabetical order):

- ACGT: http://www.eu-acgt.org/
- ARTEMIS: http://www.srdc.metu.edu.tr/webpage/projects/artemis/
  Mike Boniface, Paul Wilken, "ARTEMIS: Towards a Secure Interoperability Infrastructure for Healthcare Information Systems", Stud Health Technol Inform. 2005; 112: 181-9
- @neurIST:
  http://www.cilab.upf.edu/aneurist1/index.php?option=com_frontpage&Itemid=1
  Fingberg J, Hansen M, Hansen M, Krasemann K, Lo Iacono L., Probst T, Wright J.2006. Integrating Data Custodians in eHealth Grids - A Digest of Security and Privacy Aspects. Proceedings of Informatik 2006 - Informatik für Menschen, Lecture Notes in Informatics, vol. P-93: 695-701
- HEALTH-E-CHILD: http://www.health-e-child.org
- LHP: www.livinghuman.org/
- PRIVIREAL: http://www.privireal.org
  Beyleveld, D. Townend, S. Rouillé-Mirza, J. Wright (ed.). 2005. The data Protection Directive and Medical Research Across Europe
  D. Beyleveld, D. Townend, S. Rouillé-Mirza, J. Wright (ed.). 2004. Implementation of the Data Protection Directive in Relation to Medical Research in Europe.
- SHARE : http://www.eu-share.org/