

INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME



SENSATION

507231

Data Security and Privacy: Guidelines and European Roadmap

Deliverable No. (use the number indicated on technical annex)		D2.7.1	
SubProject No.	SP2	SubProject Title	Micro and Nano sensors development
Workpackage No.	WP2.7	Workpackage Title	Embedded Connectivity
Activity No.	A2.7.4	Activity Title	Data Security and Privacy
Authors (per company, if more than one company provide it together)		Rodrigo Díaz; Pepa Sedó (Atos Origin) Eduardo Montón (ITACA)	
Status (F: final; D: draft; RD: revised draft):		F	
File Name:		SENSATION D2_7_1 Final.doc	
Project start date and duration		01 January 2004, 48 Months	

List of Abbreviations

ACL	Access Control List
ATM	Automatic Teller Machine
CLI	Connected Line Identification
CNIL	Commission Nationale de l'Informatique et des Libertés
EC	European Council
EEA	European Economic Area
EU	European Union
PETs	Privacy Enhancing Technologies
PIN	Personal Identification Number

Table of Contents

<i>Chapter/Section</i>	<i>Page</i>
1 EXECUTIVE SUMMARY.....	6
2 INTRODUCTION.....	7
2.1 GLOSSARY.....	7
3 MAIN CONCEPTS ON DATA PRIVACY AND SECURITY.....	9
3.1 CONFIDENTIALITY.....	9
3.2 INTEGRITY.....	9
3.3 AVAILABILITY.....	9
3.4 NON-REPUDIATION	9
3.5 AUTHENTICATION	9
3.6 AUTHORIZATION	10
3.7 ACCOUNTABILITY	10
3.8 ANONYMITY.....	10
4 CURRENT EUROPEAN RELATED LEGISLATION	11
4.1 EUROPEAN DIRECTIVES	11
4.1.1 <i>Data Protection Directive (95/46/EC)</i>	11
4.1.2 <i>Electronic Communications Data Protection Directive (2002/58/EC)</i>	19
4.1.3 <i>EU Recommendation on the Protection of Medical Data</i>	22
4.2 MEMBER STATES SPECIAL FEATURES	23
4.2.1 <i>The scope of the national laws (Article 3)</i>	23
4.2.2 <i>National laws applicable (Article 4)</i>	23
4.2.3 <i>Data quality (Article 6)</i>	25
4.2.4 <i>Data processing lawful (Article 7)</i>	26
4.2.5 <i>Special categories of processing (Article 8)</i>	27
4.2.6 <i>Data protection and freedom of expression (Article 9)</i>	31
4.2.7 <i>Information to be given to the data subject (Articles 10 and 11)</i>	31
4.2.8 <i>The data subject's right of access to data (Article 12)</i>	32
4.2.9 <i>Exemptions and restrictions (Article 13)</i>	34
4.2.10 <i>The data subject's right to object (Article 14)</i>	35
4.2.11 <i>Automated individual decisions (Article 15)</i>	35
4.2.12 <i>Confidentiality and Security of processing (Article 16 and 17)</i>	36
4.2.13 <i>Notification and publicising (Articles 18-21)</i>	37
4.2.14 <i>Juridical remedies, liability and sanctions (Articles 22, 23, and 24)</i>	39
4.2.15 <i>International Transfers of Personal Data (Articles 25)</i>	39
4.2.16 <i>International Transfers of Personal Data, Exceptions and Derogations (Article 26)</i>	41
4.3 SUMMARY TABLE.....	42
5 GUIDELINES AFFECTING SENSATION	45
5.1 GUIDELINES AFFECTING SENSATION APPLICATIONS	47
5.2 GUIDELINES AFFECTING SENSATION COMMUNICATIONS.....	49
5.3 SECURITY RISK ANALYSIS	51
6 CONCLUSIONS.....	52
7 REFERENCES	53

List of Figures

Figure 1: The SENSATION embedded connectivity module layout 50

List of Tables

Table 1: Member States Legislation..... 44

1 EXECUTIVE SUMMARY

The main EU Directives affecting the SENSATION project in terms of security and privacy are: the EU Data Protection Directive (95/46/EC) and the Electronic Communications Data Protection Directive (2002/58/EC). The first Directive objective is to allow the free flow of personal data between Member States by harmonising the level of adequate protection granted to individuals. It sets forth the applicable law, conditions for data processing, information to be given to the data subject, the latter's right of access, object, confidentiality and security of processing, obligation of notification and content of such notification, as well as the limitations to the transfer of data to third countries imposed within the harmonised scope. The second Directive is designed to “particularise and complement” the Data Protection Directive (95/46/EC). It aims to ensure that all EU Member States apply equivalent levels of privacy protection regarding the processing of personal data in the electronic communications sector while ensuring that the free movement of data or equipment, or the provision of services in the EU is not obstructed.

Due to SENSATION is also focused in personal, industrial and medical environments, the EU Recommendation on the Protection of Personal and Medical Data has been considered in order to prepare the security and privacy guidelines affecting SENSATION Applications and Communications.

The main conclusions extracted from the analysis of the EU Privacy Directives, EU Recommendations and some national laws are that medical data are considered, in the EU Directive and in the national laws, as data that requires a high level of security in order to guarantee the patients care and their case history privacy. So, all electronic systems that process medical data shall incorporate strong security mechanism at communications and application level to guarantee the Medical and Personal data privacy. Data encryption is mandatory at all levels (databases, temporary files, communications, etc.) and it is also recommended anonymise data (with no possibility to identify people). Authentication mechanism shall be also included in the Communications and Applications, to identify correctly authorized users (sensors and applications in case of communications). Profiles are also required in order to implement users selective access to data. Any access to sensitive personal data shall be audited to check and establish, a *posteriori*, who has accessed to data and whom and what personal data have been processed and when.

2 Introduction

Security and privacy are often discussed together. Though they are related, they are really quite separate concepts. Privacy is a fundamental right recognised in all major international treaties and agreements on Human Rights and in constitutions of nearly every country in the world, either explicitly or implicitly. With the upcoming information technology and its controlling potentials on data, the mere recognition of a constitutional principle of privacy in general appeared to be insufficient to safeguard effectively the growing need to protect the right of privacy, with regard to processing of personal data. This is reflected in the most recently drafted constitutions that include specific rights to access and control of one's personal information. Security, on the other hand, is any number of practices and processes that respond to threats against a company's or government's ability to function. Only one such function is carrying out privacy obligations. The relevance of security to privacy is that a business or government lacking proper security may violate its privacy commitments.

The aim of this document is to collect all European Directives that can affect to the SENSATION project in terms of Security and Privacy, analyse how these Directives have been implemented in EU Members by national laws, and establish security and privacy guidelines and recommendations for the SENSATION Communications/Applications design and implementation. This document is contained inside the WP2.7 "Embedded Connectivity" and it contributes to this WP establishing the security requirements extracted from the EU Directives applicable mainly to the SENSATION Communications (BAN, LAN and WAN networks). In addition, some findings can be also applicable to the SENSATION Applications to be developed in the SP3 y SP4. Application designers and developers can find useful information regarding both the general legislation in Security and Privacy issues in the European countries where the applications will be implanted, and the implications of applications where personal and medical information has to be transferred between different countries. More specific information about security and privacy to bear in mind by the application designers can be found in the guidelines and recommendations above mentioned.

The document is structured in the following six main sections:

- This Introduction, providing an overview of the entire document- including a glossary of main terms.
- A Concepts section, describing the main key concepts to allow following the whole document contents.
- A European Legislation section, summarizing the main European Directives that can affect to SENSATION and how these directives are implemented in Member States laws.
- A Guidelines section, introducing security and privacy guidelines that shall be borne in mind before SENSATION Applications and Communications design.
- A Conclusions section, summarising all conclusions extracted from this document.
- A Reference section, containing references to other applicable documents.

2.1 Glossary

This glossary wants to define the terms employed in the different directives that are mentioned in the current document.

Personal Data

Any information relating to an identified or identifiable natural person.

Processing of personal data

Operations 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.

Filing System

Any structured set of personal data, which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Controller

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/her nomination may be designated by national or Community law.

Processor

Natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Third party

Natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

Recipient

Natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

Data subject

Individual whose data are being processed.

The data subject's consent

Shall mean any freely given specific and informed indication of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed.

3 Main concepts on data privacy and security

This chapter includes some privacy and security concepts useful to follow the current document.

3.1 Confidentiality

Confidentiality refers to limiting information access and disclosure to the set of authorized users, and preventing access by or disclosure to unauthorized ones. Authentication methods that identify systems users, and access control mechanisms that limit each user's use, underpin the goal of confidentiality.

3.2 Integrity

Integrity refers to the trustworthiness of information resources. It includes the concept of "data integrity" -- namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity. It also includes "origin" or "source integrity" -- that is, that the data actually came from the person or entity you think it did, rather than an imposter.

Integrity can even include the notion that the person or entity in question entered the right information -- that is, information that reflected the actual circumstances (in statistics, this is the concept of "validity") and that under the same circumstances would generate identical data (what statisticians call "reliability"). On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.

3.3 Availability

Availability refers, unsurprisingly, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure. An unreliable system makes users nostalgic for the days of paper records.

Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate). While the relative risks associated with these categories depend on the particular context, the general rule is that humans are the weakest link.

3.4 Non-Repudiation

The ability to reassure the sender and receiver can not deny involvement in a transaction. For security services, this usually requires the use of a digital signature and a secure digital timestamp, to establish the identity of the signer and when it was signed.

3.5 Authentication

Authentication refers to the process of verifying the identity of a user. Authorization refers to the process of establishing and enforcing a user's rights and privileges to access specified resources. Encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

Authentication answers the question, "Are you who you say you are?" It is a means of establishing the validity of a claimed identity to the system, which becomes the basis for

individual accountability. There are three means of authenticating a user's identity, which can be used alone or in combination:

- validating something the individual knows (e.g., a password, a Personal Identification Number (PIN), or a cryptographic key);
- validating something the individual possesses, referred to as a "token" (e.g., an ATM card or a smart card);
- validating something the individual "is", referred to as a "biometric" (e.g., fingerprints or voice patterns).

3.6 Authorization

Once authenticated, logical access controls are utilized to authorize and enforce a user's access to and actions towards specified resources. This authorization may be based on identity, roles (e.g., data entry clerk, administrator, supervisor) location, time, types of transactions, service constraints (e.g., number of concurrent users), access mode (e.g., read, write, delete), or a combination of these criteria. Both internal authorization safeguards (such as Access Control Lists) and external controls (such as secure gateways/firewalls) can be deployed. Another mechanism that can be used for strong access control is encryption, whereby encrypted information can only be decrypted by those possessing the appropriate cryptographic key.

3.7 Accountability

All requests for and access granted to stored information must be logged for review and possible investigation. Logging should include such items as a date/time stamp, the identification of the user, the type of access, e.g., create, read, modify, delete, the success or failure of the request, and identification of the data acted upon.

The accountability function must be protected by the system access control mechanism. In this way the system can manage need-to-know and need-to-do of users attempting to access the audit record, and to prevent changes and deletions. It needs to have the same robustness and non-bypassability as other security mechanisms.

Accountability needs to be coupled with specific policies and procedures in order for the data collected in the audit trail to be of any use.

3.8 Anonymity

Anonymity refers to the ability to engage in activity on a system (for example on the Internet, such as emailing, surfing, or posting to newsgroups) in such a manner that no one can determine who you are or practically any other nontrivial information about you.

4 Current European related legislation

4.1 *European directives*

In Europe, there is a broad consensus that data protection principles should be embodied in comprehensive law, applicable to all sectors of economy and providing the possibility for non-compliance to be sanctioned and for individuals to be given a right of redress. Such laws have incorporated additional procedural mechanisms, such as the establishment of independent supervisory authorities with monitoring and complaint investigation functions. The same approach has been followed in the EU Data Protection Directive and the Electronic Communications Data Protection Directive, both summarized in the next chapters.

4.1.1 Data Protection Directive (95/46/EC)

On October 24th, 1995, the Council and Parliament of the European Union adopted the 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 ("data protection directive").

A key objective of the data protection Directive was to allow the free flow of personal data between Member States by harmonising the level of adequate protection granted to individuals. The Directive sets forth the applicable law, conditions for data processing, information to be given to the data subject, the latter's right of access, object, confidentiality and security of processing, obligation of notification and content of such notification, as well as the limitations to the transfer of data to third countries imposed within the harmonised scope.

A great value has been placed in the individual's consent, as well as his/her entitlement to full and fair information on the collection and use of personally identifiable data, the right to access and correct such data, and the right to oppose the use or distribution of such data for marketing purposes.

Besides, the Directive encourages the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions.

The Directive also requires that any third country to which data are transferred provide "adequate" data protection. Such requirement has been the reason for a delay on its entry into force and the undertaken of negotiations with the US leading to the current "safe harbor" proposal.

The Directive has been complemented by Directive 97/66 (of 15 December 1997) on the protection of personal data in the field of telecommunications, latterly replaced by the Electronic Communications Data Protection Directive (2002/58/EC).

4.1.1.1 Scope (Article 3)

The directive limits the scope of its application to the processing of personal data wholly or partly by automatic means, and to the non-automatic processing of personal data which form part of a filing system or are intended to form part of a filing system.

4.1.1.2 National law applicable (Article 4)

A controller of personal data processing will be subject to the national law of the Member State where:

- the processing is carried out in the context of the activities of his/her establishment on the territory of the Member State. If the same controller is established on several Member States, each of his/her establishments should comply with the national law applicable;

- the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
- the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community. In this case, the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself/herself.

4.1.1.3 General Rules on the lawfulness of the processing of personal data (Article 5)

The directive establishes the conditions under which the processing of personal data is lawful. Such conditions are grouped in three categories: those related to data quality, those related to making data processing legitimate and those related to the special categories of processing.

The processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression will be exempted of these conditions to the extent that such conditions must comply with each Member State's rules regarding freedom of expression.

Principles relating to data quality (Article 6)

The controller will be obliged to make sure that personal data is:

- processed fairly and lawfully;
- 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,
- adequate, relevant and not excessive in relation to such purposes,
- 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;
- 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)

The data may only be processed if one of the following conditions is met:

- the data subject has unambiguously given his/her consent,
- 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,
- processing is necessary for compliance with a legal obligation to which the controller is subject,
- processing is necessary in order to protect the vital interests of the data subject,
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Special Categories of Processing (Article 8)

- Processing of personal data will be forbidden if revealing or concerning: racial or ethnic, origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

UNLESS any of the following takes place:

the data subject has given his/her explicit consent to the processing of those data, except where the laws of the Member State provide that the consent will not lift the prohibition,

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 authorised by national law providing for adequate safeguards,

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/her consent,

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,

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.

- Besides, processing of data within the forbidden categories will be EXCLUDED of such prohibition when it is undertaken: for the purpose of preventive medicine, for the purpose of medical diagnosis, for the purpose of the provision of care or treatment, for the purpose of management of health-care services, by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy, by another person also subject to an equivalent obligation of secrecy.

Member States may, for reasons of substantial public interest, lay down additional exemptions by national law or by decision of the supervisory authority.

- Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards.

However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

4.1.1.4 Information to be provided to the data subject (Articles 10 and 11)

Whether the data has been obtained from the data subject or not, the controller or his/her representative must provide a data subject with at least the following information related to himself/herself, except where he/she already has it:

- a) the identity of the controller and of his/her 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, when the data has been obtained from the data subject,
- the categories of data concerned, when the data has not been obtained from the data subject.
- the existence of the right of access to and the right to rectify the data concerning him/her 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.

EXCEPTION: However, this shall not apply when the data have not been obtained from the data subject and 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. Such is the case of data processing for statistical purposes or for the purposes of historical or scientific research.

Besides, when the data has not been obtained from the data subject, the provision of information must take place 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.

4.1.1.5 The data subject's right of access to data (Article 12)

The data subject has a right to obtain from the controller:

a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him/her are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him/her in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him/her at least in the case of the automated decisions,

b) the rectification, erasure or blocking of data that is incomplete or inaccurate or the processing of which does not comply with the provisions of the Directive,

c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with b), unless this proves impossible or involves a disproportionate effort.

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

a) at least in the case of processing carried out in the public interest or necessary for the purposes of the legitimate interests pursued by the controller, the data subject will have a right to object at any time on compelling legitimate grounds relating to his/her particular situation to the processing of data relating to him/her, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

b) the data subject will have a right to object, on request and free of charge, to the processing of personal data relating to him/her which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

4.1.1.7 Automated individual decisions (Article 15)

Every person shall have a right not to be subject to a decision which produces legal effects concerning him/her or significantly affects him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her, such as his/her performance at work, creditworthiness, reliability, conduct, etc.

A person may be only be subject to such decision if one of the following takes place:

- a) the decision is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his/her legitimate interests, such as arrangements allowing him/her to put his/her point of view;
- b) the decision is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

4.1.1.8 Confidentiality and security of processing (Articles 16 and 17)

CONFIDENTIALITY

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

SECURITY OF PROCESSING: AGREEMENTS CONTROLLER - PROCESSOR

The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Such measures shall ensure a level of security appropriate to the risks represented taking consideration of their cost and the state of the art.

The controller must, where processing is carried out on his/her behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the security obligations shall also be incumbent on the processor.

For the purposes of keeping proof, such contract or the legal act relating to data protection should be in writing or equivalent form (this should be kept in consistency with the electronic signatures directive).

4.1.1.9 Notification (Article 18)

The directive sets forth the obligation to notify the Member State's supervisory authority as well as the contents of such notification:

OBLIGATION TO NOTIFY THE SUPERVISORY AUTHORITY

The controller or his/her representative, if any, must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations.

Member States are compelled by the Directive to provide simplification or exemption from notification only in the following cases and under the following conditions:

- 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, when 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/her, 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,
 - keeping the register of processing operations carried out by the controller, ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

The obligation of notification 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.

The Directive allows Member States to provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations 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.

CONTENTS OF THE NOTIFICATION (Articles 19, 20 and 21)

It shall include at least:

- a) the name and address of the controller and of his/her representative, if any;
- b) the purpose or purposes of the processing;
- c) a description of the category or categories of data subject and of the data or categories of data relating to them;
- d) the recipients or categories of recipient to whom the data might be disclosed;
- e) proposed transfers of data to third countries;
- f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to the rules ensuring security of processing.

The Directive foresees an obligation of prior checking obligation by the supervisory authority, following receipt of the notification, specially important in the case of processing operations likely to present specific risks to the rights and freedoms of data subjects.

Besides, the Directive establishes that a register of processing operations notified in accordance shall be kept by the supervisory authority. The register may be inspected by any person.

4.1.1.10 Judicial remedies, liability and sanctions (Articles 22, 23 and 24)

REMEDIES: Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority, prior to referral to the judicial authority, every person will have a right to a judicial remedy for any breach of the rights guaranteed him/her by the national law applicable to the processing in question.

LIABILITY: Any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive is entitled to receive compensation from the controller for the damage suffered. However, the controller may be exempted from this liability, in whole or in part, if he/she proves that he/she is not responsible for the event giving rise to the damage.

SANCTIONS: The Member States are compelled by the Directive to lay down the sanctions to be imposed in case of infringement of its provisions.

4.1.1.11 Transfer of personal data to third countries (Article 25)

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.

ADEQUACY OF THE LEVEL OF PROTECTION IN THIRD COUNTRIES: 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.

Where the Commission finds that a third country does not ensure an adequate level of protection, Member States are required by the Directive to take the measures necessary to prevent any transfer of data of the same type to the third country in question.

The Directive also expresses the possibility that the Commission enters into negotiations with a view to remedying the aforementioned situation (which was the case with the United States, leading to the "safe harbor" negotiations).

4.1.1.12 Exceptions (Article 26)

Transfers of personal data to a third country which does not ensure an adequate level of protection may take place on condition that one of the following conditions is met:

a) the data subject has given his/her 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.

The Directive allows a Member State to authorise 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 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. This possibility will, however, be closely surveyed by the Commission, which may object to it and compel the Member State to comply with such objection.

4.1.2 Electronic Communications Data Protection Directive (2002/58/EC)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector was adopted in July 2002 and must be implemented by 31 October 2003.

The Privacy Directive updates the Telecoms Data Protections Directive (Directive 97/66/EC) to reflect new technologies and ensure that the relevant rules apply to phone and fax services, e-mail and Internet usage. Besides, the 2002/58/EC Directive is designed to “particularise and complement” the Data Protection Directive (95/46/EC).

The Directive on Privacy and Electronic Communications aims to ensure that all EU Member States apply equivalent levels of privacy protection regarding the processing of personal data in the electronic communications sector while ensuring that the free movement of data or equipment, or the provision of services in the EU is not obstructed.

4.1.2.1 Aim and Application (Article 1)

The Privacy Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks within Community. It includes provisions regarding calling and connected line identification (CLI) and call forwarding, which apply to both analogue and digital systems, except where this is technically impossible or would require disproportionate economic effort. It also applies to electronic communications and e-mail and Internet usage as well as phone networks. Point to multipoint broadcasting is not covered, but point-to-point services e.g. video on demand, value added services and e-mail and SMS are.

4.1.2.2 Security (Article 4)

The provider must take appropriate technical and organisational measures to safeguard security of its services. These measures shall ensure a level of security appropriate to the risk presented.

If there is risk of a particular breach in security of the network, the provider must inform subscribers, highlight any possible remedies and indicate the likely costs involved Security is appraised in the light of Article 17 of Data Protection Directive (95/46/EC).

Information concerning security risks should be free except for nominal costs incurred by subscribers while receiving or collecting information.

4.1.2.3 Confidentiality (Article 5)

Confidentiality of communications is guaranteed in accordance with the international agreements relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of Member States.

Confidentiality of communications should also be ensured in the course of lawful business practice. Confidentiality of communications and the related traffic data must be ensured through national legislation. In particular, this shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so.

This shall not prevent technical storage, which is necessary for the conveyance of a communication, as long as the agreed rights of an individual’s confidentiality are being respected. This shall also not affect any legally authorised recording of communications and the related traffic data out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

Cookies

When electronic communications networks are used to store information or gain access to information stored in the terminal equipment of subscribers or users clear and comprehensive information must be provided in accordance with Data Protection Directive (95/46/EC) concerning the purposes of such storage. The subscriber or user must be allowed to refuse such processing. This does not apply to technical storage or access if strictly necessary to provide information society services requested by subscribers or users. These provisions apply to use of "cookies" and similar software. However, cookie free access does not have to be provided where the cookie is essential for an on-line service which has been requested or is being used for a legitimate purpose on a web site.

4.1.2.4 Traffic Data

Traffic data relating to subscribers and users which is processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.

Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. However, processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

For either marketing purposes, for electronic communications services, or for the provision of value added services, the provider may process traffic data, only if the subscriber or user has given consent. Users or subscribers shall be given the possibility to withdraw their consent at any time.

The service provider must inform the subscriber or user of the types of traffic data being processed and of the duration of such processing prior to obtaining consent.

Processing of traffic data must be restricted to persons acting under the authority of the provider to handle billing, traffic management, customer enquiries, fraud detection, marketing or whilst providing a value added service, and must be restricted to what is necessary for the purposes of these activities.

Competent bodies will be informed of traffic data in with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

4.1.2.5 Itemised Bills (Article 7)

Subscribers are permitted to receive non-itemised bills. Member States are also obliged to ensure that privacy enhancing methods of communications or payments are available to users and subscribers. Other billing options must also be provided for.

4.1.2.6 CLI Services (Article 8)

Where presentation of calling line identification is offered, the service providers are obliged to provide certain calling and connected line identification (CLI) services. Service providers are obliged to offer various CLI services to subscribers including the right to withhold CLI on outgoing calls on a per call or per line basis and the right to block incoming calls where the CLI has been withheld. Anonymous callers should receive automatic message explaining why the call is barred and how to enable the call. Some CLI services must be provided free including the suppression of CLI on outgoing calls. Network and Service Providers may override subscribers and user's CLI or location data preferences to trace malicious or nuisance calls, or assist the emergency services.

4.1.2.7 Location Data (Article 9)

Network and service providers may also introduce value added services based on location data, e.g. location based advertising to mobile phones, or traffic or weather alert services. Any

services can be provided and third parties can be involved in their provision. The relevant data must be anonymised or the individual concerned must consent. Prior to consent subscribers and users must be informed of the service's data processing implications and must be allowed to withdraw their consent at any time and temporarily withhold consent for free.

Where consent of the users or subscribers has been obtained for the processing of location data, the user or subscriber must continue to have a free and easy method of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Processing of location data must be restricted to persons acting under the authority of the provider or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing that value added service.

4.1.2.8 Exceptions (Article 10)

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) The elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider.

(b) The elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

4.1.2.9 Automatic call forwarding (Article 11)

Member States shall ensure that any subscriber must be able, freely and simply, to block third parties automatically forwarding calls.

4.1.2.10 Subscriber directories (Article 12)

Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included, as well as any further usage possibilities based on search functions embedded in electronic versions of the directory.

Member States will ensure that subscribers are given the opportunity to determine whether their personal data is included in a public directory, and if so, the extent to which that data is relevant for the directory as determined by the provider and to verify, correct, or to withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

Member States may impose separate consent requirements for inclusion in any directory including "reverse search" functions allowing directory users to search for subscribers' names and/or addresses based on phone numbers, rather than vice versa. Subscribers must be told if any directories they are entered in can be so used.

These rights apply to subscribers who are natural persons and may be extended to legal persons. The new rules will not apply to existing editions of directories. The Privacy Directive applies to publicly available directories of subscribers of electronic communications services.

4.1.2.11 Unsolicited communications (Article 13)

The Privacy Directive maintains existing controls on unsolicited direct marketing by means of automated calling systems without human intervention, fax and phone and introduces new controls on unsolicited e-mail and SMS marketing. Individual subscribers must have prior consent or opt in rights in respect of automatic calling systems, faxes, emails and SMS. However, there is an opt in exemption allowing emails to be sent on an opt-out basis in the context of existing customer relationships, when a customer's electronic contact details have been collected during the sale of a product or a service, a company may use these electronic contact details for direct marketing of its own similar products or services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use upon collection, and thereafter on the occasion of each message in case the customer has not initially refused.

Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options is to be determined by national legislation. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, is prohibited.

These rights apply to natural persons and may be extended to legal persons. The Privacy Directive treats unsolicited SMS for advertising in the same way as e-mail messages.

4.1.2.12 Enforcement and Sanctions, Technical Standards and Exemptions For National Security and Law Enforcement Purposes

The Privacy Directive also includes a number of provisions in respect of enforcement and sanctions, technical standards and exemptions for national security and law enforcement purposes. Certain provisions of the Data Protection Directive, RIPA and the Anti-Terrorism, Crime and Security Act 2001 are also relevant.

4.1.3 EU Recommendation on the Protection of Medical Data

In February 1997 the Council of Europe adopted a "Recommendation on the Protection of Medical Data," the principles of which the 39 Members (which includes all the E.U. countries) are urged to transpose into their national laws.

This recommendation is applicable to the collection and automatic processing of medical data, unless domestic law, in a specific context outside the health-care sector, provides other appropriate safeguards. It recommends that the governments of Member States:

- take steps to ensure that the principles contained in the appendix to this recommendation are reflected in their law and practice;
- ensure wide circulation of the principles contained in the appendix to this recommendation among persons professionally involved in the collection and processing of medical data;

4.2 Member States special features

This chapter contemplates the particularities of Member States laws highlighting the special features of each country not included or differentiated from the European Data Privacy Directive (95/46/EC). The Directive 2002/58/EC is not considered in this section because the data of entry into force was 31/10/2003 and it is too early to evaluate their implementation in Member States.

4.2.1 The scope of the national laws (Article 3)

The Directive requires the Member States to apply its provisions to all automated processing of personal data and all processing of such data involving 'structured' manual files, if processing takes place within the scope of Community law and is not carried out for purely personal or household activities. Most Member States apply their laws to processing by means of both automated and 'structured' manual systems. However, some countries extend the rules to (some) manual processing not involving such a system.

Three Member States, Austria, Italy and Luxembourg extend protection quite generally to legal persons, and Denmark to certain data on such persons, while in Germany some limited protection under more general legal concepts could possibly be granted.

The Spanish law applies to any processing personal data, manual or automatised, that allows identifying a person or makes reference to an identifiable person.

The laws in all Member States apply, in principle, to matters both within and outside of the scope of Community law, even though they also often contain specific exemptions concerning typical 'third pillar' issues such as police or state security matters, as regards the information provided to the data subject. Thus, Member States have generally not availed themselves of the possibility to limit the scope of the national laws to matters within the scope of Community law.

Member States have also made rather limited use of the possibility to fully exclude from these laws processing related to the matters listed in Art. 3 (2) of the Directive. The Irish, and Spanish laws have such full exceptions for areas such as police, security and/or terrorism and serious organised crime. Other Member States subject some or most processing in the areas listed in Art. 3 (2), first indent, to separate laws, but this does not necessarily mean that they are subject to a regime which is not supposed to be compatible with the principle of the Directive. Such laws in the Netherlands, Germany, Italy and Luxembourg touch on police, security and sometimes defence matters.

Finally, the status of national laws implementing the Directive within the domestic framework of laws differs considerably. In some Member States the law in question is regarded as quasi-constitutional, or otherwise overriding other legal provisions, while in others the Parliament can pass laws which amend or alter the effect of the laws implementing the directive. This seems to be the case, at least, in the United Kingdom and Sweden.

4.2.2 National laws applicable (Article 4)

In order to determine the territorial scope of the national laws with a view to avoiding both conflicts of law, the Directive requires Member States firstly to determine the controller's establishment as grounds for an application of the respective Member State's law as a principle and, secondly, if the controller is not established on Community territory, to apply their law if the Controller makes use of equipment situated on their territory.

As regards the first main rule, several Member States use the same wording as the Directive. Others follow the Directive closely and add that the laws apply to a controller 'in respect of any data' (UK) or 'in respect of the processing of personal data' (Ireland).

The Finnish, Swedish and Greek laws all refer to processing of personal data where the controller is situated or established on the territory of that Member State, i.e. none of them refer to the processing having to take place “in the context of the activities of” the establishment of the controller in question. None of the laws explicitly specify that they do not apply to processing on their territory if the processing takes place in the context of the activities of an establishment of a controller in another Member State, or to processing by a controller who has its main office on their territory but when the processing takes place in the context of an establishment of that controller in another Member State. However, the non-applicability of domestic law is expressly mentioned in the Explanatory Memoranda to the Dutch and Belgian laws and also appears to be implicitly accepted by the other countries just mentioned. The Luxembourg law says it applies to ‘processing carried out by a controller who is subject to Luxembourg law’. This must presumably be read as covering both controllers established on Luxembourg territory and those who are not established there but subject to Luxembourg law by virtue of public international law. The ambiguity in this crucial context is, however, not helpful.

The Austrian law stipulates that its provisions apply to “processing of personal data in Austria”, except that if a controller who is established in another EU Member State processes personal data in Austria, the law of the place of establishment of that controller is to be applied, unless the processing is for a purpose which “can be attributed to an establishment of the controller in Austria”. To this, the law adds that “legal provisions departing from the above rule” are “permissible only in matters outside the scope of Community law”. The latter is recognition of the fact that the main rule in Art. 4(1) of the Directive only applies to matters within the scope of Community law. While it still retains that rule, in principle, for matters outside the scope of Community law, it allows for corrective measures if the application of this rule leads to data subjects being deprived of adequate data protection in particularly sensitive matters, such as those relating to the “third pillar”.

By contrast, the laws in Denmark, Germany, Italy and Spain contain provisions on their territorial application that in some respect differ from the general rule set out in the Directive. Thus, the Danish law applies to “processing of data carried out on behalf of a controller who is established in Denmark, if the activities are carried out within the territory of the European Community.” The latter qualification means that the Danish law does not apply to processing by a controller established in Denmark, with regard to activities in third countries which have no connection with activities in the Community. The qualification is apparently based on the Danish version of the Directive - but if that is the case, it would appear that that version is not in line with the other language versions, which do not contain such a limitation. In recognition of the fact that adequate data protection is not ensured by the Directive with regard to matters outside its scope, the Danish law furthermore stipulates that it does apply to processing in Denmark by a controller established in another EU/EEA Member State, if the processing is not subject to the Directive, i.e. if the processing relates to matters outside the scope of Community law. It follows, a *contrario* and in line with the Directive, that the law does not apply to processing in Denmark by a controller established in another EU\EEA Member State if the processing is subject to the Directive.

The German law distinguishes between processing in Germany by a controller established in another EU\EEA State, without this involving an establishment of the controller in Germany, and processing in Germany by a controller established in another EU\EEA State but which is carried out by an establishment of the controller in Germany. The law does not apply in the first situation, but does apply in the second situation. However, the law does not clarify to what extent it itself applies extraterritorially.

The Italian law applies to “processing of personal data, by anyone, carried out on the territory of [Italy]”; and the Spanish law to “processing which is carried out on Spanish territory as

part of the activities of an establishment of the controller.” Neither of these rules appear to properly reflect the first main rule in Art. 4(1)(a) of the Directive. The French law uses the criterion of location of operations of data processing on the territory of France.

The above differences in the implementation of the first main rule in Art. 4 of the Directive result in the very kinds of conflicts that Art. 4 of the Directive seeks to avoid. Clearly, this is partly the result of deficient transposition of the Art. 4 of the Directive; a deficient transposition which could be partly explained by the complexity of that provision itself.

As to the second main rule in Article 4, whereby Member States must in principle apply their laws if the controller is not established on Community territory but makes use of equipment situated on the territory of that Member State, again, several Member States avail themselves of the wording used in the Directive. Other laws use some variations and extensions.

First, many laws use a term which translates into English rather as “means” than “equipment”, which appears to be wider than “equipment”, which suggests a physical apparatus. In fact, all processing appears to involve “means”. The German and Austrian laws indeed apply to processing in these countries respectively, without the law using the term “means”. As regards the provision in the Directive by which controllers have to designate a representative in case they make use of such equipment, the Greek law extends this requirement beyond the situation envisaged in the Directive when it requires all controllers outside Greece to appoint a representative if they process data on Greek residents. Secondly, there is some confusion over the exception for controllers who use equipment for “transit through the territory of the Community”, as the Directive states. Several laws refer to transit through the Member State in question instead of the Community, others merely to “transit” without clarifying whether this means transit through their territory or the EU. The Swedish law applies the exception, if the equipment “is only used to transfer information between a third country and another such country”. The French law does not contain this second rule of Article 4.

In conclusion, it must be noted that there is no complete uniformity yet in the implementation of the ‘applicable law’ provision. Because of the substantial divergences, potential positive and negative conflicts of law remain between the Member States.

4.2.3 Data quality (Article 6)

These data protection principles of Article 6 are set out in very similar or slightly varying terms in the laws of most of the Member States of Austria, Belgium, Denmark, Finland, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Sweden and the UK. The Spanish law literally prohibits the collecting of [personal] data by “fraudulent, unfair or illicit means” (*SP: medios fraudulentos, desleales or illicitos*) - but in practice this prohibition is extended to other forms of processing too, in accordance with the Directive. There are more substantial differences between the Directive and the French law that only prohibits any collection of data in an unfair or unlawful way, and foresees that nominal information may not be kept in a form which permits identification for no longer than necessary for the purposes for which the data were collected or processed. The law does not contain however any further principles. The German law also does not contain a list of principles but refers to most of them throughout the law.

In addition, some Member States add clarification to the principles in ways which sometimes strengthen them, as is the case in the Netherlands, but sometimes do the opposite. In the UK for instance, the law adds fixed interpretations to the principles. Thus, the law adds an interpretation of the first principle (that personal data must be processed fairly and lawfully), to the effect that personal data are always to be treated as having been obtained fairly if they were received from a person who was “authorised by or under any enactment [law] to supply

it”, provided that the rules relating to the provision of information to the data subjects are complied with.

For the purpose of -specification and –limitation principle is set out in terms identical or very similar to the ones used in the Directive in the laws of most of the Member States: Austria, Belgium, Denmark, Finland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the UK, and in France. There is a considerable amount of case law within the data protection authorities on the subject, and several authorities have issued detailed guidance. However, the flexibility of the principle leaves it open to divergent application, and different Member States apply different tests in these regards. For example, the UK law, concerns the notion of “specified purpose” stipulates that the purpose of processing may be specified “in particular” in the information given to the data subject or in the particulars notified to the data protection authority.

Member States also have application divergences as regards the “incompatible use” criterion. Member States’ laws range from the “reasonable expectations” of the data subject in Belgium, to “fairness” in Greece or the application of various “balance” tests to determine incompatibility in Germany. In France, the criterion does not appear as such in the law, however, the French data protection authority, points out that the application of Convention 108 of the Council of Europe guarantees the respect of this principle.

Concerning the processing of personal data for research purposes, the Member State’ laws vary very considerably. Some fail to provide any safeguards, some lay down minimal safeguards. No safeguards have yet been provided with regard to secondary processing of personal data for research purposes in Italy and Spain, even though the laws in these countries do allow for such processing without the consent of the data subject. In the Netherlands and Sweden, processing of non-sensitive data for research purposes is subject to rather limited safeguards only, in that the Dutch law merely requires safeguards to ensure that any data used for research purposes are only used for those purposes (without otherwise protecting the data subjects), while the Swedish law allows such uses provided the data are not used to take decisions in respect of the data subjects. On the other hand, the laws in some states provide for detailed rules which limit the data and the processing and stipulate that the research must be approved by an “ethics committee”, or require researchers to apply for a special authorisation from the data protection authority (Belgium), who is to stipulate various conditions, or these additional conditions may be spelled out in the law already (Greece, Luxembourg and Portugal).

It appears that by reason of their open-ended nature, the principles are clearly capable of being differently applied in different Member States, and indeed likely to be differently applied, even in comparable cases, since some countries take a very strict view of them while others adopt a more relaxed approach. Also, they are applied in a very casuistic manner, and the cases in which individual Member States have provided clarification differ between them.

4.2.4 Data processing lawful (Article 7)

The article 7 of the Directive adds a further list of criteria to determine the lawfulness of any processing and in this way established to Article 6 that provides that personal data must be processed ‘lawfully’.

Several Member States follows basically the directive criteria as regards the implementation of the criteria for making processing legitimate. Others national laws take a more hierarchical

view in that the criteria ‘consent’ and ‘processing based on a law or to fulfil a legal obligation’ are given primary status with the other criteria seen as exceptions to these primary criteria. These criteria are as such not part of the French law.

All Member States laws allow for the processing of personal data on the basis of “consent” (Art. 7 (a)), in terms identical or close to those used in the Directive, albeit with some differences in emphasis and with some adding additional clarification or requirements. For instance, that consent must in principle be given in writing, such as the German legislation stipulates or be documented in writing (‘documentata per iscritto’), as the Italian law terms.

As regards the “processing in the public interest/in the exercise of official authority” (Art. 7 (e)), most of national laws set out these terms without additional clarification. The other laws are in principle more restrictive, in that they require that the task or function concerned must be specified by law. However, these constraints are undermined in several of the Member States by more general, and more relaxed, rules which allow for processing whenever this is “authorised by law” or by “special provisions” in or even adopted under any law. Such other laws or provisions will often relate to exactly the kinds of tasks or functions envisaged in the above-mentioned criterion - yet in some Member States, there is no guarantee that processing on the basis of such other laws or rules will be limited to what is “necessary” for the tasks or functions in question. The public sector is governed by particular principles in all Member States, such as the legality principle, being the basis rule the possibility to process data if necessary for the performance of a task carried out in the public interest.

The “balance” criteria (Art. 7 (f)) is set out for only eight Member States in the words used in the Directive or in very similar terms, but several of these attempt to add further clarifications. In Germany law, somewhat differently phrased tests are applied to the private sector and the public sector, respectively. By contrast, the test is applied more restrictively than in the Directive, and/or subject to further formal requirements, in the remaining countries.

In Finland, the law sets out a limited number of cases in which data can be processed and which can be seen as special applications of the “balance” test, but otherwise requires controllers who believe they can rely on this test to obtain a permit from the Data Protection Authority.

In Spain, the absence of this provision on the Spanish Data Protection Law is justified by the government, in the sense that the legislator sets out those cases where the balance test authorises controllers to carry out the processing of personal data. The Spanish approach is similar to the Finnish one. Therefore, in Spain, such processing operations would be those necessary for insurance purposes, credit reporting purposes and any operations involving the processing of certain type of data which would be made publicly available (from the promotional census, the telephone directories, official journals, etc). This peculiarity together with the fact that the Spanish law confers a special treatment to processing that consists of disclosure of information to a third party (“cesión de datos”) makes the processing of personal data without consent of individuals considerably more difficult in Spain than in other countries.

4.2.5 Special categories of processing (Article 8)

This Article lays down additional conditions, over and above the usual criteria for making processing lawful set down by Art.7, for the processing of these so-called “special categories of data”, more commonly referred to as “sensitive data”. Article 8 is a general prohibition with the possibility for exceptions.

Definition of sensitive data and the in-principle prohibition (Art. 8 (1))

Generally Member States set out categories of data to be regarded as sensitive as is done in this article of the Directive, but besides, some States add further categories not included in the concept of “sensitive data”. Finland law includes in “special categories” data on social affiliation, social welfare benefits and socially oriented actions targeted at a data subject. While in Greece, the law also regards membership in any association and data on social welfare as sensitive. Several countries including Denmark, Greece and Portugal impose restrictions on data on purely private matters, creditworthiness or debts; Finland imposes restrictions only on data on creditworthiness. In certain countries criminal convictions are also included under the category of sensitive data although the Directive covers such data under Art. 8(5).

The Netherlands’ definition also includes personal data connected with “unlawful or objectionable conduct for which a ban has been imposed”.

The French law neither considers ethnic origin nor data concerning health or sex life as sensitive data, but refers to ‘moeurs des personnes’.

The Spanish law too is very close to the Directive by applying “special protection” to data which “reveal” “ideology, trade-union membership, religion or belief”, or which “refer to” racial origin, health or sex life.

Several Members laws repeat the wording explain in the Directive as regards the term “revealing”, whereas others Members use terms as “referring to” “relating to”, “as to” or “on” or “describe or are intended to describe”. These differences can have implications as concerns matters which can be said to indirectly ‘reveal’ sensitive matters.

The exceptions to Article 8 (1)’s prohibition (Art. 8 (2))

Some Member States add additional requirements like prior opinions or prior authorisations for the processing of sensible data, even if the data is inside one of the exempted/permitted categories.

With respect to the exception in case of the data subject’s explicit consent in Art. 8 (2) (b), the Spanish Law follows the rule set out in the Directive, that is, that consent must be explicit for all sensitive data (like: ideology, religion, beliefs or trade union membership) but adding that the consent must be by written or legal authorisation. Personal data which refer to racial origin, health or sex life may be collected, processed and assigned only when, for reasons of general interest, this is so provided for by law or the data subject has given his/her explicit consent.

In Portugal, processing of sensitive data on “important public interest grounds” and even processing with the explicit consent of the data subject requires the authorisation of the data protection authority.

The Dutch data protection authority considers consent explicit if ‘the data subject has expressed itself actively as to the scope of the consent’. In France, case law interpreted the requirement in the law of “express consent” for the processing of sensitive data as requiring that the consent be expressed *in writing* - although the data protection authority has accepted that, as regards processing of sensitive data on the Internet, one may substitute a “double-click” for this consent.

The Portuguese data protection authority, express consent for health data means written consent. The Italian law stipulates that consent must be given in writing and in addition to that requires a prior authorisation by the data protection authority.

In Belgium a decree provides that consent of an employee may not be used to allow processing of sensitive data, including medical data, by a present or future employer. This

prohibition of processing is extended to circumstances where the data subject is in a '*relation de dépendence*'.

Under the Finnish Act on data protection at the workplace of 2001, the employer is only allowed to process personal data that is directly necessary for the employment relationship and concerns management of the rights and obligations of the parties to the relationship or benefits provided by the employer for the employee, or arises from the special nature of the work concerned. No exceptions can be made to this provision even with the employee's consent.

With regard to the exception for processing of personal data under employment law one group of States follows the Art. 8 (2) (b) of the Directive adding very little or no details. In other States, the matter is left to special domestic laws which apply in this field such as equal opportunities/anti-discrimination legislation, ethnic composition requirements or legislation on criminal records which addresses the issuing of certificates of good behaviour by relevant local authorities. The first national legislation in the EU dealing specifically with data protection at the workplace is the Finnish Act of May 2001 on protection of privacy in working life. This law is not restricted to regulating the processing of sensitive data in the employment context, however. The special legislation on workers' data protection envisaged by the German federal government has yet to be delivered.

Medical data (Art. 8 (3))

The Directive allows the Member States to lay down further exemptions, provided that the processing is necessary for the purposes of preventive medicine, medical diagnosis, provision of care, treatment or management of healthcare services.

All the Member States' laws refer to the legal obligation of confidentiality or the requirement to treat data with confidentiality although not required by law.

Most Member States transpose this provision into national law in similar terms while in the Netherlands also include the processing by insurance companies of such medical data where necessary for assessing risk and the data subject raises no objection. The Netherlands also foresee exceptions for schools processing such medical data if it is necessary for providing pupils with special support or for making special arrangements in connection with their health and for administrative bodies, pension funds, employers or institutions working for them if required by law, by collective agreements or for the reintegration of or support for workers entitled to benefit regarding sickness or work incapacity.

The Italian legislation allows for processing of health data without the authorisation of the *Garante* where it is required to safeguard the data subject's bodily integrity and health

Spanish law also allows to public and private health-care institutions and centres and the corresponding professionals may process personal data relating to the health of persons consulting them or admitted to them for treatment, in accordance with the provisions of the central or regional government legislation on health care.

Substantial public interest (Art. 8 (4))

This provision introduces an exemption from the application of Art.8 (1)'s prohibition on processing, when is justified by reasons of substantial public interest. The provisions adopted on the basis of Article 8 (4) and (5) are only very rarely notified to the Commission by Member States, contrary to their obligation set out in Article 8 (6).

French law has, since 1994, specific regime on the processing of health data for the purpose of medical research under specific conditions. There are also decrees authorising the recording of civil agreements between same sex partners so as to enable the couples to avail

of entitlements similar to those enjoyed by spouses and decrees regarding public security, anti-terrorism, defence and state security.

In the UK a special Order covers ten contexts in which sensitive data may be processed. In five of these, the relevant paragraph specifically stipulates that, for the exception to apply, the processing covered must be “in the substantial public interest”.

The research can be categorized as a purpose of substantial public interest. This applies in Belgium and Luxembourg regarding historical, statistical and scientific research, in Sweden with the consent of the Research Ethics Committee and in Denmark regarding legal information systems, scientific research and statistical studies. When important public interest demands it, the Data Protection Board in Finland can give permission to handle personal data even if the purposes of the processing does not fit into the exception categories stated in the Act.

The absence, in other Member States, of special Art. 8(4)-type exemptions does not mean that no processing of this kind is allowed in these Member States. Specifically, as repeatedly mentioned, in several countries the data protection law either defers generally to “any other law” or “any legal provision”, or even to administrative decisions taken under any other law or any other legal provision. This means that in the countries concerned- in particular, Germany, Portugal and Sweden, and to a lesser extent Spain- processing of sensitive data can take place on the basis of such other laws or rules. In some of these, there is no formal guarantee that such processing will be subject to the “suitable safeguards” demanded by the Directive, but in some, in particular, in Sweden, the authorities are reviewing such other laws to ensure that they conform to the Directive.

Criminal conventions and offences (Art. 8 (5))

Criminal offence data is included in the Finnish, UK and Greek definition of sensitive data so this allows any of the Art 8(2) exceptions to apply including that of consent of the data subject. This potentially allows for a more relaxed approach to such data than allowed by Art. 8(5) which makes express provision for suitable safeguards. The Greek law requires also a permit issued by the DPA and it includes the safeguard that such a processing can be carried out only by a public authority. Moreover there are specific legal provisions concerning the criminal records. The Belgian law extends the restrictions on the processing to data on any legal disputes and to mere suspicions.

Danish legislation implements this provision for instance states that ‘private individuals and bodies may process data about criminal records, serious social problems and other purely private matters’ other than those mentioned in Article 8 (1) of the Directive if the data subject has given his/her explicit consent. Processing may also take place where necessary for the purpose of pursuing a legitimate interest and this interest clearly overrides the interests of the data subject. However, such processing is subject to prior checking by the supervisory authority, and the data may in principle not be disclosed without the explicit consent of the data subject. In Sweden there is provision for checks on records of staff involved in pre-school activity, school and care of school children and regarding money laundering records.

Again, the Commission has very rarely been notified by Member States of the derogations applied to Article 8 (5).

National identity numbers (Art. 8 (7))

The Article 8 (7) contains an open-ended provision on national identification numbers. Not all Member States have national identity numbers and where they are used, there are great divergences in the rules regulating such processing; in several the introduction of such

numbers is being discussed. In UK, the law expressly allows for the introduction of special conditions on the use of such numbers, but there is no national identification number in the country. It is however clear that there are different approaches to the use of such numbers.

In Ireland, a Public Service Number was introduced in 1998 by means of social welfare legislation. This number is only used for all dealings with public authorities - but may not be used by private bodies (or indeed asked for by the police). Some countries, including Denmark and the Netherlands similarly allow for wide uses and exchanges of such a number between public bodies, if this is useful for the work of the bodies in question.

The law in Finland stipulates that the use of such a number is generally allowed with the consent of the data subject, but imposes strict limitations on its use otherwise. In Sweden the use of the number, even with the consent of the data subject, must still be "clearly justified". This means, in particular, that the number may not be used to "match" different databases, unless there is clear justification for this. In Luxembourg and Portugal, legislation requires that the authorities' permit be obtained before interconnections between files or combinations of data can be made. The same in Greece but when files to be interconnected contain sensitive data or the processing results to the disclosure of sensitive data.

In France, the national identity number, NIR, is subject to limitations, imposed by the data protection authority. Their use seems to be only allowed for clearly specified circumstances and for clearly defined purposes.

In Belgium, a secondary legislation is necessary in order to make use of the national identification number. In Spain, there are two numbers, the national identification document and the passport. Processing of such numbers demand a respect for privacy with an express prohibition on the inclusion of data on race, religion, ideology, etc.

4.2.6 Data protection and freedom of expression (Article 9)

The Article 9 of the Directive requires Member States to lay down exceptions from the provisions in the Directive that are necessary to reconcile the right to privacy with the rules governing freedom of expression.

This clearly, and as expected, is the area where least convergence can be discerned. The laws in the Member States range from stipulating the overall primacy of freedom of expression, through wide exemptions for the press, through fewer exemptions, to a system which contains elements equivalent to prior restraint on the publication of certain information by the press. Also, some laws defer expressly to press laws or self regulatory or quasi-imposed codes of conduct and associated regulatory mechanisms, while others set out the relevant rules in the data protection law itself.

4.2.7 Information to be given to the data subject (Articles 10 and 11)

Informing data subjects of various details of the processing of their data is a crucial measure to ensure transparency in data processing and the exercise of the data subjects' rights. Also, consent can only validly be given when it is 'informed'.

The Directive besides sets out the basic information that must be provided, and in this regard distinguishes between the situation in which data are obtained directly from the data subjects, and situations in which data are obtained from other sources than the data subjects.

The Member States have implemented this provision quite differently. Some stay quite close to the Directive, while others divert considerably from it. With regard to the kinds of information that must be provided, the form in which it must be provided, and the time at which it must be provided. They also differ as to the kinds of additional information that may need to be provided to ensure a fair processing. Some of them repeat the examples given in the Directive, others give somewhat different examples, and some give no examples at all.

The UK law and the proposed new (amended) law in Ireland appear to qualify the informing-requirement (contrary to the Directive) by stipulating that the information should be provided “or made readily available”, and by adding that the information must (only) be provided “insofar as practicable”. On this matter, some Member States follow the examples of the Directive quite closely. For instance, the law in Austria states that additional information has to be given when necessary to guarantee fair processing. To clarify when such is the case, the law provides examples of the kinds of situations, e.g. if the data subject could object and in the Netherlands this is further detailed in the Explanatory Memorandum to the Law and is evaluated on a case-by-case basis. The other Member States laws contrary to this approach are more demanding than the Directive in that they stipulate irrespective of the necessity test indicated in the Directive that some of the additional information listed in the Directive must always be provided. When dealing with information where the data have not been obtained from the data subject, the burden on the data controller is even higher with the requirement that the information should be given in writing (Italy) or at least “explicitly, precisely and unequivocally” (Spain). In Greece, the controller has to inform the data subject ‘in an appropriate and express manner’. He/she has to inform specifically and in writing if the controller requests the data subject's assistance.

As far as the timing of the information is concerned, there are similar divergences. The Dutch law determines that the data subject must be informed prior to obtaining the personal data. When data are collected directly from the individual, in roughly half of the Member States the information must be provided at the time of collection. In other Member States the legislation is silent and the laws in two Member States (Finland and Sweden) are ambiguous in this regard.

There are also some differences when the data have not been obtained from the data subject. Most Member States basically follow the Directive, some add ambiguity given the language used, e.g. Austria stipulates that the information must be provided “in connection with” (aus Anlass) the data collecting and some differ from the Directive. For example, the Greek law requires that the informing be done when the data are collected without allowing for a delay if disclosure is intended, as foreseen in the Directive, while the Spanish law stipulates that the information must be provided within three months, irrespective of whether a disclosure is intended. There is an absence of the obligation to provide information in the French law where the data has not been obtained from the data subject, but the right to be informed is part of the CNIL’s doctrine and has been followed in the codes of the marketing profession.

It seems that all Member States apply this derogation to the processing for statistical purposes or for the purposes of historical or scientific research and apply safeguards in stipulating for instance that such data may only be used for statistical purposes or that data must be kept safe and secure. Some Member States have extended this derogation to other purposes as well, in particular by general reference to “recording or disclosure expressly laid down by law”.

4.2.8 The data subject’s right of access to data (Article 12)

The laws in all the Member States provide for the right of data subjects to obtain access to their data. The overall level of harmonisation in this respect is satisfactory, irrespective of some differences. In some Member States, access requests motivate a reasonable fee while in others requests are free of charge.

As regards the reasonable intervals and the timing for the exercise of this right, despite minor differences, the general rule seems to be once a year -except if there were justified reasons- with the obligation on the data controller to respond within three months of the request. Some

countries provide for shorter periods, like Denmark, where the interval is six months and the controller is obliged to respond within four weeks in principle. In Greece the data subject has a right to submit a petition with the obligation to deposit a fee which should be reimbursed if his/her petition is deemed valid.

The most important formal difference in the laws is that some countries - Greece, Spain and Sweden - require controllers always have to inform data subjects, on request, of the sources of the data - and not just of "any available information" as to these sources-. The law in the Netherlands stipulates that if the data to which access is sought contain data on others (including sources), the controller must contact those others and must decide whether to disclose the information in the light of the response of the other person. The law in the UK contains a similar provision, according to which information about other individuals must be disclosed to the data subject if the other person consented to this, or if it is "reasonable" in the circumstances to provide the data without such consent. However, that law also contains a further (full) exemption concerning references given in confidence to the controller for the purposes of, *inter alia*, education, training or employment.

In Germany, the right of access is extended by the data protection law to data held in nonstructured files, if the controller processes the data "professionally" for the purpose of providing the data to others; in other countries such extensions flow from the special rules relating to such specific kinds of companies. The Austrian law adds that data subjects must also, on request, be provided with the identity of any processors who have processed the data on behalf of the controller, while the Greek law adds that the controller should specifically inform the data subject of any developments in the processing since the last access request.

All the Member States except Spain in principle give data subjects the right to obtain a copy of the data (although the Danish law refers to the data subjects being provided with information "on" or "about" their data, the law is in fact applied so as to require a the provision of a copy of the data there too). In Austria, Finland and the UK, the law expressly mentions that if the data subject agrees, the controller can, alternatively, offer the data subject access rather than a hard copy of the data. The Spanish law provides for this alternative too, but without stipulating that if the data subject wants he/she can demand a hard copy rather than mere access. The proposed new (amended) Irish law also allows for the provision of information other than in "permanent form" if the data subject agrees to this, but also allows for this if "the supply of [a copy in permanent form] is not possible or would involve a disproportionate effort". In France, access to data on criminal convictions, "penalty points" on a driving licence, and certain medical data is provided by allowing the data subject to inspect the data, but without providing a hard copy, so as to frustrate attempts at so-called "enforced subject access".

The laws in all Member States give data subjects the right to be provided with information about the logic used in processing operations, with three Member States, Greece, Italy and the Netherlands, extending this right to all kinds of automated decisions, i.e. not only those involving an evaluation of a data subject's 'personal aspects' and Portugal even extending the right to any automated processing concerning the data subject.

All the laws provide for the right of rectification or erasure and all, except the Finnish law, also expressly refer to "blocking" in this regard. The only minor differences refer to the fact that some laws put more emphasis on the action that should be taken if disputes arise, rather than on the prior matter of the rectification by the controller in response to a request for such action, but in all cases the right of rectification seems to be guaranteed.

4.2.9 Exemptions and restrictions (Article 13)

The Directive provides for a number of exceptions relating to major public interests for several of its provisions on the two conditions that such exemptions must be provided for in “legislative measures” and be “necessary”, i.e. respect the proportionality principle, among others, to safeguard the public interest.

Several Member States set out limitations for the matters and purposes foreseen in Article 13 with some of the laws stating that the application of such exceptions remains subject to supervision by the national data protection authority. For instance, the UK law stipulates in some cases that the exemptions only apply to the extent that the full application of the provision from which they allow derogations “would be likely to prejudice” the matters concerned. This means that the courts and the UK data protection authority are able to assess the necessity of any such exceptions and their application in practice, in accordance with the Directive but on a case by case basis.

The Greek law allows for restrictions on the exercise of data subject rights only for reasons of national security or if this is necessary to prevent or investigate “particularly serious crimes”, and even then only provided that the controller (i.e. the security or police agency involved) obtains special authorisation from the Data Protection Authority.

The Finnish law already uses more limited exemptions than the Directive would allow and adds that the right of access applies “regardless of secrecy provisions” and that any controller relying on such an exception must issue a written certificate to that effect, and this certificate must mention the reasons for the refusal. The Luxembourg law takes a similar line and in addition requires that the data protection authority must be informed of the reasons for refusal. This should ensure that the exceptions are restrictively applied, in accordance with the Directive.

The laws in the Member States vary considerably in the wording used to express the need to protect the interests of data subjects and others, Art. 13(g) and the tests applied are quite vague. Some of the laws do not contain a general provision; it might be felt in those Member States that the ordinary rules and exceptions concerning specific matters were flexible enough anyway.

The other Member States’ laws all contain an exception, or more specific exceptions, to protect data subjects or others, but they apply very different tests in this regard. Such range from mere balance tests or the need for an overriding interest of others in the German and Austrian laws, to very strict tests, as for instance in Denmark that requires an “overriding vital private interest” to trigger the exemption. The UK and Irish laws both contain more specific exception clauses than the protection of the data subject or of the rights and freedoms of others which reflect the view of the legislator on how the balance between conflicting interests must be struck in particular contexts. Thus, the UK law has a provision whereby access can be denied to “confidential references” given about job applicants and to personal data used in “management forecasts” or –“planning” and negotiations with the data subject to the extent that providing access to such information “would be likely to prejudice” the interests of the data controller. In Ireland, the law contains particular exceptions to subject access, for instance concerning in-house estimates of possible liability under claims made against the controller to the extent that providing access to such information “would be likely to prejudice” the interests of the data controller.

There is no certainty that these different tests will be applied consistently throughout the Community. On the contrary, they are likely to lead to further divergences. There are therefore again quite significant divergences between the laws in the Member States.

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

The Directive requires Member States to grant data subjects the right to object to either the processing or the disclosure or use of their data.

The laws in the Netherlands, Portugal, Ireland and the UK apply the right strictly to the minimum required by the Directive: processing for tasks carried out in the public interest or in the exercise of official authority and processing on the basis of the "balance" criterion.

Other Member State laws have extended its scope either by stipulating the right in completely general terms or to other categories of processing. For instance, the laws in Denmark and Italy stipulate the right in completely general terms, to apply to all processing; the law in Austria applies the right to all processing except processing necessary to comply with a legal obligation; the law in Luxembourg applies it to all processing except when "a legal provision expressly prescribes the processing"; and the law in Belgium to all processing except processing necessary to fulfil a contract or precontract, and processing necessary to fulfil a legal obligation. The Greek law somewhat confuses the right to object with the right to obtain rectification, erasure or blocking of data - but would still appear to apply to all processing, and not just to processing which is contrary to the law.

By contrast, the laws in Finland, Spain and Sweden do NOT contain provide for a general right to object - or at least not explicitly. Finland and Sweden law contain a specific provision granting data subjects the right to object to the use of their data for direct marketing purposes and a range of other, related personalised marketing activities. The criterion relating to processing in connection with a public task or with the exercise of official authority is, in the Spanish law, applicable only to public authorities and the use of data from such sources is subject to various requirements which enable persons listed in such sources to object to the use of those data.

4.2.11 Automated individual decisions (Article 15)

This provision reflects the injunction in the law that information technology must serve mankind and should not violate "human identity" or fundamental rights and which therefore prohibit the taking of judicial, administrative and private-sector decisions on the basis of automated processing of data which constitute a "personality profile".

All Member States laws contain provisions on the lines of the one in the Directive, but with some significant differences.

For instance, the laws in Austria, Belgium, Germany, Finland, the Netherlands, Portugal, Sweden and Ireland, set out the in-principle prohibition on the taking of the kinds of decisions mentioned, and the basic exceptions to this prohibition, in terms similar to the Directive. However the laws in Belgium, Sweden and Ireland, apply the exception relating to the data subject being allowed to "put his point of view" not only to (pre-) contractual circumstances but also to decisions based on a law. In other words, the legislator in these Member States felt that the offering of this possibility is also a sufficient safeguard in that other context.

The laws in Austria and Finland on the other hand allow for the taking of such decisions on the basis of any law - without specifying any safeguards (which is contrary to the Directive). In Portugal, the law does not contain the exception allowing for the taking of such decisions on the basis of a law, but rather allows for such decisions (other than in a contractual context) only on the basis of a special authorisation issued by the data protection authority. The German law adds the clarification that if there has been a negative decision of the kind mentioned, the data subject must be informed of this; and that if a data subject challenges such a decision, the controller is obliged to actually review that decision.

The other States laws differ more substantially from the Directive and they would be covered with greater detail, but this provision has been applied extremely rarely and we think that it is out of the scope of this document.

4.2.12 Confidentiality and Security of processing (Article 16 and 17)

All State Member laws stipulate the requirements of confidentiality and data security set out in Articles 16 and 17 of Data Protection Directive, often in identical terms or close to those of the Directive. They thus all stipulate, in only slightly varying terms, that “appropriate technical and organisational measures” must be taken, and that the appropriateness of these measures is to be determined by reference to the risks represented by the processing, the nature of the data. Some laws include additional requirements in order to give more practicality to the security. All member laws also stipulate that controllers have a duty to select a processor who offers sufficient guarantees of reliability and competence.

Finnish law only stipulates this with regard to professional processors, while the French law stipulates, more generally, that the engagement of a processor does not absolve the controller from his/her duty “to ensure that [the security measures required by the law] are adhered to.”

As regards the determination of the technical and organisational measures, most Members have adopted a formulation similar to Article 17 of Directive. Most laws also specifically stipulate, again in accordance with the Directive, that processors must process personal data only as instructed by the controller.

Countries as Belgium, Denmark and Netherlands expressly specify as an exception, processing (other than as instructed) which the processor may be required to carry out by law (this would apply, e.g., to the compulsory handing over of data tapes to the police, in accordance with the relevant legal requirements) - but this exception can of course also be read into the other laws.

The German law in this respect adds that a processor must inform the controller if he/she (the processor) believes that the instructions given to him/her by the controller are contrary to the law. The law in Finland only expressly refers to the duty (also stipulated in the other laws) of all who process data (whether working directly for the controller or employed by a processor) to maintain confidentiality in respect of any personal data they have access to.

The laws also all stipulate that the arrangements between the controller and the processor must be set out in a (written) contract - but only a few (Belgium, the Netherlands, and the proposed new (amended) law in Ireland) add expressly that other, similar (recorded) “legal acts” or other (e.g. electronic) means of recording the arrangements, or “another equivalent form” can also suffice. The proposed new French law merely refers to a “contract”, without reference to its form.

Related to the concept of Privacy Enhancing Technologies (PETs) referred also in Article 17. The concept of PETs aims at organising and/or engineering the design of information and communication systems and technologies with a view to minimising the collection and use of personal data and hindering any unlawful forms of processing by, for instance, making it technically impossible for unauthorised persons to access personal data, so as to prevent the possible destruction, alteration or disclosure of these data. The practical implementation of this concept requires organisational as well as technical solutions.

Several PET strategies are commonly known, such as PETs in the classical sense - technologies that aim at accomplishing the largest possible use of truly anonymous data-, technologies aiming at the promotion of lawful processing, taking into account all the principles of the Directive and aiming at preventing all possible forms of unlawful processing, and thirdly a combination of both strategies.

Two countries, the Netherlands and Germany, have included an article referring to privacy-enhancing technologies in their data protection legislation. The German federal law foresees

that additional legislation be passed on data protection audit, laying down detailed requirements related to the examination and evaluation and the procedure, selection and approval of the experts carrying out the audit. Some data protection authorities like the ones in the Netherlands and in the Land of Schleswig-Holstein in Germany have taken a very active role in the promotion of PETs, which has led to the development of interesting measures for instance in the field of certification and auditing in both countries that are very suitable means to push and promote the advantages of PET. In Schleswig-Holstein, for instance, a regulation concerning audits and privacy seals exists. Companies can have an audit done by the authority on a voluntary basis but financed by the controller. The results of the audit can be used by the company as positive publicity, which is an incentive for companies. The criteria for the seal of quality are both legal and technical; it should be altogether adequate for the user. The seal is valid for two years, after this it has to be obtained again. Companies can present a written report done by an independent expert to the authority that checks it and verify the results. Experts need to go through an accreditation process if they want to be qualified to write these reports. It is therefore a very interesting example of co-operation between the private and the public sector. The Dutch authority offers a so-called PET scan for companies who could like to have assistance assessing the level of technological protection offered by their own processing. This technique has been successfully used in the private and public sectors.

4.2.13 Notification and publicising (Articles 18-21)

All Member States follows the Directive requiring notification of all wholly and partly automated processing. In most cases, notifications must be submitted to the national data protection authority. However, in Spain, filing systems established by public authorities need not be notified to the Authority: instead, the details of such systems must be published in the Official Gazette (Boletín Oficial del Estado), in the form of legislative provisions. The Netherlands allows for notification of processing operations to an in-house data protection official. The same is effectively achieved in Sweden and Luxembourg, in that the laws there stipulate that notification is not required if a controller has appointed an in-house data protection official of the kind discussed above - but the controller must inform the data protection authority of the fact that such an appointment was made, and the official must maintain an in-house register of processing operations, containing the same information as would otherwise have had to be notified; in Luxembourg, this register must be sent to the data protection authority. In Germany, such "in-house notification" is provided for in more limited circumstances. In Finland, controllers are similarly obliged to draw up their own, in-house "specifications" of their processing operations, but they must provide copies of them to the data protection authority.

Some Member States extend the duty to notify processing operations (again, in principle) to all processing of personal data, including those held in manual filing systems (Denmark, Greece, Italy and Luxembourg), while some extend it to only some of the manual systems (Finland and Portugal).

As regards the content of notifications, the national laws include all the matters listed in Article 19 of the Directive, with many laws stipulating further notifiable particulars. In fact, only the Swedish law limits the particulars to those contained in the Directive. Several Member States provide for many exemptions. Austria, Belgium, Denmark, France, the Netherlands, Italy, Sweden, Finland and the United Kingdom all make more or less extensive use of the possibility to grant exceptions.

Germany, the Netherlands, Sweden and Luxembourg are the only countries that foresee the appointment of data protection officials. There is an obligation, in principle, under German law for all bodies that collect, process or use personal data by automated means to appoint a

data protection officer The consequence is that notification is then not required anymore; the officer must maintain a register of processing operations containing the information that would have had to be made in case of notification. The Luxembourg and Swedish laws, too, make provision for the appointment of an officer, and exempt controllers who make such an appointment from notification requirements; in Sweden in order to benefit from exemptions (but not from prior checking, where applicable), the appointment needs additionally to be notified to the data protection authority. The Belgian law foresees to establish a data protection official in some specific cases but does not determine status or competences. Moreover, a “conseiller en sécurité” exists under specific Belgian law. This “counsellor” appears to be rather advising on security matters, as the name suggests, and does not hold the necessary competences foreseen in Article 18 (2), 2nd indent, to be considered a personal data protection official within the meaning of the Directive.

By contrast, Spain has not availed itself of the possibility to introduce any exemptions at all from notification for innocuous processing operations Portugal has only exempted from notification those filing systems which contain publicly accessible information.

As regards “prior checks” or requirements that controllers obtain the “prior authorisation” of their national data protection authority, are the strictest form of control over processing operations. The system is most widely developed in France, where all processing operations in the public sector must in principle be based on a regulation adopted after the data protection authority has given its positive opinion which in practice comes close to an authorisation. By contrast, no processing is made subject to a prior check in the UK to date (even though the law does provide for the possibility); and indeed, the data protection authority feels that no such checks should be introduced for any processing.

Otherwise, too, there are again (in spite of some overlaps) substantial differences between the Member States as concerns the kinds of operations for which they stipulate such prior formalities. Thus, in Austria, prior check is required for processing for the purpose of credit referencing. This category is also subject to prior checking in Denmark which also adds to the list processing by staff recruitment agencies for example. In Sweden, to mention another example, prior checks have been stipulated with regard to processing sensitive data for research purposes without the consent of the data subject, unless the research has been authorised by an “ethic committee”, and also with regard to certain types of processing in the field of criminal investigations and processing of personal data concerning hereditary disposition derived from genetic investigation. In Germany, processing of sensitive data and processing involving the taking of automated individual decisions require a prior check. That check is, uniquely, to be carried out by the data protection official rather than the authority as regards the private sector. The law in Spain does not, in so many words, provide for “prior checks” for certain specified, “risky” operations. However, this is because, in effect, the data protection authority is given the possibility to subject all notified operations to a check of that kind. Specifically, the law stipulates that the data protection authority shall only enter the notified particulars in the register “if the notification meets the relevant requirements”

All the Member States provide for the establishment of a publicly accessible register of processing operations, containing all the notified particulars, except for details of the security measures taken by controllers, in accordance with the Directive (although of course, the contents of these registers will vary because of the differences in the notifiable particulars). In Spain for example, the register contains both the notified particulars with regard to private-sector controllers and the published particulars of processing by public-sector controllers.

4.2.14 Juridical remedies, liability and sanctions (Articles 22, 23, and 24)

Remedies (Article 22)

The Article 22 reference to judicial remedies is without prejudice to any administrative remedy provided under Article 28 by the supervisory authority. Article 22 instead contains a guarantee of access to the courts. All the Member States allow for such a possibility of data subjects to seek redress and corrective action through the courts.

The data protection authorities are not penal authorities but often have an obligation to report offences against data protection law to the police, the competent Minister or Public Prosecutor (e.g. Austria, Italy, Spain, Denmark and the Netherlands).

In Spain, in normal circumstances violations of the data protection law are investigated and sanctioned by the Spanish data protection authority in accordance with an administrative procedure. In exceptional circumstances, where the Spanish Authority considers that the facts under investigation may also constitute a criminal offence, it may report this fact to the Public Prosecutor.

Liability (Article 23)

All the Member States allow for the possibility of data subjects seeking redress, and corrective action, including damages, through the courts. There are, however, differences in the scope of liability. Whereas in some Member States, the controller is liable for any kind of damage, material and immaterial, in others the law is more restrictive as concerns the latter. As regards the grounds for determining the controller's responsibility and exculpation, the Austrian law provides for responsibility only in case of culpable unlawful use of data, as opposed to the rest of Member States. All Member States avail themselves of the exculpatory provision, with some specifying the conditions for a controller to rely on this provision in the law itself and others applying the ordinary rules on civil and administrative liability.

Sanctions (Article 24)

All the Member States laws contain extensive penal provisions, making most actions contrary to the data protection law a criminal offence, punishable by fines or, in serious cases even by imprisonment. Member States have adopted somewhat different formal procedures. For instance, in the UK and Ireland, criminal sanctions are largely linked to 'enforcement notices' which can be issued by the data protection authorities, and which are subject to appeal, while other countries solely rely on denunciations of wrong-doers by the national authority to the prosecuting authorities, or allow the data protection authorities themselves to bring prosecutions. These differences reflect the different legal cultures in the Member States; they do not detract from the in-principle availability of penal sanctions in all of them.

All Member States with the exception of Ireland and Denmark foresee administrative penalties in the legislation which in most cases are to be imposed by the national supervisory authorities. There are important differences both in the amount of these administrative penalties and in the use of them by the Member States.

4.2.15 International Transfers of Personal Data (Articles 25)

As regards the principle of adequacy, the laws of almost all the Member States - Austria, Belgium, Denmark, France, Finland, Greece, Ireland, Italy, the Netherlands, Portugal, Spain, Sweden and the UK - clearly contain the in-principle prohibition of transfer to "third countries" without "adequate" data protection, set out in Art. 25(1) of the Directive, quoted above. The French law of 1978 does not refer to this issue; instead the data protection

authority applies the Articles 25 and 26 of the Directive directly. In determining such “adequacy” the same matters are taken into account as are listed in Art. 25(2) of the Directive - with the Spanish law adding some other matters, such as reports issued by the Commission and the Irish law referring to ‘codes of conduct or other [sectoral] rules which are enforceable in that country or territory’. The Luxembourg law prohibits transfers of data to third countries which do not ensure a level of protection which is “adequate and ensures respect for the provisions of [the Luxembourg] law and regulations” - which could be read as requiring adherence, not just to a generally “adequate” law but to a law which in specific details corresponds to the Luxembourg rules. The same applies for Finland.

The German law is somewhat ambiguous in this respect, by stating the in-principle prohibition rather indirectly in a series of provisions which would, at first glance, appear to deal mainly with transfers outside the scope of Community law- but it must be assumed that the in-principle prohibition also applies to matters within the scope of Community law. It should also be noted that the German law generally focuses on the “adequacy” or otherwise of the protection offered by the recipient in any “third country”, rather than by the level of protection offered by the laws and regulations in force in that country.

Also, Denmark, Finland, Ireland, Germany, Sweden and the UK do not regard the non-EU EEA States (Iceland, Liechtenstein and Norway) as “third countries” in this respect, and they therefore do not apply the in-principle prohibition to these countries, whereas the other Member States - Austria, Belgium, France, Greece, Italy, Luxembourg, the Netherlands and Spain - do regard these three countries as “third countries”.

About the assessment of adequate protection, there are considerable differences about the involvement of data protection authorities in taking of adequacy findings. France, Portugal and Spain, may the national authority take adequacy findings with general effects on its initiative, but even in these countries such findings have been extremely rare. In Belgium, Netherlands and Sweden the national supervisory authorities do not take such general adequacy findings but instead it is the Minister of Justice or the Government, although it is expected that they would consult the data protection authorities.

The Member States also take different approaches to the situation pending formal findings of “adequacy” by either their national authorities or the Commission. In Austria, Greece, Portugal and Spain the law makes clear that only the national authorities can determine that a particular “third country” provides “adequate” protection. In other words, until and unless such a domestic (or European) finding has been made with regard to a particular “third country”, transfer of personal data to that country are subject to the in-principle prohibition. However, in the other countries it would appear that pending such a formal determination, individual controllers can make this assessment for themselves, and can therefore decide to transfer data to “third countries” with regard to which there is no formal (domestic or European) finding of “adequacy”, if they themselves believe that the laws or regulations in the country in question (or indeed in the sector in the country in question) are “adequate”. This is formally stipulated in the Luxembourg law (which merely adds that “in case of doubt”, the controller should seek advice from the data protection authority). While for many non-EU\EEA countries it will perhaps be obvious that they do not provide “adequate” protection, there will be others for which this is less clear, and there can be further differences of views if one were to look at specific sectors. The different approaches to this question pending formal findings therefore result in substantial divergences between the Member States. In this regard, the remark by the French data protection authority, that it “has never encountered a situation in which a transborder flow of [personal] data violated the provisions of the Directive” would appear to be, if not naive then indicative of a desire to “see no evil, hear no evil, speak no evil.”

Regarding the effects of adequacy findings of the EC, the laws in Austria, Finland, Ireland, the Netherlands, Spain, Sweden, Portugal, Italy and the UK all expressly ensure that if and when the Commission does make a “finding of adequacy” under Art. 25(6) of the Directive, such findings are given effect domestically. The Luxembourg law requires adherence to a Commission finding to the effect that a particular third country does not ensure “adequate” protection (Art. 25(4) of the Directive). In Denmark, Commission findings of this kind are adhered to in practice without further ado, which means that a special provision in the law, allowing for the implementation of EC decisions on the implementation of the Directive has not been used.

4.2.16 International Transfers of Personal Data, Exceptions and Derogations (Article 26)

As far as the derogations listed in Art. 26 of the Directive are concerned, the Member States have generally closely followed the text of the provisions in that Article. However, there are also matters in which the laws differ from the Directive (and from each other).

In Spain, the law contains a derogation which only refers to the public interest, rather than to an important public interest, to which it adds that transfers “requested by a tax or customs authority” in any country without “adequate” (or indeed any) data protection “shall be considered as meeting this condition.” The law also contains a special derogation concerning processing “related to money transfers”, provided the data transfer is in accordance with special legislation on such transfers.

The law in Ireland lists as the first derogation transfers of data which are “required or authorised by or under any enactment or required by any convention or other instrument imposing an international obligation on [the Republic]”. Part of this can be said to be covered by the derogation contained in Art. 26(1)(d): transfers which are “necessary or legally required on important public interest grounds” (if one assumes that the legal instruments referred to all serve such interests) - but transfers which are merely “authorised” (i.e. permitted) on the grounds mentioned are not necessarily “necessary or legally required” Comparative Summary of national laws for the purposes mentioned.

The laws in Greece and Italy also add the proviso to the derogation concerning transfer of personal data to protect the vital interests of the data subject that this derogation only applies if the data subject is (legally/mentally or physically) incapable of giving his or her consent to the transfer. The Greek law limits the derogation to protect important public interests to cases in which there is an exceptional need.

All but one of the laws of the Member States provide for the possibility of allowing transfers on the basis of safeguards resulting from contractual clauses. The only country in which this is not expressly done is Greece although in this country (as in Portugal) all data transfers are subject to authorisation. Most of the Member States have not taken major steps in this regard at the domestic level, because of the efforts being made at various international fora, and by the European Commission. Exceptions are the Netherlands and Spain, where the Data Protection Authorities have issued papers on international transfers which include a list of matters to be addressed in such contracts. In France, the data protection authority has been asked to review contract clauses drafted by companies on many occasions.

As regards Article 26 (3) of the Directive, that is, the duty to notify the European Commission of any authorisations granted pursuant to Article 26 (2) on the basis of sufficient safeguards adduced by the data controller, such an obligation is only contained in the laws of Denmark, Portugal, the Netherlands, UK and Austria. Those countries have notified to the European Commission a rather low number of authorisations. Although such a duty is not provided by

the national laws, the European Commission has also received several notifications from Spain, Finland, and Germany. The extremely low number of notifications indicates either that Member States have failed to notify authorisations to the European Commission or that Member States are not granting authorisations as provided for in Article 26 (2) of the Directive and national laws transposing it.

4.3 Summary Table

The following table summarizes the status of the national laws that implement the Privacy Directive described in the previous chapter.

Member State	Member State law status	Date of entry into force
Austria	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) of 17.08.1999	01.01.2000
Belgium	<ul style="list-style-type: none"> • Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data. • Modified by the implementation law of December 11, 1998 (O.J. 3.2.1999). • Secondary legislation adopted on 13 February 2001 and published in the Official Journal of 13 March 2001. 	01.09.2001 (exception for information when the data were not collected from the data subject then three years more)
Denmark	The Act on Processing of Personal Data (Act No. 429) of 31 May 2000	01.07.2000
Finland	<ul style="list-style-type: none"> • The Finnish Personal Data Act (523/1999) was given on 22.4.1999 • Act on the amendment of the Finnish Personal Data Act 	<ul style="list-style-type: none"> • 01.06.1999 • 01.12.2000
France	<ul style="list-style-type: none"> • Law 78-17 of 6 January 1978 • Draft implementation law of July 2001 	---
Germany	The Federal Data Protection Act (Bundesdatenschutzgesetz) was	23.05.2001

Member State	Member State law status	Date of entry into force
	adopted 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May	
Greece	Implementation Law 2472 on the Protection of individuals with regard to the processing of personal data Original version	10.04.1997
Ireland	<ul style="list-style-type: none"> • Data Protection Act 1988 • Data Protection (Amendment) Act 2003 enacted on 10 April 2003 	01.07.2003
Italy	<ul style="list-style-type: none"> • Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31.12.1996 • New Data Protection Code 	<ul style="list-style-type: none"> • 08.05.1997 • 01.01.2004
Luxembourg	DPL approved on 2 August 2002 and published in Memorial A 91 of 13 August 2002	01.12.2002
Netherlands	<ul style="list-style-type: none"> • DPL approved by the Senate on 06.07.2000 (O.J. 302/2000). Original version: Personal Data Protection Act (Wet bescherming persoonsgegevens), Act of 6 July 2000 • Secondary legislation adopted 	01.09.2001
Portugal	Directive implemented by Law 67/98 of 26.10.1998. 'Lei da protecção de dados pessoais'	27.10.1998
Spain	<ul style="list-style-type: none"> • Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999). 	14.01.2000

Member State	Member State law status	Date of entry into force
	<ul style="list-style-type: none"> • Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal. 	
Sweden	Directive implemented by SFS 1998:204 of 29.4.98 and regulation SFS 1998:1191 of 03.09.98	24.10.1998
United Kingdom	<ul style="list-style-type: none"> • Data Protection Act 1998, passed on: 16.07.1998 • Subordinate legislation passed on 17.02.2000 	01.03. 2000

Table 1: Member States Legislation

5 Guidelines affecting Sensation

The SENSATION Integrated Project *aims* at promoting the health, safety and quality of life of people and protect the environment by reducing relevant accidents and thus the impact on environment through the *application of novel micro and nano sensors* and related technologies, of low-cost and high-efficiency, *for physiological state monitoring*. The focus of the work will be the brain activity, including the *sleep and wakefulness states and their boundaries, stress, inattention and hypovigilance states*, for hypovigilance detection, prediction and management as well as diagnosis, treatment and remote monitoring of sleep disorders.

The SENSATION is basing its research into four research core areas.

- **Neurosensing**: development of ubiquitous and novel biosensing technologies.
- **Core Computation**: development and implementation of signal processing and computational intelligence algorithms to study human state, with a focus on sleep, stress, attention and fatigue.
- **Medical**: the application of Biosensing and Core Computation to Medical and Neurology early diagnosis and treatment.
- **Industrial**: The application of Biosensing and Core computation to critical (in terms of time and accident impact) industrial processes.

This project focuses on the first of these, but attention is also paid to the other three. This needs to be the case: sensors cannot be developed in an application void.

SENSATION contributes to ‘industrialization’ of knowledge and dissemination of solutions to enable the application present and future research for continuous monitoring and management of health and performance.

According to the Recommendation of the Committee of Ministers (see EU Recommendation on the Protection of Medical Data chapter), medical data used for scientific research purposes should be, whenever possible, anonymous and systems (in our case SENSATION) that process these data would include techniques and procedures securing anonymity.

From a privacy-protection perspective, there is a wide distinction between **personally identifiable data** and **truly anonymised data**. But, in practice, the demarcation between these extremes is not sharp. Attending assiduously to where particular data lie on the spectrum between them, and especially to data that are somewhere in the middle, is a crucial protection strategy.

At present, large amounts of data lie in-between—they are not completely anonymised, but they are not readily identified, either. The power of computers to perform elaborate, powerful, rapid searches, and the pressures for access, mean that merely assigning simple pseudonyms affords little protection.

For data whose identifiability has, up to now, been only lightly obscured, greater efforts must now be made either: (a) to much more effectively remove personally identifying information, or to aggregate, and thus anonymise, the data; or (b) to seek the data-subjects' informed consent and hold the data under a suitably protective regimen if identifiability is retained.

For **key-coded data**—that is, data for which personal identifiers are removed and secreted but which are still potentially traceable via a matching code, held separately—a variety of measures must be taken to mask the identifiability near the source, separate and lock up the identifiers, safeguard the linking codes, and carefully manage linking-back to the data-subject when it is required.

For many purposes researchers must potentially be able to trace back, even if through intermediaries, to the data-subject. Irreversible anonymisation is not necessarily desirable. There are a number of important reasons why retaining personal identifiability—either openly labelled or via key-coding—may be essential:

- To allow technical validation of reports, such as to confirm the correspondence of various data with the data-subjects, or even to verify the very existence and identity of subjects, in order to prevent scientific errors or fraud.
- To avoid duplicate records or redundant cases, such as to be certain that two case reports are independent and not just the same case recorded in two files.
- To facilitate internal scientific data-quality control, such as enabling working-back to original records and ancillary data.
- To allow case follow-up if more evidence or confirmation are needed.
- To check data-subject consent records, or to examine Institutional Review Board stipulations or opinions on a case.
- To allow tracking of consequences after some research intervention, to be able later, if necessary, to notify the patient or physician in order to recommend reexamination or other measures in-between research and health care.
- To ensure accurate correspondence in linking data on data-subjects, or cases, or groups, or specimens, among different files or databases, perhaps over a long period, even over decades, and possibly to follow-on to descendants.

Data anonymisation must be taken into account in SENSATION applications and communication in order to guarantee the personal data privacy of SENSATION patients. A way to avoid the data anonymisation requirement is to obtain the data subject consent for the SENSATION research purpose.

Another important point to be considered in medical environments is the availability. Patient care is so highly valued there must be a high priority placed on keeping such information available. The health information necessary for patient care needs to be available for access as quickly as possible during normal operations. Furthermore, there must be mechanisms and procedures in place to insure that health information in electronic form continues to be available even in the light of predictable equipment faults or power outages.

For these reasons, health care systems need to plan against disasters. Disasters could include simple machine failures as well as outright destruction of public infrastructure by natural calamities that might wipe out entire installations. The plan against disasters can vary from simple backup tapes, to the use of very comprehensive processes that might include off-site support and backup systems.

The SENSATION consortium is composed of 45 participants from different countries, most of them are UE Members but there are also some non UE partners from: Australia, China, Iceland, Romania, etc. So, the flow of information between non-UE Members must be foreseen in the project in order to guarantee the personal data privacy.

Thus, the Privacy Directive not only regulates processing personal data in the EU but also comprises provisions on the transfer of data towards third countries (articles 25 and 26) where adequate protection is not ensured. The basic principle is that Member States should permit this type of transfer only when the third countries concerned ensure an “adequate” level of protection.

The adequate level of protection is assessed in the light of all circumstances surrounding a data transfer operation. Specific reference is made not only to rules of law but also to “professional rules and security measures which are complied with in that country”. Where

there is an absence of adequate protection in the sense of Article 25 (2), Article 26 (2) of the Directive also envisages the possibility of ad hoc measures. One possibility is the conclusion of a contract between the data provider in the EU and the recipient in the third country. Such a contract must provide additional safeguards for the data subject made necessary by the fact that the recipient in the third country is not subject to an enforceable set of data protection rules providing an adequate level of protection.

The UE Privacy Directive also provides, in Article 26 paragraph 1, a limited number of cases in which an exemption from the "adequacy" requirement for third country transfers may apply. These exemptions concern cases where the risks to the data subject are relatively small or where other interests (public interests of those of the data subject himself/herself) override the data subject's right to privacy.

These considerations must be borne in mind if it is foreseen that SENSATION modules are located in non-members countries.

EU Recommendation on the Protection of Medical Data also recommends the existence of a responsible of security that shall draw up a Security Document specifying the internal security policies. This document must be reviewed periodically, and particularly in case of any changes in the information systems, in order to verify that the document is updated.

Some Member States with more restrictive laws require the existence of some additional measures to guarantee the privacy:

- **Record of Incidences:** The record should indicate the procedures followed to recover the data, the name of the person who recovered such data, and the data manually re-introduced.
- **Audit:** The personal data database shall be audited periodically by an employee or a third independent party. The audit report shall indicate the adequacy of the security measures adopted, deficiencies of the security measures and alternative or additional measures that shall be implemented. It must also include the data, facts or comments on which such report is based.

All these security measures shall be checked periodically in order to assure their fulfilment and to verify that they are enough to guarantee the required security level.

5.1 Guidelines affecting Sensation Applications

SENSATION applications can be mainly categorized in two major groups:

- **Medical:** Medical applications targeted cover the whole medical services spectrum, from diagnosis to treatment. A few sleep-related disorders will be selected for such applications, in order to remain focused on displaying the developed sensors effectiveness and establish the first business cases and not to drift to a medical project.
- **Industrial:** Industrial applications cover in good balance hypovigilance detection and prediction and include various industrial environments (i.e. air traffic controllers, chemical and nuclear factories controllers, heavy machine operators, vehicle and train drivers, ship pilots, etc.). In addition to the above time critical tasks, also sleep management for shift work personalised planning and even QoL improvement is targeted; thus aiming at promoting safety and comfort at the same time. Still, the applications do not overextend in any domain and are not aiming to cover i.e. all transport modes, all road types, all environmental conditions, etc.

The medical data such as the case medical of a patient are considered by the current legislation of most of Member States as one of the personal data types that require greater protection, being included in the higher level of security. Thus, measures shall be taken in the design of SENSATION applications to protect personal data against accidental or illegal destruction, accidental loss, as well against unauthorised access, alteration, communication or any other form of processing. These measures shall be reviewed periodically.

The SENSATION applications must ensure the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, with appropriate measures:

- To prevent the access to any unauthorised person to installations used for processing the SENSATION personal data. This control of entrance to installations is not directly a responsibility of SENSATION applications, but must be borne in mind before the implantation of SENSATION applications in a real environment.
- To prevent data media from being read, copied, altered or removed by unauthorised persons. SENSATION applications must include mechanism to authenticate and identify authorised persons.
- With a view to, on the one hand, selective access to data and, on the other hand, the security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of: identifiers and data relating to the identity of persons, administrative data, medical data, social data, etc. The SENSATION applications must include access profiles establishing the group of authorised users that can access to personal data and the operations that they can perform. The objective of these profiles is to separate the access to data depending on their nature.
- To prevent the unauthorised entry of data into the SENSATION applications, and any unauthorised consultation, modification or deletion of processed personal data.
- To guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment.
- To guarantee that it is possible to check and establish a *posteriori* who has had access to the SENSATION applications and what personal data have been processed, when and by whom. The SENSATION applications must integrate audit mechanisms in order to trace access to personal data.
- To safeguard data by making security copies and establish mechanism in advance to restore data in case of data destruction/loss, partial or total. These backup/restore mechanisms must be checked periodically in order to verify the correct operation. This requirement not only implies to SENSATION applications, it involves all SENSATION system. Furthermore, the backup/recovery copy shall be stored outside the place where the information systems are located, and such copy will be protected by implementing all the above security measures.

The SENSATION applications shall kept medical data no longer than necessary to achieve the purpose for which they were collected and processed. If it is necessary to conserve medical data that no longer serve- their original purpose, technical arrangements shall be made by SENSATION applications to ensure their correct conservation and security, taking into account the privacy of the patient. SENSATION applications shall foresee mechanisms to allow patients to erase their medical data - unless they have been made anonymous or there are overriding and legitimate interest, or there is an obligation to keep the data on record.

SENSATION applications shall store the sensitive personal data that allow the identification of individual and passwords, encrypted in Databases. In this way, only it is readable a set of anonym information, without possibility to identify any person. Also temporary files must be securised depending on the nature of the data stored in it. Furthermore to store sensitive data

encrypted/anonymised, databases and temporary files must be protected by authentication mechanisms to prevent unauthorised access (consultation, modification or deletion) if they contain sensitive personal data.

If SENSATION applications include Web interface, security mechanisms (HTTPS, Digital Certificate, Firewall rules, authentication, etc.) shall be adopted to guarantee the same security level that in local applications.

Any tests to be conducted prior to the implementation or modification of SENSATION applications that manage personal data shall be done with no real data (only fictitious data may be used in such tests), unless if it assures the required security level.

SENSATION applications must consider that personal data used for scientific research may not be published in a form which enables the data subjects to be identified, unless they have given their consent for the publication.

5.2 Guidelines affecting Sensation Communications

The SENSATION Communications are one of the central elements of the SENSATION project. Their main goal is to guarantee the full interoperability of SENSATION modules with different technologies and communication protocols, minimising the time-to-market of further sensors and widening the sort of devices that can be connected.

Three different networks compose the SENSATION Communications:

- The Body Area Network (BAN): The BAN aim is the communication between the sensors and the device that will receive the data from them. The device is called the **Personal Data Processing Unit** and will perform data analysis, required user and body area applications feedback, and communication management.
- The Local Area Network (LAN): The LAN's aim is related to the communication between the different Personal Data Processing Units to provide a collaborative network where a local application can take advantages of the interaction among them. Examples of the LAN scope can be applications where different persons are being controlled for their attention level in their hazardous jobs or a hospital where the patients are being monitored.
- The Wide Area Network (WAN): The WAN's aim is related to the data communications for applications that cross the 'local' boundaries in a long distributed system.

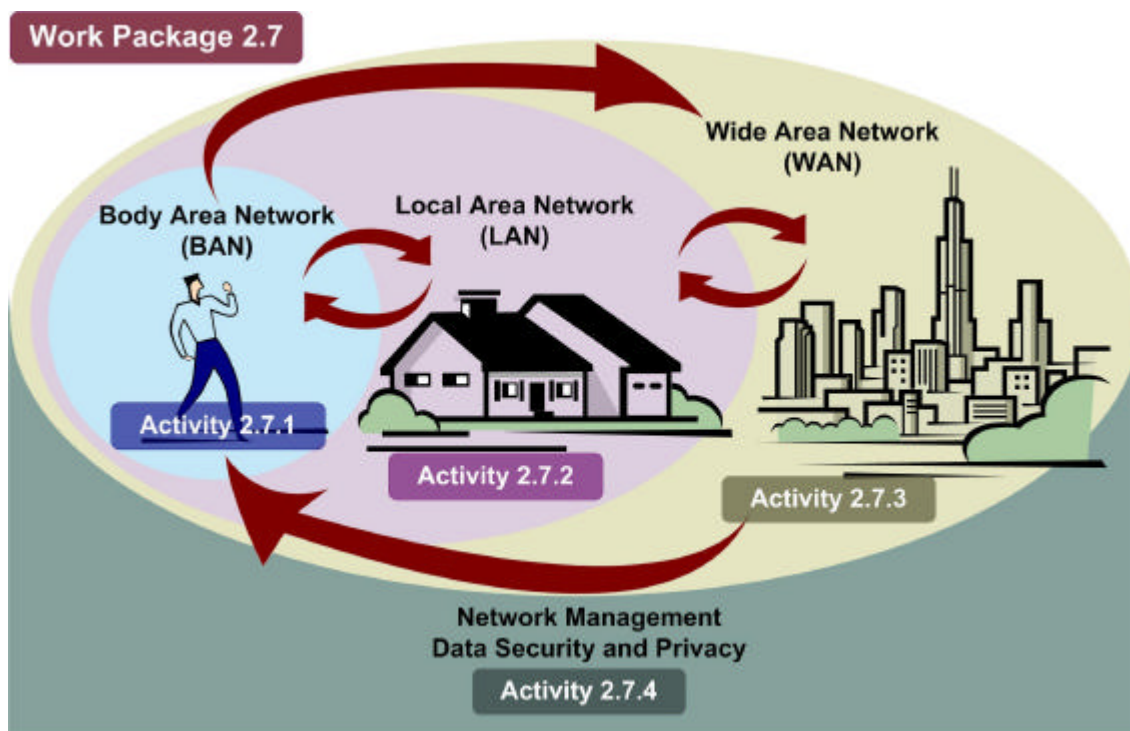


Figure 1: The SENSATION embedded connectivity module layout

The security and privacy in SENSATION communications is crucial to guarantee the security and data privacy in SENSATION, since all data acquired from sensors travel across the communications system until arrive to applications.

To guarantee the required security level, all data communications shall be encrypted to prevent the unauthorised entry of data into the SENSATION applications, and any unauthorised consultation, modification or deletion of processed personal data. SENSATION personal data will go across multiple public network as Internet, GPRS/UMTS, etc. where they can be intercepted by unauthorized people, so it should be recommended to send sensitive personal data anonymised.

Databases and temporary files (such as traces, logs, etc.), if required by SENSATION communications, shall be securised depending on the nature of the stored data. Sensitive data shall be encrypted/anonymised and mechanisms to prevent unauthorised access (consultation, modification or deletion) must be provided if they contain sensitive personal data.

To prevent data media from being read, copied, altered or removed by unauthorised users, SENSATION communications must include mechanism to authenticate and identify authorised users. Since SENSATION communications users are applications and sensors, these authentication mechanisms must provide the communications the way to identify and check the sensors and applications identity. Moreover, the SENSATION communications shall provide selective access capabilities to data. So, communication profiles are required to determine the sensors/applications communications matrix (which applications can communicate with which sensors and vice versa).

Many of SENSATION communications elements are wireless elements, in order to provide the required flexibility and ubiquitously, security requirements must be taken into account in the system communications design. Disconnections occur often in wireless communications, they can be forced by the user because of saving communication costs or they can be induced

by faults. This situation can endanger the data consistency, even without considering replicas. Disconnections are primarily a problem of the underlying layers of a communications system, but the communications system is also responsible for avoiding data loss in case of such unexpected disconnections with the help of transaction recovery.

The higher frequency of network partitioning requires a more powerful error recovery than in fixed networks. Besides error recovery, this situation offers attackers the possibility to masquerade as either the mobile unit or the base station. With the help of masking the identity, data are at risk to be released improperly. Moreover, the use of a wireless link facilitates eavesdropping, because air-emitted information is accessible to anyone with a receiver without any additional effort required.

This kind of security violation is hard to detect. In both cases, security relies on cryptography to achieve user authentication and data privacy. Mobile users are registered with their real identity or with a pseudonym on that domain's authentication server. The authentication service should provide to the communicating parties the confidence that they are in fact communicating with each other. The subsequent communication should protect the data transfer content against attacks and eavesdropping.

BAN Security, due its particular characteristics, requires a deeper study before implementing security measures.

5.3 Security Risk Analysis

Security Risk Analysis is the process of evaluating system vulnerabilities and the threats facing it, is an essential part of any risk management program. The analysis process identifies the probable consequences or risks associated with the vulnerabilities and provide the basis for establishing a cost-effective security program.

To develop a complete security risk analysis is not the aim of this chapter, due to SENSATION applications and communications are still in a definition phase. The objective of this chapter is to outline the main SENSATION threats and vulnerabilities in order to be borne in mind in the SENSATION Applications and Communications design.

At first sight, SENSATION communications seem one of the most vulnerable points of the project. Due to their wireless nature and the use of public networks, communications can be the object of multiple threats because air-emitted information is accessible to anyone with a receiver without any additional effort required. Furthermore, across communications goes all information exchanged between sensors and applications, most of this information is specially sensitive since it contains medical data of the patients and possible application actions on sensors. So, communications are one of the most important points to securise, they shall include mechanisms as encryption, authentication, anonymisation, etc to assure the privacy and security in SENSATION.

Applications are also specially vulnerable because they are the users entry point to data. At this level, the main threat is the access of unauthorized users to data or the access of authorized users to restricted operations/data. Consequently, applications shall contain security mechanism to protect the data access, including databases, temporary files, backups, etc.

A generic threat of all Health Systems is the damage of availability. Patient care is so highly valued there must be a high priority placed on keeping such information available. Health care systems shall include strong mechanism to tolerate Denial of Service attacks.

6 Conclusions

Medical data are considered, by EU Directive and most of national laws, like data that requires a high level of security in order to guarantee the patient care and their case history privacy. Therefore, SENSATION Communications and Applications shall include strong security mechanism to ensure this privacy. The encryption of all sensitive personal data, both in communications and in applications, is mandatory. This data encryption must be done it at all levels, at databases, at temporary files, at exchanges of information, etc. In addition to the encryption, it is strongly recommended, if it is possible, to anonymise data without possibility to identify any person.

Authentication mechanism must be also included by communications and applications in order to identify correctly authorized users (sensors and applications in case of communications). Also profiles are required in order to implement users selective access to data.

Any access (consultation, modification, deletion, ...) to sensitive personal data shall be audited to check and establish a *posteriori* who has had access to data and what personal data have been processed, when and by whom.

Other organizational and administrative capabilities as backups/recovery plans, physical access control, Security document and controller, record of incidences, periodic audits, etc. are also required to strengthen the security and privacy policies.

Findings proposed in this document apply mainly to the implementation and design of the SENSATION Communications system (D2.7.2, D2.7.3, D2.7.4 and D2.7.5) included in WP 2.7 (Embedded Connectivity). All the relevant mechanisms to ensure the security and privacy during the transmission of the information will be addressed in the communication system design and development in this WP.

On the other hand, Applications designers and developers in SP3 and SP4 should be in charge of ensuring the security and privacy of the information processed, and stored by the applications, and accessed and manipulated by the users. Useful findings have been detailed in this document in order to achieve these objectives.

7 References

[1] - 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.

http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm, 2004

[2] - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett, 2004

[3] - Study on Implementation of Data Protection Directive – Comparative Summary of National laws, by Douwe Korff, Human Rights Centre, University of Essex. (16.05.2003).

http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf, 2004

[4] - Recommendation no. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data (Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting).

<http://www.unav.es/cdb/ccoerec97-5.html>, 2004