Community Research

Specific Targeted REsearch Project

PRISM

D2.1.1: Assessment of the Legal and Regulatory Framework

Project acronym: PRISM
Project full title: Privacy aware secure monitoring
Contract No.: 2153350
Project Document Number: ICT-2007-215350-WP2.1-D2.1.1-R1
Project Document Date: 30/06/2008
Workpackage Contributing to the Project Document: WP2.1
Deliverable Type and Security: Public
Author(s): Francesca Gaudino (Baker and McKenzie), Michael Schmidl ,Christoph Rittweger, Denise Lebeau-Marianna, Nicolas Quoy , David Charlot, Charlotte Story , Ilana Saltzman, Ian Walden , Nicolas Passadelis, Philipp Spring (Baker and McKenzie), Elisa Boschi (Hitachi Europe), Sathya Rao (Telscom), Georgios V. Lioudakis, Dimitra I. Kaklamani, Iakovos S. Venieris (ICCS, National Technical University of Athens)

Abstract:

The goal of this document is to identify the applicable law provisions to network monitoring, to interpret them (i.e. define what rules apply to network monitoring and why), and to explain the content of the law provisions, always with an eye to practical issues and use cases. In order to do so we analyse the Directives 95/46/EC, 2002/58/EC and 2006/24/EC together with other relevant law provisions and address the issue of applicability of data protection legislat ion to network monitoring. Together with the European Union directives we selected 7 European jurisdictions and give an overview of the implementation in the selected jurisdictions of the regulatory framework. This work contains and discusses the main reasons, goals and rationale of the Prism project.

Keyword list: PRISM, IST-2007-215350, Requirements, Data Protection Law.

Table of Contents

1 Executive Summary

This deliverable occurs at month 4 of the project activities. Its goal is to identify the applicable law provisions to network monitoring, to interpret them (i.e. define what rules apply to network monitoring and why), and to explain the content of the law provisions, always with an eye to practical issues and use cases. This has been achieved through the following steps:

1. assessing whether the activity of network monitoring is subject to data protection law;
2. reviewing current data protection legislation at a EU level;
3. identifying provisions applicable to network monitoring at EU level;
4. specifying the reasons for the selection of jurisdictions;
5. detailing laws and regulations applicable to network monitoring within seven selected jurisdictions;
6. providing some closing comments on the Prism project and aims.

In particular, Section 2 provides a brief overview of the main purpose of the network monitoring and on the potential impact deriving from application to performance of network monitoring activities on the data protection legislation. Section 3 tackles the issue of applicability of data protection legislation to network monitoring. Section 4 analyzes the Directives 95/46/EC, 2002/58/EC and 2006/24/EC in relation to network monitoring, together with other relevant law provisions. Section 5 lists the jurisdictions selected for the project, clarifies the reasons of the selection, and gives an overview of the implementation in the selected jurisdictions of the regulatory framework designed in Section 4. Section 6 provides some conclusions on application of data protection legislation to network monitoring activities and specifies the main reasons, goals and rationale of the Prism project.

2 Introduction

Traffic monitoring is of essence for any kind of networks, from very small access networks to world-wide operator domains. It should be indeed considered that traffic monitoring is an important way to gather important information that is useful for operating and managing of real networks and also for Service Level Agreement validation.

Furthermore, traffic monitoring is an important prerequisite to guarantee the security of the network infrastructure and of its users. To give an example, continuous traffic monitoring is deployed to detect, alert and set up appropriate countermeasures with regards to events such as network anomalies, network intrusions, denial of service attacks, worm infections and similar incidents. Traffic monitoring is a means that is also used by public authorities (usually in the form of traffic logging) particularly after September 11, 2001 to protect the citizens' and national safety by facilitating the trace-back of malicious or criminal network users.

It may be concluded that network traffic monitoring in general terms is deployed by service or network providers to enhance the service levels offered to their users, to properly manage the network bandwidth, and to prevent abuses and attacks to the networking environment. From a public sector perspective, traffic monitoring is performed to guarantee national security by monitoring the activities performed on the internet.

The reasoning that leads to application of data protection legislation to network monitoring is highlighted in details in the following Section 3 of this deliverable. Taking as an assumption that data protection legislation does apply to network monitoring, it should be outlined that besides the positive effects above outlined, network monitoring triggers data protection concerns. It should be first of all highlighted that as traffic is generated by fixed and mobile communication network users, its monitoring means monitoring the activities performed by users when they make use of a communications network or service (for example, traffic monitoring provides information on when users access and visit a web sites, when and what kind of applications are used, the places in which users are located, etc.).

On the other hand, it should also be pointed out that the amount of data that may be gathered through communications network traffic analysis is potentially indefinite. The possibility of having available such a large amount of data triggers concerns on the possible misuse of said data, for example by application of data mining algorithms and specific elaboration techniques that provide the possibility of building precise users' profiles and then using users' personal data for marketing and promotional purposes.

Furthermore, another important aspect to be taken account of is that traffic monitoring activities are not always made known to users. In practical terms, the fact is that users cannot be aware that their activities over the internet are monitored; the only way they can know it is that the entity performing traffic monitoring activities clearly informs users. Informing users on how their data are used and the relevant purposes represent some of the mandatory provisions set forth by the European legislation on data protection.

Saying that network traffic monitoring implies processing of users' personal data leads to the need for the entities performing monitoring activities to apply data protection regulation. The relevant legal and regulatory framework to be taken into account is detailed in the following Sections 4 and 5 of this deliverable.

3 Application Of Data Protection Legislation

This section is devoted to assess whether the European Union data protection legislation is applicable to the activity of network monitoring. We will start with determining the definition of the term 'personal data', then proceed with the assessment of the type of data gathered through network monitoring, and lastly determine possible application of data protection legal provisions to network monitoring, also focusing on some specific issues such as the identification of the data Controllers.

3.1 Definition of 'personal data' under Directive 95/46/EC

3.1.1 Definitions of 'Personal Data' and 'Processing' under Directive 95/46/EC

Article 3 of Directive 95/46/EC[1] (Scope) states as follows: "This Directive shall apply to the processing of personal data…."[2].

From the foregoing definition it stems that the firs step to determine if data protection legislation is applicable to network traffic monitoring is assessing whether the data processing generated by network monitoring falls within application of Directive 95/46/EC (henceforth, also referred to as the "Data Protection Directive") , which means ascertaining whether network monitoring involves the **processing** of **personal data.**

Article 2 (Definitions) letter (a) of the Data Protection Directive defines 'personal data' as follows: *"Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*.

Artcile 2 (Definitions) letter (b) of the Data Protection Directive reads as follows with regard to term 'processing': *"'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage,*

[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; O.J. L 281, 23 November 1995.

[2] Article 3 (Scope) of the Data Protection Directive reads as follows: "*1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Directive shall not apply to the processing of personal data: - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law, - by a natural person in the course of a purely personal or household activity.*".

adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

At first reading it is clear that the Data Protection Directive has adopted broad definitions of what is a personal data and what means processing of personal data.

As to the term processing, in practice, any kind of activity that is performed on personal data represents data processing, even the mere consultation of personal data. It follows that since the activity of network monitoring basically consists in gathering and processing data, it does represent a 'processing' activity.

Now we should focus on the term 'personal data' in order to assess whether the processing activities performed through network monitoring have as their subject matter 'personal data'. The above reported definition splits the category of personal data in two sub-categories: personal data that identify directly the data subject[3], so-called identification data; and personal data allowing an indirect identification of the data subject.

Identification data are basically pieces of information that distinguish a data subject from all the others and therefore act as identifying factors.

In contrast, indirect identification data are data that do not identify directly the data subject, yet they may identify the data subject through association with other available information, thus in an indirect way.
Recitals 26 of the Data Protection Directive to this regards expressly states that "*to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*". Hence, even if at a first impression these data are anonymous since they do not refer to a specific data subject, they still keep the potentiality of identification. In light of the circumstance that data allowing only an indirect identification of the data subject are in between identification and anonymous data, these data are some times referred to as 'quasi-anonymous' data. It seems appropriate recalling that the wording 'other information available' has regards not only to other information available to the Controller[4], namely the entity primarily in charge of the data processing, but also to any information that may be possessed by any third party other than the Controller. It is important to focus on the circumstance that the definition of indirect identification data is significantly extended by the circumstance that the identification of the data subject may be possible by reverting to any information possessed by any third party other than the Controller.

Moreover, it should also be clarified that the action of identifying the data subject is not necessary as such, it is enough that in general terms said identification is possible, notwithstanding the fact that the relevant data Controller is willing to proceed to the identification or not. In brief, the potentiality of identification makes the data falling within the definition of 'personal data' and as such they are subject to the applicable

[3] The data subject is the subject whose data are processed.

[4] The Controller under Article 1, letter d) of the Directive 95/46/EC is defined as " *the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law*".

data protection legislation, irrespective of the intention of the Controller that holds and processes said data.

As a further explanation of the meaning of indirect identification data, it seems appropriate to recall a Decision of the Italian Data Protection Authority (the "Garante") issued on January 9, 1999 in relation to the publication on a scientific journal of the radiography of a woman. The x-ray photograph was displayed with reference to only the first name and the age of the woman. The Italian Data Protection Authority held that such information is personal data, namely a quasi-anonymous data, because considering the peculiar name of the woman, the age of the woman, the circumstance that the woman lived in a small town where basically anyone might have known the other people from the same town, and the means of diffusion of the information (notably publication on a scientific journal), the woman might have been identified by someone, especially by other people form the same town of the woman [5].

Article 29 Data Protection Working Party [6] in a recent Document issued on June 2007 [7] expressly states the following with regard to the wide scope of the definition of personal data under the Data Protection Directive: "It needs to be noted that this definition reflects the intention of the European lawmaker for a wide notion of "personal data", maintained throughout the legislative process. The Commission's original proposal explained that "*as in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual*"[8]. The Commission's modified proposal noted that "*the amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual*"[9], a wish that also the Council took into account in the common position [10]".

With regard to the issue of data that identify the data subject both directly and indirectly, Article 29 Data Protection Working Party specifies that the most common element used as identifier, in the sense of a directly identifying data, is the name of a data subject. However, the name as such may not always be enough for identification purposes, hence other elements, other pieces of information are needed to identify a data subject.

Article 29 Data Protection Working Party clarifies the foregoing matters through the examples of electronic processing of data. When a computerized file stores personal data, it normally generates a unique identifier for the entries registered that is the data subjects that are registered, in order to prevent confusion between the different registrations. On the web, the device deployed for traffic surveillance allow to define and identify in an easy way the behavior of a certain machine, and since the machine is operated by a data subject (user), ultimately the behavior of said user. It follows that

[5] The Decision of the Italian data Protection Authority is published on the Bulletin n. 7 of January 1999, page 35, and available in Italian language at the following web address:
http://www.garanteprivacy.it/garante/doc.jsp?ID=31031 .

[6] Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is a Working Party set up by Article 29 of the Directive 95/46/CE; for further information on Article 29 Working Party, please refer to the following web address:
http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm.

[7] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf .

[8] COM (90) 314 final, 13.9.1990, p. 19 (commentary on Article 2).

[9] COM (92) 422 final, 28.10.1992, p. 10 (commentary on Article 2).

[10] Common position (EC) No 1/95, adopted by the Council on 20 February 1995, OJ NO C 93 of 13.4.1995, p.20.

the name as such looses its importance in the process of identifying a data subject, and may no longer be required for identifying purposes, and the definition of personal data mirrors this standpoint[11].

With regards to dynamic IP addresses, Art. 29 Working Party considers them as personal data in the sense of information that relates to an identifiable data subject.
In a Working Document adopted in the year of 2000 in relation to the issue of Privacy on the Internet[12], Art. 29 Working Party has taken the view that "*Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2 a) of the Directive …)"* (Reference is made to the Data Protection Directive).

Article 29 Data Protection Working Party in the quoted Opinion on the concept of personal data under the Data Protection Directive [13] clarifies that as to the content of the information representing a personal data, the definition of personal data comprises *any sort of information*, also including information on *whatever types of activity is undertaken* by the data subject.

Taking into consideration the format or the medium on which personal data are stored, Article 29 Data Protection Working Party states that *the concept of personal data includes information available in whatever form*. This means that personal data may be in the alphabetical, numerical, graphical, photographical or even acoustic form, and of course it also refers to information in the electronic format or stored in electronic media, for example *stored in a computer memory by means of binary code*. *This is a logical consequence of covering automatic processing of personal data within its scope* (reference is made to the scope of the Data Protection Directive).

The scope of the definition of personal data is further widened by the interpretation provided by Article 29 Data Protection Working Party with regard to the relationship standing between the information and the data subject under Article 2 letter (a) of the Data Protection Directive when it states that: "*Personal data shall mean any information relating to an identified or identifiable natural person..*".

An information is said to *relate* to a data subject when it is *about* that data subject, and this relationship may be characterized by the presence of a content, purpose or result element.

The content element means that the content of information itself relates to a data subject, that the content of the information itself is about a data subject, for example the information on a company's client that is contained in the client's folder is an information that relates to that client from the content element perspective.

[11] Report on the application of data protection principles to the worldwide telecommunication networks, by Mr. Yves POULLET and his team, for the Council of Europe's T-PD Committee, point 2.3.1, T-PD (2004) 04 final.
[12] Working Document WP 37: Privacy on the Internet - An integrated EU Approach to On-line Data Protection, adopted on November 21, 2000, and available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.
[13] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

The purpose element is present when an information is meant to be used with the purpose of evaluating, treating, or influencing in a certain way the status or the behavior of a data subject.
Article 29 Data Protection Working Party gives as an example the call log of a telephone inside a company office, which may give information about the calls made, which may be information about the company (considered as the contracting party of the telephone operator), about the employee that has been granted the telephone by the company (the telephone is supposed to be controlled by the employee and calls are therefore supposed to be made by him), and also about the data subjects called by that telephone. It follows that the same information (call logs) may be related to different data subjects according to the different purposes for which said information is collected and processed.

The result element means that data relate to a data subject when their use is likely to have an impact on the data subject's right and interests, being it understood that said impact does not necessarily need to be significant.

The content, purpose and results elements are alternative and not cumulative conditions, which means that the presence of only one of them is enough to qualify an information as relating to a certain data subject.

The output of this interpretation according to Article 29 Data Protection Working Party is that *the same piece of information may relate to different individuals at the same time, depending on what element is present with regard to each one. The same information may relate to individual Titius because of the "content" element (the data is clearly about Titius), AND to Gaius because of the "purpose" element (it will be used in order to treat Gaius in a certain way) AND to Sempronius because of the "result" element (it is likely to have an impact on the rights and interests of Sempronius). This means also that it is not necessary that the data "focuses" on someone in order to consider that it relates to him*.

3.1.2 'Anonymous Data' under Directive 95/46/EC

Having specified the meanings of personal data (in the sense of data that identify the data subjects both indirectly and indirectly) and that of data processing, it is left to determine what are 'anonymous data'.

Whereas 26 of the Data Protection Directive, referring to anonymous data, provides that said data are: "*data rendered anonymous in such a way that the data subject is no longer identifiable*". Thus anonymous data are data that do not allow, not even indirectly, the identification of the data subject.

In the Opinion on the concept of personal data above referenced, Art. 29 Data Protection Working Party[14] defines anonymous data as: "any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, *taking account of all the means likely reasonably to be used either by the controller or by any other person* to identify that individual.

[14] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

"Anonymised data" would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible. ".

In practice, data usually are not born as anonymous data, yet they are rendered anonymous through processing and elaboration activities (for example, elaboration in aggregate form). The result of said elaboration is aggregate data, but for the activities consisting in the first gathering and in the elaboration, data have been processed in the form of personal data, and thus they should be processed according to the applicable data protection legislation until they are made anonymous.

From the considerations outlined in this deliverable, it stems that the EU data protection legislation does not apply to anonymous data, and to data that do not fall within the definition of 'personal data' as set forth in the Data Protection Directive, for example when the data do not refer to natural persons, or when the data subject is not considered to be identified or identifiable.

However, the circumstance that the Data Protection Directive is not applicable, does not automatically preclude any kind of protection for the data subjects.
First of all, as outlined in section 3.1.4 of this deliverable, in implementing the Data Protection Directive the EU member states are granted a certain degree of freedom and flexibility, so they can extend the scope of application of the relevant national data protection legislation, as long as they do not breach other provisions of Community laws, and this concept has been clearly approved by the European Court of Justice[15].

Therefore, it may happen that certain circumstances that are out of the scope of the Data Protection Directive receive protection in EU member states. For example, as outlined in section 3.1.4 of this deliverable, in some EU member states the national data protection legislation, differently from the Data Protection Directive, applies not only to natural persons but also to legal entities. The same difference in approach may be taken with regard to matters like pseudonymized or key-coded data.

Moreover, in certain cases the activities that do not fall within the meaning of *data processing* may be subject to protection as they interfere with Article 8 of the European Convention on Human Rights, which is aimed at protecting the right to private and family life, also in consideration of the applicable jurisprudence of the ECHR.

Lastly, other law provisions may have an impact and be applicable, for example criminal law or public law.

3.1.3 Pseudonymised and key-coded data

We have assessed in the above sections that the Data Protection Directive applies to personal data, meaning information that identifies either directly or indirectly a data subject.

Anonymous data, that is information whose deployment does not allow to identify the data subject, not even indirectly, are not subject to application of the Data Protection Directive.

[15] Judgment of the European Court of Justice C-101/2001 of 06.11.2003 (Lindqvist), § 98.

Another type of data that plays an important role is that of pseudionymised and key-coded data. Said data represent personal data that are processed so that they become quasi-anonymous data.
In practice, they are data that usually provide the possibility to identify the data subject, an in this sense they are personal data to which the Data Protection Directive is applicable, but for these specific kinds of data the identification of the data subject is rendered more difficult by the data Controller itself after collection of the data by disguising the identity of the data subject, which usually consists in the identification factors such as name and surname (for natural persons).

The reasons why the data Controller renders the identity of the data subject not known at first glance should be retrieved in Article 6 of the Data Protection Directive [16], which sets forth the main principles for a lawful data processing, including the data quality principles, which may be regarded as representing a sort of benchmark of the all data protection legislation in the sense that the specific rules that discipline the data processing activity contained in the EU data protection legislation stem from these fundamental principles.

These principles are linked one with the others, and as to data quality, they provide that a data Controller should collect and process only the kind and number of data that are functional and necessary to the specific processing purpose that is pursued.

Moreover, data should be kept in a form that identifies the data subject only when and as long as the identification is necessary for the processing purposes to be achieved. It follows that using pseudonymised and key-coded data instead of personal data that identify directly and immediately the data subject represents an adequate and necessary measure to protect data. It may for example be the case that data are necessary not in relation to the data subject to which they refer to, but in relation to their content, or other elements that may be retrieved from the data and that do not have connection with the identity of the data subject.

In conclusion, pseudonymised data that are retraceably are subject to application of the Data Protection Directive and disguise the identity of the data subject, which remains indirectly identifiable, so that they allow to backtrack to the data subject, yet the reidentification process may be performed only by certain subjects and only under predefined circumstances. The psedonymisation procedure is fostered by the Data Protection Directive since it lowers the possible risks for the data subject deriving from the processing of his indirectly identifiable information.

[16] Article 6 of the Data Protection Directive reads as follows: " *1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. 2. It shall be for the controller to ensure that paragraph 1 is complied with.*".

Article 29 Data Protection Working Party in the aforementioned document on the concept of personal data[17] defines the pseudonymisation as the "*process of disguising identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity. This is particularly relevant in the context of research and statistics.*".

A personal data may be pseudonymised in a twofold way, that is in a way that allows and in a way that does not allow reidentification of the data subject.

Reidentification of the data subject is possible for example with the deployment of lists that map and match the real identities of the data subjects with the assigned pseudonyms or through use of two-way cryptography algorythms.

In contrast, if the reidentification of the data subject is no longer possible after pseudonymisation, for example when one-way cryptography solutions are deployed, anonymised data are created.

The features of the pseudonymisation procedure as to results and effectiveness vary on the basis of different factors, for example the moment when it is deployed, the level of security against reverse tracing, the numbers of data subjects involved in the whole data processing, the technical possibility of associating other individually identified information relating to the data subject, etc..

In order to enhance the level of security and to provide a higher degree of protection to the identity of the data subject, the process of pseudonymisation should take place in a random and unpredictable way, and the number of pseudonyms deployed should be large enough to avoid re-using of the same pseudonym (one pseudonym should be used only once). Moreover, for a higher security degree, *the set of potential pseudonyms must be at least equal to the range of values of secure cryptographic hash functions*[18].

Taking into account key-coded data, these are identified by Article 29 Data Protection Working Party in the aforementioned document on the concept of personal data[19] as a "*classical example of pseudonimisation*.".

The procedure that applies in relation to key coded data is that data and information pertaining to a certain data subject are earmarked by a code, and there is another specific document containing the key that associates the assigned codes with the identifying elements of the data subject (for example name, surname, date of birth, contact details such as address and place of residence), which is kept separately form the documentation containing the information referring to the data subject whose identity is disguised under the assigned code.

[17] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[18] Please refer to the Working document entitled "Privacy -enhancing technologies" issued by the Working Group on "privacy enhancing technologies" of the Committee on "Technical and organisational aspects of data protection" of the German Federal and State Data Protection Commissioners (October 1997), available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm.

[19] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf .

With regard to the issue of considering key-coded data as personal data under the Data Protection Directive, Article 29 Data Protection Working Party in the aforementioned document[20] makes two examples to clarify this issue, notably the examples of non-aggregate data to be used for statistic purposes and the key-coded data usually deployed for clinical trials.

The basic principle set forth by Article 29 Data Protection Working Party is that in order to assess if the key-coded data are personal data, focus has to be devoted to the question whether the data subjects may be identified starting from the key-coded data "*taking into account all the means likely reasonably to be used by the controller or any other person*".

As to statistic activities, Article 29 Data Protection Working Party highlights that the use of unique codes as identifiers (meaning that the same code is not assigned to more than one data subject) increases the risk of identification since identification may indeed occur each time that it is possible to access the document or the key containing the correspondence between codes and data subjects.
In said case, consideration should be devoted to the risks of malicious intruders that gain access to said key, for example an external hack, someone within the data Controller's organization that may unlawfully get access to said key or communicate it to unauthorized third parties, also in breach of professional secrecy and confidentiality obligations.
The risks above outlined, that may exist in practice notwithstanding the security measures adopted by the relevant data Controller, make the key-coded data falling within the definition of 'personal data' under the Data Protection Directive.

In contrast, the above outlined risk is limited in case of deployment of codes that are not unique, in the sense that the same code may be assigned to different data subjects that are part of the statistic activities; for example the same code may be assigned to data subjects residing in different cities, and the same codes may be used for different years of the statistic surveys, and in such a case the possibility of identifying the data subject sharply decreases since for identification it would be necessary to access the key document and also to know the relevant year and city of residence of the data subject. In case this further information is no more available in any way, and it is not likely reasonably to be retrieved, the key-coded data may be considered as not referring to identifiable data subjects and therefore they would not be subject to the Data Protection Directive.

Going to analyzing the case of data collected and used in the area of clinical trials with medicines[21], Article 29 Data Protection Working Party in the aforementioned document on the concept of personal data under the Data Protection Directive[22] recognizes that key-coded data are commonly used for said purposes.

The personal data on patients taking part to clinical trials are collected in data collection forms in which patients are usually identified by a code. The medical professional/researcher (usually referred to as the principal investigator) that is in

[20] Please see above footnote.
[21] The regulation on clinical trials with medicines is laid down by Directive 2001/20 of 4 April 2001 on the implementation of good clinical practice and the conduct of clinical trials; JO L 121 du 1.5.2001, p. 34.
[22] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

charge of the clinical trial holds the document containing the 'key' to know the associations between the codes assigned and the identifiers elements of the patients, such as name and surname of the patients.

The so named sponsor, that is the pharmaceutical company that manages the clinical trials, together with or other third parties possibly involved in the clinical trials, only get the key-coded data, and usually do not have access to the identifying personal data of patients, since they are not interested in these data for purposes of the clinical trials: they are indeed only interested in the results of the trials.

The reason why there must exist a document through which it is possible to retrieve the real identity of patients is that in case of adverse effects or risks deriving from the medicines under trail, the principal investigator needs to know who are the patients in order to take appropriate and necessary actions for protecting their health.

Art. 29 Data Protection Working Party, starting from the above outlined principle that "*account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify*" the data subject, reaches the conclusion that key-coded data used for clinical trials should be considered as data relating to *identifiable* data subject (and thus they are subject to the Data Protection Directive) since the identification of the patients to apply appropriate measures and health treatment in case of need is one of the purposes for which the key-coded data are processed.
In brief, it might be held that the whole processing, including the security and organizational measures adopted, is designed so that the ultimate identification of patients is something that is envisaged from the very beginning of the data processing, and is something that is planned to happen when certain circumstances occur, such as adverse effects of the medicines under trial or danger to the patients' health.

However, Article 29 Data Protection Working Party admits that the key-coded data are to be considered personal data for any data Controller involved in the reidentification process; however, the same conclusion may not be applicable to any other data Controller that may have access to the key-coded data.
Attention should be paid to the circumstance whether the other data Controllers operate under a designed data processing that expressly excludes any reidentification of the patients, and to this purpose appropriate technical and organizational measures are implemented (such as for example cryptographic solutions, irreversible hashing measures).

In said circumstances, it is possible that reidentification of patients may be performed, for some technical or other reasons. In said case, it should be noted that reidentification is in principle excluded under any circumstance from the designing of the whole data processing, and appropriate steps have been taken to impede reidentification to take place, so if reidentification of some patients would occur, it would do so as something not supposed or unexpected to take place, as a result of unforeseeable circumstances.

In the above depicted scenario the key-coded data processed by the original data Controller should not be regarded as personal data relating to identified or identifiable data subjects, in consideration of *all the means likely reasonably to be used by the controller or by any other person*, and the data processing of said original data Controller should therefore not be subject to application of the Data Protection

Directive. In contrast, the data processing performed by the new data Controller that performed reidentification of the patients is indeed subject to the rules of the Data Protection Directive, since this new data Controller has identified the data patients and thus it has processed personal information.

In general terms, this is a matter to be considered carefully, having regard to all the specific circumstances of a certain situation, and definitively on a case-by-case basis, since general rules cannot be set forth and applied.

In case the Data Protection Directive does apply, another issue to be taken into account is that of considering that deployment of pseudonyms and key-coded data reduces the risks of breach of the data protection rights of the data subjects, thus the whole data processing, even though subject to the Data Protection Directive, might be subject to less strict conditions, due to the flexibility provided by the Data Protection Directive.

3.1.4 Natural Persons and Legal Entities as the 'Data Subjects' under Directive 95/46/EC

The rules set forth by the Data Protection Directive refer to the data subjects as natural persons, notably as human beings.

However, this should not automatically lead to the conclusion that legal entities are definitively out of the scope of application of the Data Protection Directive from a twofold perspective.

First of all, form a regulatory point of view, national EU member state data protection legislation does refer in same cases to legal persons as data subjects. This is for example the case of Austria, Italy and Luxembourg, where the relevant data protection laws acknowledge almost the same or the same degree of protection to both natural persons and legal entities.

The foregoing is in line with the opinion of the European Court of Justice that has clarified that Member States are free to extend the scope of the national legislation while they implement the Data Protection Directive rules to areas that are not comprised within the Data Protection Directive, as long as there are no other provisions of community law that prohibit it [23].

Moreover, the Directive 2002/58/EC[24] (henceforth, also referred to as the "e-privacy Directive") contains some provisions (specifically some rules under Articles 12 and 13 of the e-privacy Directive on directories of subscribers and unsolicited communication) that are applicable also to legal entities due to the fact that Article 1 of the e-privacy Directive provides that "*2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.*"

[23] Judgment of the European Court of Justice C-101/2001 of 06.11.2003 (Lindqvist), § 98.
[24] Directive 2002/58/EC 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 communication), O.J. L 201/37, 31 July 2002.

From the second point of view, it should be noted that in some cases information on legal entities may be considered as information *relating to* natural persons, and thus subject matter of data protection legislation, due to application of the above recalled criteria of content, purpose or result (please refer to Section 3.1.1. above). The foregoing may happen for example in case of business e-mail correspondence, which in principle may be considered as containing data on the company's organization, but application of one of the aforementioned criteria may lead this information to *relates* to one employee and as such turning into a personal data of a natural person.

The foregoing considerations lead to the conclusion that data subjects are in general terms natural persons, but some regulatory rules of the e-privacy Directive and also the data protection legislation of specific EU member states also apply to the personal data of legal entities.

3.2 Assessment of type of data gathered through network monitoring

Network monitoring and measurement applications generally consist of a front-end, which collects data from points in the network under observation, and a back-end, which stores and analyzes the collected data. The front-end may consist of dedicated sensors, or routers which export information about packets as they pass through the network.

The data collected will of course vary based upon the application. Traffic engineering applications generally export very coarse grained information about flow volume between pairs of routers, quality of service applications export detailed delay information between pairs of routers or hosts, intrusion detection applications will export information about the contents of the packets or the behaviors of the hosts or networks, and so on. However, the protocols which the front-end uses to export measurement data to the back-end may be examined to describe the types of data collected.

In this section we refer to two emerging standards for network monitoring data export: the IP Flow Information eXport (IPFIX) protocol, and the Packet SAMPling (PSAMP) protocol which is based on IPFIX [25]. Both protocols are defined by the Internet Engineering Task Force (IETF). We choose them as they are the most generally flexible protocols for measurement information export, without constraints to a single set of measurement applications or vendor implementation; however, any measurement data export protocol will export broadly the same types of data.

Essentially, any information that may appear in a packet, that may be derived from information appearing in a packet or set of packets, or that may be inferred by how the packet is treated by an intermediate device such as a router or middlebox, may be exported using IPFIX or PSAMP. IPFIX defines a set of *information elements* (IEs) for describing flows, which may be broadly divided into the following groups:

- Flow attributes: e.g. source IP address, number of packets
- Packet treatment information: e.g., routed next hop and AS
- Detailed counters: e.g., sum of squares, flag counters
- Timestamps down to nanosecond resolution

[25] RFC5101, "Specification of the IPFIX protocol for the export of IP flow information". For PSAMP see : http://www.ietf.org/html.charters/psamp-charter.html

- Any ICMP, TCP, UDP header field
- Layer 2, VLAN, MPLS, and other sub-IP information
- Information about the flow metering and exporting processes: e.g. flow timeout interval.

PSAMP extends this set of elements by adding the possibility to export

- Payload information (usually limited to a part of the packet payload)
- Information about the packet metering and exporting processes: e.g. packet observation point, packet sampling rate

Of all these data only information contained in the packet payload or IP addresses might be used to identify the sender or the receiver directly. Note anyway that in most cases IP addresses are not directly linked to a person, so only in a limited amount of cases they can be used for direct identification of persons. Direct identification of legal entities on the other end would be rather easy.

Note that all the attributes in a record can contribute to indirect identification, through e.g. usage patterns. For example timestamps can be used to identify the sender or the receiver in injection attacks or fingerprinting, all invariant fields can be useful for linking or frequency attacks.

3.3 Applicability of EU data protection legislation to network monitoring

In the above section 3.1 of this deliverable we have assessed the meaning of 'processing' of 'personal data' under the Data Protection Directive.

In the foregoing section 3.2 of this deliverable we have given same examples of the type of data generally gathered through network monitoring.

In this section of this deliverable we can therefore give some conclusions on the applicability of the EU data protection legislation to the activity of network monitoring.

The activity of network monitoring for its own nature (monitoring what happens on the network) implies the gathering of a substantial and potentially undefined amount of users' data. Moreover, also in case the monitoring activity is focused only to the header part of the transmitted packets, with the exclusion of the users' payload data, there is still collection of some personal information about users, such as for example who is connecting with whom or with which servers, which applications are used, etc.

It follows that the activity of network monitoring may raise privacy concerns, and therefore it calls for application of Article 8 of the European Charter of Fundamental Rights. As a matter of fact, through network monitoring it is possible to define the activities performed by users online, to understand their habits, preferences, and to gather a significant number of information on the users' life. There is also the risk that said data are used for unlawful purposes, or for purposes for which the users have not given the consent, or even worse, that said data are used without the users being aware of said processing of their data. The same data may as well be collected and processed by competent national authorities for legitimate monitoring and public security purposes.

Since the broad extent of the definitions of personal data and of processing, it stems that the activity of network monitoring does indeed represent a data processing activity that is subject to application of the EU data protection legislation.

It seems appropriate to recall that Recital 2 of the Data Protection Directive expressly states the need that "*data-processing systems …. must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals*"[26].

We have above highlighted that in some cases (for example as to legal entities) the data protection legislation is not always applicable. However, it should be noted that in general terms it may be said that data protection legislation is composed of the following sets of requirements:

(i) requirements towards the data subjects, for example information/consent forms;
(ii) requirements towards the national data protection authorities, for example notification, registration, prior checking;
(iii) requirements towards third parties involved in the data processing, for example appointment as data processor, contractual clauses;
(iv) requirements related to data security measures, for example technical, information and organizational measures;
(v) requirements relating to guaranteeing to the data subjects correct enforcement of their privacy rights, for example the rights to access data, to ask for data amendment, correction, deletion, etc.

If for example there is a data Controller that performs network monitoring activities and is therefore bound by national data protection legislation, but it processes data of both natural persons and legal entities, and the national law requirements only apply to natural persons, said Controller would basically apply the data protection requirements also for the use of data relating to legal entities, except for the items (i) and (v) above, which are specifically focused on activities to be performed towards the data subjects. As a matter of fact, the requirements towards the national data protection authorities will in any case be satisfied, except that the data Controller will focus only on the processing of data relating to natural persons; the requirements towards the third parties accessing and processing data will as well be accomplished, and the data security measures will be in any case implemented.

3.4 The issue of identification of the data Controller

Article 2 – Definitions, letter (d) of the Data Protection Directive defines the data Controller as: "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law*".

[26] Recital 2 of the Data Protection Directive reads as follows: " *Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals*".

The important elements of the above definition are th at the data Controller may be a natural person or a legal entity, of both public and private nature, that operates alone or jointly with others and defines the data processing purposes and conditions.
The terms *jointly or with others* refer to the possibility of having more than one data Controller as decisional center of interests and authorities with regard to the same data processing. This situation should be assessed on a case by case basis and in any case it does not affect the fact that in order to understand who is the data Controller the criteria of judgment to be used are identifying who has authority and independence in deciding the purposes of the data processing (which means for what reasons data are collected) and means of the data processing (w hich means what the main features and characters of the data processing).

Coming to network monitoring, at this early stage of the Prism project it seems that there may be two categories of data Controller, notably service providers that offer to their users a set of e-services (of whatever nature and content), and that perform network monitoring on their own network for different reasons (for example to guarantee effectiveness of the services offered to their users; to monitor and guarantee security of the network; to study means to improve their network and consequently their services, etc.). Further to service providers, network monitoring may also be performed by other data Controllers that have no relationship with the users whose data are gathered, but that perform network monitoring for (usually) scientific and research purposes.

In both the aforementioned cases, whoever is the data Controller, it would be subject to applicable data protection law.

With regard to data Controllers other than service providers, it seems appropriate to recall here the question on key-coded and pseudonymised data that do not allow reversibility should be here recalled.

As above stated, key-coded and pseudonyised data are in general terms considered as falling within the definition of personal data under the Data Protection Directive. However, it may be the case that reidentificatuion of the data subject Is made impossible or very hard through implementation of appropriate technical measures (for example, one way cryptographic solutions). In such cases, if the data Controller has no intention at all to identify the data subjects, because said identification is definitively out of the scope of its processing activities, and it is also irrelevant for the same, then in some circumstances it may be the case that data protection legislation does not apply or applies with a lower degree of severity. In other cases, data protection legislation may applies in the same way as for service providers. This is a situation to be assessed after having performed a specific factual analysis that takes into account the important factors of the specific scenario at stake.

Coming to service providers performing monitoring activities on their own network, it is important to highlight that the circumstance that said service providers already hold the data of their users is irrelevant as to application of privacy law requirements to the specific activity of monitoring.
Indeed, to identify a data processing it is necessary to start from the purpos es of said processing: why, for what reasons, to achieve what results does the data Controller decide to collect and process the relevant data?

It may well be the case (and in real life it often happens) that the same data are processed by the same data Controller but for different purposes. In such cases, each purpose identifies one specific data processing. To provide a trivial but hopefully clear example, the data contained in the customers' databank of a company may be used by that company for different purposes, for example to perform contractual obligations (one purpose), to perform marketing and promotional activities (second purpose) to evaluate the customers' satisfaction (third purpose), to profile customers (forth purpose), and so on. In this case we would have the same data Controller, using the same databank, processing the same personal data that relate to the same data subjects (the customers of the company), yet we would still have four different data processing, and each of them might be subject to different rules (for example the customers' consent would be required for marketing purpose but for not compliance with obligations arising from the contract). Please also refer to what stated in details in the below section 4.1.2.2 of this deliverable with regard to the relationship between the purpose of a processing activity and the identification of different data processing activities.

Applying the foregoing reasoning to the service provider performing network monitoring on the data of its users, it results that the service provider should for example specifically inform its users that their data would be deployed for network monitoring purposes, and depending on the specific reasons why the service providers monitors the network and on the applicable national data protection law, the users' consent may be necessary.

3.5 The issue of assessment of applicable data protection law

When it comes to the internet, national boundaries often loose of importance, in the sense that the virtual world has been conceived and designed as a global phenomenon, capable of going beyond the material state lines existing in the real world.
Moreover, in the information technology sector it often happens that who provides the service (the service provider) is not physically located in the same place where are located the data subjects (users) to which the services are offered and provided.

Going to network monitoring, it may happen that since more entities are involved in the monitoring, and the entities are established in different locations, it may be difficult to assess what is the applicable data protection law.

Art. 29 Data Protection Working Party has recently tackled this issue in an opinion relating to search engines[27], which presents the problem of assessing what is the applicable data protection law within the frame of the business activity of search engines. Reference should also be made to another working document of Art. 29 Data Protection Working Party on the international application of EU data protection law to personal data processing by non-EU based web sites[28].

[27] Opinion 4/2007 on data protection issues related to search engines issued on 4 April 2008, WP 148; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf .
[28] Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites issued on 30 May 2002, WP 56; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf .

In order to determine the applicable data protection law, the first step is identifying who is the data Controller. Secondly, attention should be paid to the place of the establishment of the data Controller where the data processing is performed.
Article 4 of the Data Protection Directive[29] is the law provision to be considered as it deals with the issue of providing the criteria to be deployed in order to determine the national applicable data protection law.

The big watershed is the fact that the data Controller is established within or out of the European Union boundaries.

If a data Controller is established within one of the EU member states, it should apply the national data protection law of the member state in which it is located the establishment where the data processing is carried out, for example a data Controller established in France applies French data protection law; in the UK applies English data protection law; and so on.

In case the data Controller has establishments where the data processing is performed that are located in several and different EU member states, each establishment should apply the national data protection law of the EU member state in which it is located, so for example if a Controller has an establishment in Italy and another in France, the Italian establishment will apply Italian data protection law, and the French establishment will apply French data protection law, and so on.

In the aforementioned documents of Art. 29 Data Protection Working Party it is clarified that: "*the existence of an "establishment" implies the effective and real exercise of activity through stable arrangements and has to be determined in conformity with the case law of the Court of Justice of the European Communities. The legal form of the establishment – a local office, a subsidiary with legal personality or a third party agency – is not decisive. However, a further requirement is that the processing operation is carried out "in the context of the activities" of the establishment. This means that the establishment should also play a relevant role in the particular processing operation*".

The foregoing implies that the mere presence of an establishment in a country is not decisive as such, because it is also necessary that within said establishment the Controller should perform data processing activities that are relevant with regard to the entire data processing that is considered.

The situation is different if we consider a data Controller that is based out of the European Union. In such a scenario, the Data Protection Directive under Article 4 sets forth two cases in which the EU data protection legislation has to be applied.

[29] Article 4 (National law applicable) reads as follows: " *1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Me mber State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law; (c) the controller is not established on Community territory and, for purposes of processing personal data ma kes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community. 2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.*".

In brief, it may be said that the non-EU based data Controller should apply the Community data protection legislation when it (i) has an establishment within a EU member state (Article 4 (1) (a) of the Data Protection Directive); or (ii) makes use of equipment that is located within the territory of a EU member state (Article 4 (1) (c) of the Data Protection Directive).
The *equipment* referenced in the latter case may be automated (electronic) or not, and the only exemption to this rule is if the equipment is used for purposes of mere transit of data through the territory of the Community.

Coming to what can be defined as *equipment*, Art. 29 Data Protection Working Party has provided some guidance and clarifications in the above referenced opinions.
In general terms, equipment is any means used to process data (for example cookies other than session cookies are considered to be falling within the meaning of equipment for purposes of application of the EU data protection legislation by non-EU based data Controllers).
The final assessment on the applicable data protection legislation should in any case be reached after a detailed analysis of the factual scenario, and on a case-by-case basis.
As a general comment it may be said that the criteria set forth under the Data Protection Directive to determine the applicable data protection law do provide specific guidance and support in determining what are the specific privacy obligations that the relevant Controller should comply with.

4 Legal And Regulatory Framework

Having established that network monitoring does involve the activity of processing of personal data under the Data Protection Directive, in the following sections of this deliverable we will try to provide the legal and regulatory framework applying to network monitoring at an European Union level.

The same framework will be further provided also with regard to the jurisdictions selected for the Prism project.

4.1 Application to network monitoring of Directive 95/46/EC (Data Protection Directive)

4.1.1 Scope and extent of application

The scope of the Data Protection Directive is specified under Article 1 of the same (Object of the Directive) as follows: "*1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data...*".

The aforementioned law provisions recalls the scope of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data[30], as well as Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [31].

[30] Council of Europe, Convention No 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, adopted in 1981; available at the following address: http://www.privacy.org/pi/intl_orgs/coe/dp_convention_108.txt; Article 1 of the Convention, Object and purpose, states as follows: "*The purpose of this convention is to secure in the territory of each Party for every individual,*

Article 1 (1) of the Data Protection Directive represents the acknowledgement of the right to data protection as a fundamental right of the individual, which is acknowledged as deserving legal protection within the European Union, and in some EU member states said right is acknowledged as a constitutional right of the individuals.

Article 1 (2) of the Data Protection Directive highlights that the scope of the Data Protection Directive is also offering an equivalent level of data protection within the Community, for the right to data protection to not longer constitute an obstacle to the free flow of data among the EU Member States.

This principle is deeply linked with the criteria provided by the Data Protection Directive to determine the applicable data protection law, in the sense that application of one EU member state national privacy legislation is considered as equivalent to any other EU member state, because all of them derive from the Data Protection Directive, which sets forth a common benchmark that represents a guarantee of fairness and lawfulness in the data processing.

4.1.2 The lawfulness of the data processing and the data quality principle

Article 6 of the Data Protection Directive[32] provides the so named principle of fair and lawfulness processing, and the principle of data quality.
These principles are considered to represent the grounding of the entire EU data protection legislation, in the sense that the other rules and limitations set forth by the Data Protection Directive stem from the general principles provided under Article 6 of the Data Protection Directive.
Said articles state that personal data must be processed fairly and lawfully; that personal data can be collected only for specified, explicit and legitimate purposes, and that personal data cannot be processed for other purposes that are incompatible with these for which the personal data have been originally collected.
Furthermore, the personal data that are processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

4.1.2.1 Lawfulness and fairness of the data processing

---

whatever his nationality or residence, respect for his rights and fundamental freedoms , and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")".

[31] European Convention for the Protection of Human Rights and Fundamental Freedoms; Council of Europe; Rome, 1950; available at the following address: http://www.echr.coe.int/NR/rdonlyres/D5CC24A7 -DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf.

[32] Article 6 of the Data Protection Directive states the following:" *1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. 2. It shall be for the controller to ensure that paragraph 1 is complied with.".*

The provision imposing that *data must be processed fairly* poses an obligation on the data Controller to act fairly, thus prohibiting to process personal data with malicious intent or with an aim to cause harm to the data subject.
The meaning of *fairness* is usually recognized as the concept of good faith that exists in contractual and social relationships.

The consequences that the processing of personal data may cause to the data subject are usually taken as a criterion to assess whether a data processing is fair.
Examples of unfair behaviours from a data protection law perspective are, for example, to provide to the data subject misleading information on the kind and purposes of the processing; to obtain the data subject's consent maliciously; etc.

Saying that the data processing must be *lawful* implies that it should be performed according not only to applicable data protection legislation, but also to any other applicable law, regulation, and provision that may also be not a legislative act from a strict legal interpretation.

To this regard we may for example think to the opinions and interpretations issued by the competent national data protection authorities, to the recommendations, working documents and opinions of Art. 29 Data Protection Working Party, to applicable codes of conduct, up to the consolidated doctrine, to the extent that it is applicable.

The reason of extending the legislative scenario also to laws and provisions other than applicable data protection laws should be found in the circumstance that the data protection legislation is not meant to contradict to or contrast with other applicable laws and regulations.
An usual example to this respect is labour law. In case a specific activity of data processing is prohibited under applicable labour law (for example because it implies an unlawful monitoring of the employees' activity), the fact that said activity is compliant with applicable data protection requirements does not render the processing lawful, so for example an employer wishing to monitor his employees in breach of applicable labour law provisions, may not claim as legal ground of this activity the fact that he complies with applicable data protection law because he has duly informed the employees and that he has also obtained the employees' consent to the data processing consisting in unlawful monitoring activities.

4.1.2.2 The purpose principle

The purpose principle states that personal data can be collected only for specified, explicit and legitimate purposes, and they cannot be processed for other purposes that are incompatible with these for which the personal data have been originally collected.

The purpose principle is very important in order to determine the different data processing activities that are performed by a Controller. Please also refer to what stated in details in the above section 3.4 of this deliverable with regard to the issue of identifying a data processing activity in connection with the purpose for which data are used by the Controller.

Basically the processing purpose defines the data processing, in the sense that in order to determine the number and kind of processing activities that are in fact carried out, it is necessary first of all to look at the reasons for which personal data are processed.

The databank containing the data and the subjects processing the data are not elements of relevance, since the same subjects may be processing the same personal data that are moreover kept in the same databanks, but the processing may take place for different purposes. The fact that the purposes are different leads to the consequence that we have different data processing activities.

Moreover, the purposes for which data are processed in same cases also impact on the specific law provisions to be complied with.
A simple example is if we consider the customers of a given company as data subjects. The company may process the customers' data for purposes of performance of the contract relationship, and also to perform customer satisfaction surveys, and lastly for marketing activities.

In said example we have three different purposes: performance of contractual obligations; customer satisfaction surveys, and marketing activities.
For the first purpose the customers' consent to the data processing is not required under the Data Protection Directive, while the consent is usually required for the other two processing purposes (notably customer satisfaction surveys and marketing activities).

The purpose principle is fundamental since it also bounds the data Controller to the obligation of acting in a transparent way, in the sense that the processing purposes should always be *specified* and made *explicit* by the Controller.

The Controller basically cannot use the data for purposes that it has not clearly stated. This applies especially towards the data subject, with regard to the reasons why the data Controller wishes to process the data subject's personal data , and which is deeply linked with the right of information acknowledged to the data subject, who should always be made aware of the processing carried out on his data.

This rule is aimed at guaranteeing to the data subject an effective control on the processing of his data, considered under the points of view of information to be received by the data subject, of possibility for the data subject to enforce his privacy rights (for example right to access his data, to ask for deletion, updating of his data, etc.), and consciousness of the data subject when he gives his consent to the data processing.

The set of mandatory information to be given to the data subject in part vary from one EU member state to another, yet the core of the information rule set forth in the Data Protection Directive cannot be disregarded.

Saying that the processing of personal data must be *legitimate* means that the data processing lawfulness should be assessed against not only data protection legislation, but also against any applicable laws and regulations, as specified in the above section 4.1.2.1 of this deliverable.

The personal data should not only be collected and processed for specified, explicit and legitimate purposes, but should also be not further processed for purposes that are incompatible with these for which data have been originally collected and/or processed in order to guarantee consistency and lawfulness of the whole personal data processing.

The change of the data processing purposes is allowed only in accordance with the principle of compatibility that has to be assessed on a case -by-case basis.
The Data Protection Directive has made *a priori* an assessment of compatibility saying that the further processing of data for historical, statistical or scientific purposes is not incompatible with other data processing purposes, provided that the national applicable privacy laws of the relevant EU member state set forth appropriate safeguards.

4.1.2.3 The data quality principle

The data quality principle states that the personal data that are processed must be *adequate*, *relevant* and *not excessive* in relation to the purposes for which they are collected and/or further processed.
Said principle is concerned with the features of the data used to achieve a specific processing purpose since a processing in order to be lawful must be carried out on data that are functional to the processing purpose that it is sought.

In this sense, it should be created a kind of correlation between the personal data and the activity of processing, and they should be processed only the personal data that are strictly necessary to achieve a specific processing purpose. Accordingly, the personal data which, when assessed towards the purpose of their processing, result to be redundant or not necessary, cannot be collected or used.
In case of data that were necessary to achieve a specific processing purpose and that further begin no longer necessary since said purpose has been achieved or the way to achieve it is for any reason changed, then these data when they become unnecessary should be promptly either deleted or made anonymous.

The data quality principle also provides that personal data must be accurate and, where necessary, kept up to date.
Moreover, the Controller should take every reasonable step in order to ensure that personal 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. This obligation exists independently of specific orders issued by local data protection authorities or of requests of the data subject.

The rationale of the obligations relating to the rules on quality of personal data as above outlined resides in the fact that it is very important to ensure protection of the quality of personal data as information relating to the data subject, also in light of the possible damages and contrivances that may occur as a consequence of the processing, communication or spreading of incomplete or inaccurate information.

In order to comply with the data quality principle, the Controller should perform periodic audits on each data processing activity that it carries out to verify that the personal data that the personal data that it process, assessed against the purposes for which said data are processed, result to be adequate, relevant and not excessive.

The principle of data quality intended as adequacy, relevance and not excess of the personal data processed should be considered in tight interaction with the data minimization and the data retention principles below considered.

4.1.2.4 The data storage principle

The data storage principle provides that personal data must be kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data were collected or for which they are further processed.

We have stated that the data quality principle provides, inter alia, that the Controller may process only the personal data that result to be adequate, proportionate and not excessive if compared against the purposes for which they are processed.
Since the activity of storing personal data falls within the definition of processing of personal data under the Data Protection Directive, it follows that personal data cannot be kept forever, for an undefined period of time, since in contrast personal data may be kept (thus processed) only until the purposes for which they have been collected are achieved. After that, personal data should be immediately either deleted or made anonymous.

The Data Protection Directive could not list the specific data retention periods allowed for a lawful processing of personal data, since it would have been impossible to specify the time for which data could have been retained in relation to all the possible purposes of personal data processing.
The Data Protection Directive therefore provides a general principle (the data storage principle) that identifies the criterion to be used for a lawful storage of data, and to assess the specific period of time for which the Controller may keep the personal data that it processes.
The Controller is thus charged with the burden to verify the time for which it can keep the personal data, and also to provide for solutions that allow either deletion or anonymization of data when these are no longer necessary to the pursued purpose.

The rules above outlined that derive from the data quality principle and the data storage principle are connected one with the others, and should be considered as a whole, since each of them is prerequisite for compliance with the others, and all together they form the fundamentals on which a lawful data processing is based upon. For example, the principle of transparency allows assessing consistency of the data with the purposes for which they are processed and also serves the purpose of determining the period of time for which data may be retained [33].

With regard to the data storage principle, it should be said that this important rule is often breached. Indeed, since information as such in the business world is often a valuable asset, some times Controllers tend to keep data forever.

This problem has been recently tackled also by Art. 29 Data Protection Working Party in the aforementioned opinion relating to search engines [34], in which it states as follows: "*If personal data are stored, the retention period should be no longer than necessary for the specific purposes of the processing. Therefore, after the end of a search session, personal data could be deleted, and continued storage therefore needs an adequate justification. However, some search engine companies seem to retain*

[33] G. BUTTARELLI, "Banche dati e tutela della riservatezza. La privacy nella società dell'informazione"; *Giuffrè; Milano;* 1997.
[34] Opinion 4/2007 on data protection issues related to search engines issued on 4 April 2008, WP 148; available at the following web address:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf .

data indefinitely, which is prohibited. For each purpose, a limited retention time should be defined. Moreover, the set of personal data to be retained should not be excessive in relation to each purpose.".

The issue of data retention period for search engines had been previously tackled with specific regard to Google that has therefore decided to limit the initial time of storage of the data on users' search activities [35].

It comes clear from the foregoing that whatever is the purpose for which data are processed, there must be an end to the retention of data, since retention of data indefinitely is against the data protection legislation.

Mr. Francesco Pizzetti, current President of the Italian Data Protection Authority, has raised the issue of compliance with data protection legislation in the virtual internet world, also with specific reference to the issue of retention of data and the so named 'right to oblivion', notably the right to be forgotten.
Hereinafter some pieces of the speech given by Mr. Pizzetti in the 2006 Annual Report of the Italian Data Protection Authority to the Parliament[36]: "*On the network, the data has a life of its own that is unbounded and makes it impossible to envisage all the purposes and contexts of its use…. What does the right to oblivion mean when one is faced with search engines keeping and making available data and information on individuals for a basically indefinite time ?*".

4.2 Main principles and rules to be applied

Hereinafter it follows an outline of the main principles and rules of the Data Protection Directive that are of relevance in relation to the data that may be gathered through network monitoring.

4.2.1 Articles 18; 19 and 21 of the Data Protection Directive: the notification

The notification is a formal communication of the Controller in which it declares to the national data protection authority that it is processing personal data, and also provides some specific information on said processing as requested by applicable national data protection legislation.

The Data Protection Directive leaves a certain degree of freedom to the member states in implementing the notification rule, in the sense that member states are for example free to determine the cases of simplification of and exemption from the notification requirement.

The register of the notifications received by the national data protection authorities must be kept available for inspection by any person[37], in order to ensure full transparency and acknowledgement of the processing operations performed within a

[35] For more information, please refer to articles available in English at the following web addresses:
http://news.zdnet.co.uk/internet/0,1000000097,39287254,00.htm , and
http://news.zdnet.co.uk/security/0,1000000189,39288141,00.htm?r=10.
[36] The speech delivered by the President of the Italian Data Protection Authority, Mr. Francesco Pizzetti, on the occasion of the presentation to Parliament of the 2006 Annual report – Rome, 12 July 2007, is available in English at the following web address:
http://www.garanteprivacy.it/garante/doc.jsp?ID=1426858 .
[37] Article 21, paragraph 2 of the Data Protection Directive.

certain member state and also to provide any possible data subject with the possibility to enforce the rights as acknowledged by the Data Protection Directive.

4.2.2 Articles 10 and 11 of the Data Protection Directive: the information to be given to the data subject

As we have above highlighted, the data processing in general must be inspired to full transparency, especially with regard to the data subject, in order to make the data subject first of all aware that his data are being processed, and also to inform the data subject on the main features and conditions of the processing of his data. This information is important also because it enables the data subject to correctly enforce his rights under the Data Protection Directive.

It is worth it recalling that the information to the data subject is fairly considered as one of the fundamental rules of a lawful personal data processing. As pointed out in this section of this deliverable dealing with the Data Protection Directive, the obligation of providing with the notification the national data protection authority may be simplified or exempted by national data protection law of the member states; as to the need to obtain the consent of the data subject, we will see that the Data Protection Directive itself provides for some exemptions, and leaves member states free to determine further cases of exclusions. In contrast, with regard to the information requirement, exemptions and limitations are very circumscribed, both at a European and also member state national level.

Article 10 of the Data Protection Directive provides a list of the mandatory information that the data subject should receive prior that the Controller begins to process his personal data.

The minimum list of mandatory information that the Controller should provide the data subject with is as follows: the identity of the Controller and of his representative, if any; the purposes of the processing for which data are intended; the extent of data communication, intended as the recipients or categories of recipients of the data; specification whether providing of personal data is mandatory or voluntary together with specification of the possible consequences of failure to provide them; express acknowledgement of the right of access to and the right to rectify the data concerning the data subject.
The information already known by the data subject does not need to be provided to him.

Article 11 of the Data Protection Directive takes care of the issue of personal data that are not gathered directly from the data subject, yet form third parties, and specifies the time when the Controller has to inform the data subject that it has collected personal data relating to him from other third parties.

In said case the mandatory information should be given to the data subject at the time when the Controller records the personal data or, if the Controller is to communicate the data to other third parties, the information to the data subject should be provided no later than the time when said disclosure of personal data takes place.

The foregoing does not apply in case the fact of providing the data subject with the mandatory information proves to be impossible or it would require a disproportionate

effort or if the applicable law expressly requires the recording or disclosure of the relevant personal data. These exemptions may be set forth by member states, which must as a counterbalance provide also for appropriate safeguards. As an example of exemption under the Data Protection Directive we may recall the processing for statistical purposes or for the purposes of historical or scientific research.

4.2.3 Article 7 of the Data Protection Directive: the criteria for a legitimate processing of personal data

Article 7 of the Data Protection Directive lists the six grounds for a legitimate processing that any personal data processing has to meet in order to be lawful, and it reads as follows: "*Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).*".

From the foregoing it may be derived that the consent is one of the mandatory ground for a lawful processing of personal data, and that only when specific circumstances occur, the consent of the data subject may not be obtained.

Looking at the cases when the consent of the data subject is not required, it may be reckoned that the Data Protection Directive has strived to find a fair counterbalance between the consent requirement and the burden to obtain it that is posed on the Controller. The output of the counterbalancing assessment is not asking for the data subject's consent when the above specified cases or circumstances occur since in said cases the burden on the Controller would have appeared not to be justified in light of the specific personal data processing purposes pursued by the Controller.

This is why the consent is not necessary if the Controller performs the personal data for performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or when the Controller uses the personal data to comply with applicable laws and regulations to which the Controller is subject to; or in case the Controller processes personal data in order to protect the vital interests of the data subject; or if the processing of personal data results functional to performance of a task that is performed 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 also when the Controller processes the personal data in pursuing of one legitimate interest of the Controller itself or of the third parties that personal data are disclosed to, save the case in which said legitimate interest is beaten by the interests for fundamental rights and freedoms of the data subject which requires protection.

4.2.4 Articles 8 and 9 of the Data Protection Directive: the special categories of processing

Article 8 of the Data Protection Directive sets forth the conditions for a lawful processing of the so named sensitive and judicial data.

Sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life; judicial data are data relating to offences, criminal convictions or security measures. Data relating to administrative sanctions or judgements in civil cases are not granted the same high degree of protection, but member states may provide that for their processing it is necessary the supervision of an official authority.

Sensitive and judicial data are granted a higher degree of protection, resulting for example in tighter data security measures to be adopted, in a greater number of requirements by the Controller, in specific intervention from the local data protection authorities (for example authorizations), due to the particular kind of information that they relate to, also considering the more significant impact and risks that their unlawful processing may have on the data subject's life and rights.

Sensitive data may be processed exclusively if one of the following conditions is met: if the data subject has given his explicit consent; when the 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 the consent; when the Controller processes said data to comply with obligations and specific rights in the field of employment law in so far as he is authorized by national privacy law providing for adequate safeguards; when the 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; the processing is necessary for the establishment, exercise or defence of legal claims.

In case the processing of sensitive data is necessary with regard to purposes relating to medical and health-care related activities, and it is necessary to provide care or treatment, the above outlined limitations do not apply.

Judicial data can be processed only under the control of an official authority, or if suitable specific safeguards are provided under national privacy law of the member states, subject to derogations which may be granted by the member state under national provisions that provide for suitable and specific safeguards. A complete register of criminal convictions can be maintained only under the control of official authority.

Article 9 of the Data Protection Directive finds a balance between the right to data protection and the right to freedom of expression, stating that member states have to set forth exemptions or derogations with regard to the processing of personal data that is performed only for journalistic purposes or the purpose of artistic or literary

expression, only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

4.2.5 Articles 12, 13, 14 and 15 of the Data Protection Directive: the privacy rights of the data subject

We have seen that the information requirement imposes on the Controller the obligation to provide a set of mandatory information to the data subject. This obligation is deeply linked with the articles of the Data Protection Directive setting forth the rights of the data subject.

It comes indeed as a clear reasoning that without the necessary information on the processing of his data, the data subject would not be able to enforce his rights.

This is also connected with the principle of a fair and transparent data processing: the fact that the Controller must expressly and clearly states what he does with the personal data enables the data subject to know who processes his data, why, how, who has access or receives his data, and who are the subjects to contact to ask for information or for actively intervening on the processing of his personal data.

As a general comment, we may say that the privacy rights of the data subject may be split into two categories: rights of information and rights of intervention.

The rights of information are the rights of the data subject to receive specified and detailed information on the features and conditions of the processing of his personal data. Further to the obligations imposed to this regard to the Controller, the Data Protection Directive also acknowledges to the data subject specific rights to ask for information, and also poses on the Controller a specific obligation to reply to the data subject's requests.

Together with the information rights, the data subject has also intervention rights, in the sense that he can also actively intervene on the processing of his data for example asking that his personal data be amended, updated, deleted, made anonymous. The data subject may also ask for block of the data processing for breach of law and may further oppose to the personal data processing for legitimate reasons.

In this way the data subject is provided with control and a certain degree of authority on the activities that the Controller may perform on his data.

The Data Protection Directive also provides for exemptions and limitations to the possibility of the data subject to enforce his rights. This because it is necessary to find a balance between the data subject's rights and the kind of processing that is considered. For example the data subject could not ask to a public authority to block the processing of his data, provided said processing is performed in line with applicable law.

As it always is the case when it comes to the data protection legislation, the latter provides for a set of rules and provisions that guarantee a fair and lawful processing of personal data, but of course the data protection legislation may not be used as a means to infringe or circumvent other legislative provisions.

Coming to the specific privacy rights of the data subject, Article 12 of the Data Protection Directive lists the privacy rights of the data subjects, which may be

summarized as follows: to obtain confirmation as to whether or not data relating to the data subject 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; to obtain communication in an intelligible form of the data undergoing processing and of any available information as to their source; to obtain knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions; to obtain as appropriate the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of the Data Protection Directive, in particular because of the incomplete or inaccurate nature of the data; to obtain notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the foregoing, unless this proves impossible or involves a disproportionate effort.

It is worth it outlined that the data subject should be enabled to enforce his privacy rights without constraint, at reasonable intervals and without excessive delay or expense.

When specific circumstances occur, the data subject under Article 14 of the Data Protection Directive[38] is also acknowledged the rights to object at any time to the processing of his personal data on compelling legitimate grounds that relate to his particular situation, and may also object, on request and free of charge, to the processing of his personal data which the Controller anticipates being processed for the purposes of direct marketing.

The data subject has further the rights 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 said disclosures or uses.

Article 13 of the Data Protection Directive takes into account the cases under which the privacy rights of the data subject may undergo restrictions or limitations, which are basically significant reasons in which the rights to data protection of the data subject are overcome by superior legitimate interests and represent a necessary measure to safeguard said superior legitimate interests.

Said exceptional cases may be summarized as follows: safeguard of national security, defence, public security; prevention, investigation, detection and prosecution of criminal offences, or breaches of ethics for regulated professions; in case of an important economic or financial interest of a member state or of the European Union, including monetary, budgetary and taxation matters; in relation to a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of

[38] Article 14 (The data subject's right to object) of the Data Protection Directive reads as follows: "*Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data; (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses. Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).*".

official authority in some of the cases above mentioned; in order to protect the data subject or the rights and freedoms of others.

Article 15 of the Data Protection Directive is concerned with the matter of automated individual decisions, notably on decisions concerning the data subject that are taken only on the basis of automatic means and reasoning, and it provides that said kind of automated decisions are basically permitted only when they are taken upon execution of a contract or for performance of a contract on condition that the request to enter or perform the contract, submitted by the data subject, has been satisfied, or in presence of adequate measures that protect the data subject's legitimate interests, for example arrangements that permit to the data subject to present his point of view; or in case said automated decisions are authorized by operation of laws, which also provide for measures to safeguard the data subject's legitimate interests.

In other cases, automated decisions are not allowed, since the individual is acknowledged the right not to be subject to a decision which produces legal effects concerning him or that significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the individual, such as the individual's performance at work, creditworthiness, reliability, conduct, etc.

The rationale of Article 15 of the Data Protection Directive is to protect the individual's identity limiting the possibility to take decisions having impact on him through automated means, since the individual should undergo the consequences of a decision when this is taken using the human criterion and the human being, since a decision or judgment that may impact on the life of an individual may not be the result of information provided by a machine [39].

4.2.6 Articles 16 and 17 of the Data Protection Directive: confidentiality and security of the processing of personal data

Articles 16 and 17 of the Data Protection Directive tackle the important matter of confidentiality and security requirements of the personal data undergoing processing activities.

The issues of personal data security and confidentiality are among the foundation principles for a lawful data processing under the Data Protection Directive. Indeed, it may be said that the European data protection legal framework in principle provides for a set of rules, limitations and requirements that have to be satisfied in order to process personal data while observing the legitimate interests and rights to data protection of the data subjects, notably of the subjects whose personal data are processed.

Since the activity of data processing is considered as a whole and under all of its elements under the Data Protection Directive, it had been necessary to specify also confidentiality and security obligations for the subjects involved in the data processing in order to protect data during the static time of processing (notably storage of data within databanks) and the dynamic time of processing (notably when data are made available and communicated to third parties).

[39] RICCARDO IMPERIALI, ROSARIO IMPERIALI, "Codice della Privacy"; Roma, *Il Sole 24 Ore*, 2005.

To this regard, the confidentiality and security provisions of the Data Protection Directive represent a due corollary to the rational of the legislative implant that is aimed at protecting personal data. The other provisions relating for example to obligations towards the national data protection authorities (for example notification, prior checking) or towards the data subject (for example information and consent requirements), and the sanctioning implant established for violations of the law provisions, would have lost their effectiveness if they had not been supported by provisions aimed at guaranteeing the security and confidentiality of the processing of personal data.

The aforementioned approach (security and confidentiality obligations as going together with other obligations on the data processing) is a peculiar feature of the Community legislation. In other countries out of the European Union, as for example the United States, the approach is different in the sense that high attention is posed on the issue of security and confidentiality of data, yet not the same attention is paid to the general *right to data protection*, due to the circumstance that this right has not yet been acknowledged by act of laws, as it has been the case in Europe [40].

The security obligations provided for by the Data Protection Directive impose on the Controller the obligation to implement the necessary measures and to take the necessary actions to protect the personal data processed, with regard to the static as well as the dynamic phase of the data processing.
The security measures that the Controller has to implement are physical, technical and organizational security measures, and said measures should have regard to data that are processed both by electronic and without electronic means (for example, in paper form).

The foregoing implies for example that the Controller has to adopt physical security measures to protect the places where data are stored (intended as the Controller's premises, and the offices and places where data are kept, both in electronic and not electronic format). Moreover, the Controller has to implement the technical measures necessary to protect personal data, for example appropriate technical safeguards to protect the servers in which data are stored, and to prevent unlawful use or access to the personal computers or other electronic device deployed for the electronic data processing.

As to organizational measures, these are concerned with the set of instructions, policies, internal procedures that the Controller implements in order to ensure that any subject that processes personal data acts in compliance with applicable data protection legislation and with the instructions of the Controller itself, for example internal policies on the way in which paper documents should be used by employees of the Controller, how to cerate a 'safe' password to access the electronic device used for the data processing, etc.

It seems worth it highlighting the importance of the organizational security measures, and the fact that they are deeply linked with the technical security measures. Indeed

[40] In the United States security obligations are imposed by dedicated legislate, as for example with regard to corporate governance legislation, see Sarbanes-Oxley Act, Pub. L. 107-204, Sections 302 and 404.

the organizational security measures represent the 'rules' of the Controller on how personal data have to be processed.

In this set of internal procedures and policies, there are also the instructions on the use of the technical device deployed to process personal data. To this regard, the Controller may adopt the best technical security measures in principle, but in lack of specific organizational procedures and instructions said technical measures undergo the risk of losing effectiveness.
Indeed, the technical security measures are in the end used and implemented by the human being, and if the latest does not act so as to permit the proper and exact functioning of the technical measures, the same loose efficiency and are like 'non implemented'. This is the reason why the human being in the technical security area is often considered as the 'weak ring' of the chain.

The aim of the above mentioned security measures should be to prevent the occurring of risks and damages to the personal data processed, to react in case the potential threat begins real danger, and to detect in order to understand what has gone wrong and also in order to limit possible adverse effects and damages to the personal data processed when they are under threat.

Article 17 of the Data Protection Directive provides that appropriate technical and organizational data security measures are to be implemented by the Controller in order 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.
In consideration of the state of the art and the implementation costs, the security measures adopted by the Controller have to guarantee a security level that is appropriate with regard to the risks represented by the data processing and also the nature of the personal data that have to be protected.

Reading Article 17 of the Data Protection Directive it appears clear that the security obligations posed on the Controller are significant.

First of all, Article 17 basically asks the Controller to protect personal data against any possible risk that may jeopardize them.
Furthermore, making reference to the state of the art implies that the Controller should constantly verify the security measures already adopted against the technical innovations and, as necessary, the Controller should update or replace the security measured already in place.

If we step into the technical security world, we would found the following concepts.
Security is a process, which starts with an internal audit to assess what is the situation at stake, what are the assets to be protected, and what has so far been done to reach protection.
Furthermore, it is necessary to analyze the existing and possible risks, and perform a risk assessment in order to understand if what is in place is enough or if more has to be done.
Once the appropriate security measures have been implemented, it s necessary a constant monitoring and check of the circumstances in order to ensure that the security architecture works properly, and also in order to intervene by updating, replacing and amending it according to changes occurred in the technical state of the

art, in the specific reality in which the security measures are in place, and also in the applicable legislation.

The aforementioned concepts have been dragged by the Data Protection Directive into the security obligations imposed on the Controller for a lawful processing of personal data.

The data security measures should also be fine tuned to the personal data processed, in the sense that they should change and adapt according to the different categories and kind of personal data that they aim to protect. We may for example say that a higher degree of protection is required for sensitive data, because they are information relating to the very intimate and personal sphere of the data subject and also in light of the more significant possible consequences deriving to the data subject in case of misuse of sensitive data.

Articles 16 and 17 of the Data Protection Directive take into account also the possible involvement in the data processing of third parties, specifically they provide rules applicable to the data processor.

The processor is a subject that acts on behalf of and under the instructions received by the Controller. In order to guarantee lawfulness of the outsourced data processing, and that the same reflects the same level of security and lawfulness than that of the Controller, the Controller has an obligation to select as data processor a subject providing sufficient guarantees as to the technical security and organizational measures deployed to process personal data, and as compliance with those measures. The Controller and the data processor usually govern the respective duties and liabilities by contract or other legal act that specifically binds the data processor to the Controller.

The issue of outsourcing of data processing activities by the Controller to third parties is ruled by the Data Protection Directive together with that of security and confidentiality because the provisions relating to the data processor are aimed at guaranteeing security and confidentiality, also when the Controller is no more the only subject processing personal data, so also in case of third parties intervening in the data processing by act of the Controller.

4.2.7 Articles 20 and 27 of the Data Protection Directive: prior checking and codes of conduct

Article 20 of the Data Protection Directive lays down the so called prior checking procedure.

Member states have to establish what are the data processing activities that are likely to present specific risks to the rights and freedoms of the data subject and have to make sure that these processing activities undergo examination prior to relevant beginning. These prior checks should be performed by the competent national data protection authorities after having received a notification from the Controller or the data protection official, who, in cases of doubt, must consult the national data protection authority. It is also provided that member states may perform prior checks in relation to preparation of a measure coming from the national parliament or which

is based on such a legislative measure, which defines the nature of the processing and set forth appropriate safeguards.

The aim of this provision is to ensure that when the personal data processing is likely to cause specific risks to the rights and freedoms of the data subject, said processing is notified to the national competent data protection authority to be verified before the data processing starts, thus for prior checking.
The prior checking mechanism assigns to the national competent data protection authority the right to be informed on data processing operations that may result in a risk for the data subject, and also recognizes to it the authority to intervene setting forth the measures to be complied with for said processing, or even blocking it.
The assessment of the level of risk that a processing of personal data may present is to be determined against the nature of the data that are to be processed, the features of the data processing or the consequences that the data processing may have on the rights, freedoms and dignity of the data subject.

In consideration of the facts that the evaluation under the prior checking mechanism is on a case-by-case basis criterion, and that is based on the evaluation of the national data protection authority, that should be aware of what happens within the boundaries of the jurisdiction of its competence, the prior checking instrument is proving an effective and efficient tool to link regulatory provisions to the factual reality and also to monitor and discipline the data processing activities that may cause concerns from a data protection law perspective.

Article 27 of the Data Protection Directive is posed upon a rationale similar to that of the prior checking mechanism, and it encourages the implementation in member states of code of conducts that should contribute to proper implementation of the national data protection legislation, taking into account the specific features of the various sectors in which the codes of conduct are issued.

The national legislation should provide so that trade associations and other bodies representing other categories of Controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes can submit them to the opinion of the national data protection authority. The national data protection authority has the duty to verify that the proposed codes of conduct are in line with the applicable national data protection legislation, and as appropriate they should also seek consultation with the data subjects or their representatives.
The same duties of verification and consultation are acknowledged by article 27 of the Data Protection Directive to Art. 29 Data Protection Working Party, and the Commission can ensure that appropriate publicity is given to the codes of conduct that have been approved by Art. 29 Data Protection Working Party.

The constant attention of the Data Protection Directive to means such as the prior checking and the codes of conduct is important since as above outlined these mechanisms allow to link the data protection legislation to reality, and also to provide for regulatory rules that take into account the specific area in which said provisions are to be applied.

Considering the wide definition of *processing of personal data*, we may say that the areas in which the data protection legislation does not apply are very limited. It follows that a limited numbers of legislative acts such as the Data Protection Directive and the e-Privacy Directive (which set forth the main principles and rules of the data

protection legislation) and the member states national data protection laws and regulations (which represent the implementation of the EU data protection legal framework) cannot discipline all the possible scenarios in which the data protection legislation is to be applied, and cannot consider all the possible issues, especially with regard to sectors with specific peculiarities and features. Just to give some examples, we may think to the particular issues arising in the area of health care, clinical trials, in the banking and insurance business, in the employment area, and so on.

The solution adopted has been to introduce in the data protection legislation some mechanisms that allow introducing law provisions that one the one hand are targeted on specific issues, and on the other hand may benefit of a constant contact with the reality in which they are to be implemented.

From a doctrinal perspective on the creation of data protection legislative acts, the fact that the data protection issue will be ruled by legislative acts (EU Directives and national laws) and also by regulations of local authorities and codes of conducts allows to get the benefits of both the so named legislative and the self-regulatory approaches.

The legislative approach takes the view that it should be the legislator that issues the privacy legislation; the self-regulatory approaches leaves said task to the voluntary regulation.
Positive element of the legislative approach is that it provides for uniformity and the possibility of enforcement, negative element is that it is not flexible and not always able to take into account the specific needs of individuals. Positive element of the self-regulation approach is that it is not rigid and is capable of fast changes on the basis of the specific scenario to be governed, but it does not ensure uniformity and enforceability.
The codes of conduct mechanism combines the benefits of the two above referenced approaches, in the sense that it combines flexibility and adaptability with uniformity and enforcement in relevant sectors[41].

4.2.8 Articles 25 and 26 of the Data Protection Directive: the transfer of personal data to third countries

Whereas 8 of the Data Protection Directives reads as follows: "I*n order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States…. ".*

It stems that one of the aims of the Data Protection Directive is to harmonize the data protection legislation of the member states to provide for a homogeneous level of data protection within the Community. The result is that within the Community it is afforded the same degree of protection of personal data, hence personal data may be freely communicated among Controllers established within the safe boundaries of the

[41] RICCARDO IMPERIALI, ROSARIO IMPERIALI, "Codice della Privacy"; literary work cited.

Community. The issue comes when data are to be transferred out of said safe boundaries, notably to third countries that are not part of the Community.

Article 25 of the Data Protection Directive provides that the transfer of personal data towards third countries 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*.".

The adequacy of the level of data protection offered by the third country might be determined by the European Commission considering the nature of the personal data to be transferred, the purposes and the duration of the proposed data processing operations, the country of origin and the country of final destination, the law provisions that are applicable in the third country where personal data are transferred, and the professional rules and security measures that are applied in said country.

There should be a constant flow of information and updating between the European Commission and member states on the cases in which a third country is considered as ensuring an adequate level of data protection. The transfer of personal data should be prohibited by member states when the transfer is towards third countries that have been recognized by the European Commission as not providing for an adequate level of data protection.

It is possible for the European Commission to enter into negotiations with the third countries in order to remedy the lack of adequate data protection, and in the end the said level may be assessed as adequate.

The so-named "Safe Harbor Principles"[42] are an important result of said activity of negotiation of the European Commission with the US Federal Government for the provision of an adequate level of data protection when data are transferred to the United States. Another example is the negotiations with the United States for the agreement on the transfer of air passenger name record (PNR)[43]. Furthermore, the European Commission has recognized the following third countries as providing an adequate level of data protection: Argentina; Canada; Switzerland; Hungary; Guernsey and Isle of Man[44].

Article 26 of the Data Protection Directive provides for a set of conditions that, if met, allow the transfer of personal data to third countries not providing for an adequate level of data protection, for example when the data subject has given his unambiguous consent to the transfer; when the transfer is necessary to perform a contract between the data subject and the Controller, or to implement pre-contractual measures following the data subject's request or to finalize or perform a contract between the Controller and a third party that is concluded in the interest of the data subject; when the transfer is necessary or required by law on the ground of important public interests, to establish or defend legal claims or to protect the data subject's vital interests.

[42] For further information please refer to: http://www.export.gov/safeharbor/.
[43] For further information please refer to: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp145_en.pdf
[44] For further information please refer to: http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm.

If a Controller wishes to transfer personal data to a third country without an adequate level of data protection, it may be authorized to do so by the relevant member state if it submits adequate data protection safeguards, particularly consisting of appropriate contractual clauses.

Lastly, the European Commission may authorize the transfer of personal data towards third countries without an adequate data protection level upon enforcement of certain standard contractual clauses offering sufficient safeguards. The 'Model Contract' is the set of contract provisions contained in the decision of the European Commission, and until the time of drafting of this deliverable, the European Commission has issued three sets of Model Contract: Commission Decision (2002/16/EC) of 27 December 2001 on the transfer towards data processors established in third countries; Commission Decision 2001/497/EC of 15 June 2001 and Commission Decision C(2004)5271 of 27 December 2004 on the transfer towards Controllers established in third countries [45].

The European Commission's decisions relating to the transfer of personal data toward third country not providing for an adequate level of data protection have to be implemented by the member states by adoption of the necessary measures

4.2.9 Articles 29 and 30 of the Data Protection Directive: Working Party on the protection of individuals with regard to the processing of personal data

Article 29 Data Protection Working Party (the Working Party on the Protection of Individuals with regard to the Processing of Personal Data) is set up by article 29 of the Data Protection Directive [46].

The components of Article 29 Data Protection Working Party are the representatives of the data protection authorities designated by each member state and of that established for the Community institutions and bodies, together with a representative of the European Commission. Article 29 Data Protection Working Party adopts its own rules of procedure, has advisory status and acts independently.

Article 29 Data Protection Working Party has different duties; among others, it is in charge of the following activities: fostering uniform application of the Data Protection Directive upon examining questions on the application of national measures adopted under the Data Protection Directive, and also informing the European Commission about divergences detected between laws or practices of member states when they may affect the equivalence of data protection for individuals; providing the European Commission with opinions about the level of data protection in the Community and in third countries; advising the European Commission on proposed amendments to the Data Protection Directive, about measures aimed at safeguarding the data protection rights and other proposed Community measures affecting it; providing opinions on codes of conduct drawn up at a Community level (please see the above section of this deliverable 4.2.7); drawing up an annual report on the situation relating to the data protection rights in the Community and in third countries, which is notified to the

[45] For further information please refer to:
http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm.
[46] For further information please refer to:
http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm.

European Commission, the European Parliament and the Council , and it is also made public.

Article 29 Data Protection Working Party plays an important role as to harmonization of national member states data protection laws and regulations.

Most of all, Article 29 Data Protection Working Party , at its own discretion and on its own initiative, submits recommendations and adopts documents in relation to any issue and matter that relates to data protection that id deems to be relevant.
The European Commission and a competent committee are provided with the opinions and recommendations of Article 29 Data Protection Working Party , and Article 29 Data Protection Working Party in turn has to be informed by the European Commission about the actions taken as a result and in response to its opinions and recommendations through a report submitted to the European Parliament and the Council, and that is also made public.
This procedure has been set up in order to ensure that the opinions and recommendations of Article 29 Data Protection Working Party are granted the appropriate level of attention and follow-up.

So far, Article 29 Data Protection Working Party has been very active and thanks to its constant efforts and work many difficult matters have been tackled, there is a continuous updating towards the state of the art in technology and business trends, and practical and very useful guidance has been provided to member states in relation to proper application of the European data protection legislation.

4.3 Application to network monitoring of Directive 2002/58/EC (ePrivacy Directive)

4.3.1 Scope and extent of application

The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, herein referred to as the "ePrivacy Directive")[47] has replaced the Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[48], which has first translated the legislative framework provided by the Data Protection Directive in to principles and rules to be applied in the telecommunications sector.

Directive 97/66/EC has been replaced and repealed since it *"has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used"*[49].

[47] Directive 2002/58/EC 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 communication), O.J. L 201/37, 31 July 2002.
[48] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector, O.J. L 53, 14 January 1998.
[49] Recital 4 of the Directive 2002/58/EC.

It should be noted that the electronic telecommunications area is a difficult issue to be addressed from a privacy law perspective, since the regulatory provisions have to be applied and enforced in the so named *virtual* world, and in some cases difficulties arise. Moreover, the constant developments of new technologies and solutions, such as for example Internet applications and services, digital technologies, biometrics, interactive technologies, ubiquitous services, coupled by the circumstance of the significant wide spread and use of these technologies, that nowadays are available and deployed by an always increasing number of users have reached the result that on one side the new technologies are part of our lives, but on the other side they may pose significant risk of our right to data protection.
This is why it has been perceived since the beginning the need to have a specific set of law provisions governing electronic communications services, also taking into account the fast changing reality in which said provisions are to operate .

Indeed, the European Commission recently felt the need to further update and amend the ePrivacy Directive. On 13 November 2007, the Commission adopted a proposal to amend, among others directives, also the ePrivacy Directive, with the aim to enhance the protection of personal data and the privacy of individuals in the electronic communications sector, in particular, by strengthening security-related provisions and enforcement mechanisms[50].

The scope of the ePrivacy Directive is clarified under article 1 of the same, that is to provide harmonization of the member states provisions concerning the right to data protection with regard to the peculiar electronic communications sector in order to guarantee an equivalent level of data protection within the Community, and also in order to guarantee and foster the free movement of data and of electronic communications equipment and services within the Community.

As to the extent of application, the ePrivacy Directive in article 3 specifies that it applies to "*the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community*".

Taking into consideration the different kind of technical devices used within the electronic communications sector, the ePrivacy Directive held the so named principle of 'technological neutrality', in the sense that it disregards what is the specific technical instrument used to provide the electronic communications service, since it applies anyway.

4.4 Main principles and rules to be applied

4.4.1 Articles 4 and 5 of the ePrivacy Directive: security and confidentiality of the communications

Article 4 of the ePrivacy Directive poses an obligation to adopt *appropriate technical and organisational* measure to protect personal data, specifying that *having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented*.

[50] Art. 29 Data Protection Working Party has provided some comments on the proposed amendments, please refer to WP 150, Opinion on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive) adopted on May 15, 2008 and available at the following web address : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf .

The approach taken by the ePrivacy Directive recalls that of the Data Protection Directive as to the issue of security, in the sense that it is posed on the entity processing personal data the duty to adopt appropriate security measures, and benchmark criterion to evaluate the appropriateness of these measures is again the state of the art.

As a difference, the ePrivacy Directive takes also into account the implementation costs, and on the other hand it poses the burden of ensuring security not only on the service provider, but also on the network provider: paragraph 1 of Article 4 of the ePrivacy Directive reads that: "*The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security…* ".

Furthermore, the service provider should also specifically inform its user in case there are particular risks for the network security, and where said risks are not under the control of the service provider and cannot be prevented with the security measures adopted by the service provider, the latest has an obligation of notifying users of any possible remedy, also covering their possible costs.

Article 5 of the ePrivacy Directive deals with the matter of confidentiality of electronic communications, which is acknowledged at a European level and also in many if not all member states legislations as a fundamental right of the individual, and it is often regarded a right that goes together that of freedom of speech.

The right to confidentiality in communications is basically transposed from the paper communications to the electronic communications, since the means used to exchange the communications are irrelevant: an individual has the same right to confidentiality, irrespective of whether the communications is sent by post or by e-mail.
Article 5 of the ePrivacy Directive starts from the beginning saying that: "*Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation…* ".

The aforementioned provisions may undergo limitations and exemptions only when it is necessary, appropriate and proportionate in order to protect superior public interests such as for example the national security or defence, the public security, and also for the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications system.

Member states furthermore should implement national legislation that prohibits the actions of listening, tapping, storing or performing of other kinds of interception or surveillance of communications and the related traffic data that is carried out by subjects other than the users themselves.
These activities may be performed either with the users' specific consent or if they are legally authorised, and save for the activity of technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality, and other legally authorized recording of communications together with the related traffic data when it is performed in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

Member states shall also ensure that their national legislations allow to use electronic communications networks for the purpose of storing information or gaining access to information that is stored in the terminal equipment of a subscriber or user only when the relevant subscriber or user has been informed according to the information requirements set forth by the Data Protection Directive, and the data subject is also provided with the right to refuse such processing.

The foregoing applies except for the activities of technical storage or access performed *for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*[51].

The rationale of the above provisions should be found in the consideration that in the terminal equipment that the user deploys to access and benefit of the electronic communications services offered by service providers in the majority of cases the user stores personal information, hence the right to confidentiality in the communications has to be guaranteed not only with regard to the communication itself, but also with regard to the technical instrument used to access the electronic communications services and the information therein contained.

This is true especially if we think to invasive and tracking technologies such as tags, pervasive cookies, spy wares, web bugs, hidden identifiers, etc., which present the high danger of being invisible to most of the users, while they can download information on the user's equipment, gather information from it, and also track the online user's activities.

With specific regard to the use of cookies, Recital 25 of the ePrivacy Directive recognizes as legitimate their use when it is aimed to certain specified purposes, for example to evaluate and analyze effectiveness of website design and advertising, to verify the identify of the user, to ease performance of the services offered.
However, even though legitimate, the use of cookies has to be notified to the user according to the information requirement set forth by the Data Protection Directive, and user should always be given the opportunity to block cookies or similar device from being stored on his terminal equipment.

If cookies are really necessary to access some specific web contents or features, and said necessity may be assessed with objective and also technical evidence (that is if the web site cannot really operate in the absence of cookies, and at the relevant current time no other technical solution is available) the acceptance by user of cookies may be posed as a necessary condition to access the specific website content or features, always provided that user is duly informed and that the purposes for which cookies are deployed are specifically stated and also legitimate.

4.4.2 Article 6 of the ePrivacy Directive: traffic data

In general terms, traffic data should be either erased or made anonymous when they are no longer needed to transmit the relevant electronic communication, with the

[51] Paragraph 3 of Article 5 of the ePrivacy Directive.

exceptions of specific and limited circumstances, such as for example in case of traffic data that are processed for purposes of billing and interconnection purposes (yet only up to the end of the period during which the bill may lawfully be challenged or payment pursued) and, after having obtained the consent of the relevant user, for marketing of electronic communications services or in order to perform value added services (yet only to the extent and for the duration necessary for such services to be provided or to such marketing activities to be pe4rformed).

This rigid approach with regard to the processing of traffic data is due to the fact that the processing of traffic data may expose the privacy of the data subject to high risks. Indeed, said data may be gathered and processed without the data subject being aware of it, and the data subject is in a way 'forced' to generate these data (he generat es them each time he makes use of the electronic communications service).
Moreover, recent technology development, coupled by data processing techniques such as data mining, allow to gather a tremendous amount of information from traffic data, which of course poses serious risks to the user's privacy.

Further obligations for a lawful processing of traffic data are the specific information to be provided to the data subject about the types of traffic data that are processed and also about the specific duration of such processing.
Moreover, traffic data can be processed exclusively by the persons who act under the authority of the service or network provider and who specifically deal with billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or value added services.
Lastly, the traffic data processing activities should be strictly limited to these that are functional to pursue these specific purposes.

The aforementioned limitations apply without p rejudice to the possibility for competent bodies and authorities to be informed about traffic data according to applicable legislation in order to settle disputes, particularly interconnection or billing disputes.

We have above outlined that in case the C ontroller wishes to perform value added services through processing of traffic data, it must seek the consent of the data subject. This provision may appear inconsistent with the rule that exempts fr om the need to obtain the data subject's consent in case the processing is aimed at performing obligations arising from a contract with the data subject [52].

The rational to this 'exception to an existing exception' has to be found in the intent of the legislator to keep a high degree of protection with regards to the processing of traffic data since this activity as above highlighted is deeply linked with the fundamental rights of the individual to confidentiality in the communications and freedom of expression.

4.4.3 Article 9 of the ePrivacy Directive: location data other than traffic data

Article 9 of the ePrivacy Directive starts saying that when it is admissible to process location data other than traffic data, *such data may only be processed when they are*

[52] Article 7 of the Data Protection Directive.

made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.
Furthermore, the data subject should be specifically informed, prior to giving his consent, about the type of location data other than traffic data that are to be processed, the purposes of the processing and the duration of the processing, and whether the data are to be transmitted to a third party for the purpose of providing the relevant value added service.

With regard to the consent of the data subject, the data subject has to be provided with the possibility to withdraw his consent at any time, and must continue to have the possibility, using simple means and free of charge, of temporarily refusing the processing of location data other than traffic data for each connection to the network or for each transmission of a communication.

Lastly, the location data other than traffic data *must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service*.

The definition of what has to be intended with the term ' of location data other than traffic data' is contained in Recital 14 of the ePrivacy Directive, which explains that said data are data that "*May refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded"*.

As above outlined with regard to traffic data, the legislator has guaranteed a higher level of protection for the processing of location data other than traffic data, with regard for example to the need to obtain the data subject consent even though the processing is aimed at providing a service to the data subject, to the limitations in terms of subjects authorized to access and process said data.

The reason of this stricter set of rules lays in the peculiar nature of location data other than traffic data, which are basically information relating to the movements and thus the intimate private sphere of the individual in relation to communications services that are based on the users' localization, and may further represent an invasive and pervasive surveillance of the data subject's life.

4.4.4 Article 12 of the ePrivacy Directive: directories of subscribers

Article 12 of the ePrivacy Directive has a significant impact on marketing activities such as direct marketing, since it rules in details the limitations and conditions to be fulfilled with regard to inclusion into and further use of the individuals' personal data with regard to printed or electronic directories of subscribers that are available to the public or obtainable through directory enquiry services.

Member states shall first of all take measure to guarantee that all data subjects are duly informed, free of charge and also in advance, with regard to the inclusion of their personal data in the aforementioned directories, their purposes, and also any other

possible purpose of data processing. The data subject must be given the opportunity to choose whether being inserted in said directories or not and the specific data to be included, and must also be given the possibility to verify, correct or withdraw the relevant data.

The aforementioned provisions in a sense have changed the world of the direct marketing, since before its enforcement directories might have been freely used for direct marketing purposes. Article 12 of the ePrivacy Directive has restricted said possibility to the data subjects that expressly consented to be called for direct marketing purposes. It seems worth it highlighting that once again the focus of the law provision is on providing the data subject with information necessary to make the choices of his interest.

It is also interesting noting that paragraph 4 of article 12 of the ePrivacy Directive in a way extends the protection steaming from the aforementioned rules on directories so as to take into account also legal entities, since it reads as follows: "*Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected*".

4.4.5 Article 13 of the ePrivacy Directive: unsolicited communications

Article 13 of the ePrivacy Directive states that automated calling systems can be deployed for direct marketing purposes solely after having obtained the prior data subject's consent. Automated calling systems are defined as "*Automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail*".

There is an exemption that applies in case of existence of a business relationship between the Controller and the data subject, notably if the Controller has obtained the data subject's mail electronic contact details within a sale of a product or a service, and in any case according to applicable data protection law, then the Controller is allowed to use said data for direct marketing purposes, but only in relation to its own products or services that are to be similar to these subject matter of the relationship already standing with the data subject, and provided that the Controller gives to the data subject, in a clear and distinct way, the possibility to object to said data processing through means that are easy and free of charge, both upon data collection and on the occasion of each message, and always provided that the data subject has not initially objected the use of his data for marketing purposes.

Unsolicited communications for direct marketing purposes are prohibited either without the data subject's consent or with regard to data subjects not willing to receive said communications, and it is put on the member states the obligation to provide as per the foregoing.

It is also forbidden to send electronic communications for purposes of direct marketing if the sender's identity is disguised or concealed, or when there is no valid address that the data subject may use to address the requests of block of the communications.

As for the above article 12 of the ePrivacy Directive dealing with directories of subscribers and direct marketing, also the protection relating to unsolicited communications is somehow extended to legal entities. The last paragraph (5) of article 13 of the e Privacy Directive indeed states that *the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected*.

4.5 Application to network monitoring of Directive 2006/24/EC (Data Retention Directive)

4.5.1 Article 1 of the Data Retention Directive: scope and extent of application

Directive 2006/24/EC (henceforth, also referred to as the "Data Retention Directive")[53], states that it *aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law*.

The reason that at a European level it has been felt the need of having a common benchmark for data retention legislation in order to fight crimes has been the acknowledgement of the importance of electronic communications as a means used to plan, design and in some case also to commit crimes. It follows that the gathering and monitoring of the data relating to the use of electronic communications have become particularly significant as an effective means to prevent, investigate, detect and prosecute criminal offences, and especially terrorism and organized crimes[54].

Before issuance of the Data Retention Directive, different member states adopted specific laws and regulations ruling on data retention obligations to be fulfilled by service providers in order to prevent, investigate, detect, and prosecute criminal offences.
However, the fact that each member state acted on an individual basis, caused significant differences in the various data retention legislations from both a legal and also a technical standpoint. The concern at a European level was that said discrepancies might have turned into an obstacle to the electronic communication internal market, also in light of the fact that service providers were subject to different national requirements with regard to the types of traffic and location data to be retained and also with regard to the conditions and periods of data retention[55].

Whereas 11 of the Data Retention Directive further explains that *given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by*

[53] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC; O.J. L 105/54, 13 April 2006.
[54] Please also refer to Whereas 7 of the Data Retention Directive.
[55] Please also refer to Whereas 5 and 6 of the Data Retention Directive.

providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.

However, the obligations of data retention pose the issue of an intrusive encroaching into the individual's life, especially with regard to the right to confidentiality in the communications, as acknowledged under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

Said fundamentals rights may indeed be compressed only in specific and limited circumstances, that is only according to applicable law and when this is necessary in a democratic society, among others, in the interests of national security or public safety, to prevent disorders or crimes, or to protect the rights and freedoms of others. Moreover, Whereas 15 of the Data Retention Directive expressly recalls the Data Protection Directive and the ePrivacy Directive, stating that they must be in any case applied[56].

4.5.2 Articles 3 and 4 of the Data Retention Directive: obligation to retain data and access to data

Article 3 of the Data Retention Directive specifies who are the addresses of the data retention obligations.

In general terms, it may be said that providers of publicly available electronic communications services or of a public communications network should retain the data that they generate or process within the relevant jurisdiction during the supply of the relevant communications services.

The data retention obligations extend to the data relating to unsuccessful call attempts, provided that said data are generated or processed, and stored (with reference to telephone data) or logged (with reference to Internet data), by the providers of publicly available electronic communications services or of a public communications network as above identified. The Data Retention Directive does not apply to data relating to unconnected calls.

Data retained may be accessed only by the competent national authorities, in line with the applicable legislative framework, which should always take into account the necessity and proportionality requirements.

4.5.3 Articles 5, 6 and 12 of the Data Retention Directive: categories of data to be retained; periods of retention; and future measures

The data to be retained under the Data Retention Directive are as follows:

[56] Whereas 15 of the Data Retention Directive states as follows: "*Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of that Directive* .".

With regard to the data that are necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

With regard to the data that are necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication.

With regard to the data that are necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone.

With regard to the data that are necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used.

With regard to the data that are necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated.

(3) Concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication.

With regard to the data that are necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

Any data that reveals the content of the communication is expressly excluded from the data retention obligations.

With regards to the periods of retention, these should be *periods of not less than six months and no more than two years from the date of the communication* [57].

Under article 12 of the Data Retention Directive, member states may extend the maximum period of data retention above referred to in case particular circumstances occur. The Commission should be immediately notified, and the other Member States informed thereon, with specification of the grounds for said extension.

The Commission after six months from the above referenced notification, may approve or reject the member state relevant measure. If the Commission does not decide within the above referenced deadline, the national measure is deemed to be approved. In case the measure derogating to the retention time is approved, the Commission might take into consideration the possibility to propose an amendment to the Data Retention Directive.

4.5.4 Articles 7 and 8 of the Data Retention Directive: data retention and data security; and storage requirements for retained data

Article 7 of the Data Retention Directive expressly recalls the security provisions as set forth by the Data Protection Directive and the ePrivacy Directive, and further adds that the data retained should be of the same quality as those that are present on the relevant network, and should also undergo the same security and protection.

Furthermore, appropriate technical and organizational measures should be applied in order to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure, and to ensure that the data may be accessed exclusively by specifically authorized personnel. Lastly, the data, with the exception of the data that have been accessed and preserved, should be destroyed upon expiry of the retention period.

The data retained and any relevant information should be stored in such a way that they may be transmitted to the competent national authorities upon relevant request without any delay.

4.5.5 Articles 9 and 10 of the Data Retention Directive: supervisory authority; and statistics

In order to provide some guarantees with regard to the correct enforcement of the Data Retention Directive and also in order to avoid possible violations of the citizens' fundamental rights and freedoms, article 9 of the Data Protection Directive requires that member states designate one or more public authorities (also the same national data protection authority) that should be in charge of monitoring the measures adopted by the member states to guarantee security of the data stored under the Data Retention Directive within the relevant territory and according to article 7 of the Data Retention Directive.

Furthermore, member states have to make sure that they provide yearly to the European Commission statistics about the retention of the data that are generated or

[57] Article 6 of the Data Retention Directive.

that are processed in connection with the provision of publicly available electron ic communications services or a public communications network .

The issue of data retention has been throughout discussed by Article 29 Data Protection Working Party[58] in different documents[59].
Art. 29 Data Protection Working Party takes the view that any kind of interception, considered as acquiring knowledge not only of the content but also of other data relating to a private communication, particularly traffic data *"constitutes a violation of individuals' right to privacy and of the confidentiality of cor respondence. It follows that interceptions are unacceptable unless they fulfill three fundamental criteria, in accordance with Article 8 (2) of the European Co nvention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 [60], and the European Court of Human Rights' interpretation of this provision: a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention"[61].*

[58] For more information on Article 29 Data Protection Working party see also Section 4.4 Other Re quirements of this document and the fo llowing address:
http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm.
[59] Recommendation 3/97 on Anonymity on the Internet adopted on December 3 1997; XV D /5022/97 final; WP 6; available at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1997/wp6_en.pdf ;
Recommendation 2/99 on the respect of privacy in the contex t of interception of telecommunications, adopted on 3 May 1999; 5005/99/FINAL; WP 18; available at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1999/wp18en.pdf;
Recommendation 3/99 on the preservation of traffic da ta by Internet Service Providers for law enforcement purposes, adopted on 7 Septe mber 1999; 5085/99/EN/FINAL; WP 25; available at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1999/wp25en.pdf ;
Opinion 7/200 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the pro cessing of personal data and the protection of priv acy in the electronic communications sector of 12 July 2000 COM (2000) 385 adopted on 2 nd November 2000; 5042/00/EN/FINAL; WP36; available at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp36en.pdf ;
Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber -crime adopted on 22 March 2001; 5001/01/EN/Final; WP 41;
Available at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp41en.pdf;
Opinion 10/2001 on the need for a balance approach in the fight against terrorism adopted on 14 December 2001; 0901/02/EN/Final; WP 53; available at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf ;
Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the Internat ional Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data adopted on 11 October 2002; 11818/02/EN/Final; WP 64; avai lable at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp64_en.pdf ;
Opinion 1/2003 on the storage of traffic data for billing purposes adopted on 29 January 2003; 12054/02/EN; WP 69; available at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp69_en.pdf;
Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communicatio ns services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]; adopted on November 9 th, 2004; 11885/04/EN; WP 99; available at the following address: http://europa.eu.int/comm/justice_ho me/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf ;
Opinion 3/2006 on the Directive 2006/XX/EC of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amen ding Directive 2002/58/EC, as adopted by the Council on 21 Febr uary 2006 adopted on 25 March, 2006; 654/06/EN; WP 119; available at the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf.
[60] *"It should be stressed that the fundamental guarantees recognised by the Council of Europe on the interception of telecommunications create obligations for Member States regardless of the distinctions made at European Union level according to the Community or intergovernmental nature of the fields addressed"*; Opinion 3/2006 of Article 29 Working Party above quoted.
[61] *"Council of Europe Convention No 108 also stipulates that interference may be tolerated only when it constitutes a necessary measure in a democratic society for the protection of the national interests listed in Article 9 (2) of that Convention (NB the*

In the Opinion 3/2006[62] relating to the Data Retention Directive, Art. 29 Data Protection Working Party identifies the following as its main concerns with regard to the provisions set forth by said Directive.

- Specification of the data retention purposes.

The retained data should be aimed at specific and determined purposes. In contrast, the term "serious crime" used in the Data Retention Directive with regards to the crimes for which data retention is allowed should be further and expressly clarified so as to have a clear definition of the same.
Furthermore, specific provisions should expressly prohibit and curtail with specific safeguards any kind of data processing that does not fall within the identified scope of the data retention.

- Limitation to data access.

The list of competent law enforcement authorities that can have access to the retained data should be made public, and limited to authorities specifically and clearly identified. Access to the retained data should take place on a strict need-to-know basis, only when the access is necessary for purposes of investigation, detection, and prosecution of relevant crimes.
Moreover, there should be measures in place so that any access and retrieval of data be recorded, and said records should further be provided and made available to supervisory authorities, in order to ensure proper and effective monitoring of the use of the retained data.

- Data minimization principle.

The data that may be retained under the Data retention Directive should be first of all clearly identified, and in any case the kind and amount of said data should be kept to the very minimum necessary to achieve the pursued purposes.
A strict necessity test should be performed every time that the list of retained data is to be amended.

- Prohibition of data mining activities.

Since the list of data to be retained under the Data Retention Directive is significant, this large amount of data raises concerns since data represent an important asset for commercial companies, thus there should be a specific and strait forward prohibiti on to use the data collected for data retention purposes for data mining activities.

- Judicial/independent and very detailed assessment of the authorized access.

The access to the retained data should be granted only on a strict case-by-case basis by competent judicial authorities, with the exception of the member states in which the national legislation acknowledges a specific possibility of access, subject to independent oversight.

---

national interests listed in Convention 108 and in the Convention for the Protection of Human Rights are not exactly the same), and when it is strictly defined in terms of this purpose"; Opinion 3/2006 of Article 29 Working Party above quoted.

[62] Opinion 3/2006 on the Directive 2006/XX/EC of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, as adopted by the Council on 21 February 2006 above quoted.

The possible authorizations should also appropriately identify the specific data that are necessary in relation to the relevant specific situation.

- Specific exclusion of purposes other than data retention.

The providers of public electronic communications services or networks that are subject to data retention obligations should be expressly prohibited from using in any way the data collected under the Data Retention Directive for other and different purposes, especially for their own purposes.

- Separation of the systems.

The providers of public electronic communications services or networks that are subject to data retention obligations should implement a specific system for the data retained, logically separated and different from the other systems that they use for business purposes.

- Data security measures.

The data security measures set forth under the Data Retention Directive need to be further specified in more details in order to identify by operation of law what are the minimum security standards in terms of technical and organizational security measures that have to be implemented.

The concerns risen by Article 29 Data Protection Working Party with regard to the Data Retention Directive, and in particular with regard to the opinion that the activity of data retention basically implies interception of communications, seems to be confirmed by a recent survey carried out in Germany, that shows how data retention has influenced the behavior of German people.

Starting next year, data retention law requirements will be indeed implemented in Germany. The law has been the subject matter of debates, but the government decided for implementation[63].

In general terms, it may be said that service providers of electronic communications will have to record information about the communications such as the identity of the sender and the addressee of the communication, the time when the communication takes place. The content of the communication remains out of the scope of the law. The information will be stored for a period of six months and will be made available to law enforcement authorities with regard to certain specific crimes.

Coming to the survey above referenced, this has been performed by the well established German Forsa institute[64] and is concerned with the social impact of data retention in the sense of the impacts that these regulations is having on citizens.

[63] For more information on German data retention law, pleas refer to the following web address: http://www.kreativrauschen.com/blog/2007/11/09/german-bundestag-decides-to-implement-data-retention/.

[64] For more information on the survey on social impact of data retention law provisions in German, please see the article available at the following web address: http://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/.
The study was commissioned by Arbeitskreis Vorratsdatenspeicherung [a network of civil rights and privacy activists], eco [German ISP and Internet Association], Deutscher Fachjournalisten-Verband [German association of specialized journalists] and JonDos GmbH [an anonymizer company].

The output of said research is that 11% of the persons interviewed said that it had already refrained from single telecommunication acts, and 52% would not make use of the telephone or the e-mail with regard to contacts deemed to be of a confidential nature.

It appears that the core of the matter is not only that someone can have access to private communications, but also and particularly that being aware that surveillance means are in place as such changes the behavior of people, who do not feel anymore confident of behaving freely and normally.

Hereinafter the specific results of the survey above referenced.

They have been interviewed a total amount of 1.002 persons, during the days May 27th and 28th 2008. Out of the persons interviewed, 73% of them declared to be aware about data retention; the 11% of them stated to have already refrained from using telephones, cellular phones or e-mail communications in some specific circumstances; 6% of them declared to believe that they have received less communication due to data retention law provisions; 52% of them declared their intention to probably not revert to telecommunication services in some specific cases such as to contact drug counselors, psychotherapists or marriage counselors in light of the data retention law requirements; and 48% of them stated to believe in the necessity of data retention for the purpose of crime prevention.

5 Legal And Regulatory Framework In the Selected Jurisdictions

5.1 List of selected jurisdictions and reasons for the selection

The jurisdictions selected for the Prism project are the following: Austria; France; Germany; Greece; Italy; Switzerland; and the UK.

Hereinafter it follows a brief highlight of the main reasons of said choices, and an overview of implementation of the European Union data protection legislation in the jurisdictions selected for the Prism project.

5.1.1 Reasons for the selection

Austria

Austria's data protection legislation does not have a long history regarding the control of automatic data production but provides for a structured transposition of the Directive 95/46/EC.

Compared to other European jurisdiction – from our experience – Austrian Data Protection Authority is quite strict on data protection issues, which especially applies to data transfers to third countries. Even if the transfer agreement uses EU Model Clauses the agreement still has to be approved by the Data Protection Commission before any transfer takes place. As approval will take minimum 2-3 months this is quite cumbersome for big legal entities.

Furthermore, we have experienced that the implementation of new systems i.e. whistleblowing hotlines also takes a long time.

France

The French Data Processing, Data files and Individual Liberties Act of January 6, 1978 (hereinafter, the "Privacy Act") is one of the oldest in Europe and has in many ways inspired the Directive 95/46/EC.

The French Data Protection Authority (hereinafter, the "CNIL") is also very dynamic in ensuring the application of both the Privacy Act and the Directive 95/46/EC, and is therefore often at the origin of certain decisions which are followed at a European level within Article 29 Data Protection Working Party [65].

A recent example is the decision on how to make "ethics hot lines" compliant with European regulations which has been followed by Article 29 Data Protection Working Party in its Opinion 1/2006 adopted on 1 February, 2006 [66].

The CNIL is very active in informing the general public on the use of their personal data such as over the Internet[67], or for biometric systems, RFID and video surveillance systems.

Moreover, further to its 2006 yearly report, the CNIL established a workshop on the *offshoring* of IT services in order to ensure compliance with the Privacy Act with regard to international transfers of personal data, and information of data subjects. Also, in 2008, French president of the CNIL, Alex Turk, was elected as president of the Article 29 Data Protection Working Party.

France has amended its Privacy Act in August 6, 2004 to adopt a more practical approach and implement simplified notification procedures for specific recurring data processing. Further modifications concern improvement of the CNIL's powers of investigation and sanction against fraudulent data controllers and data processors.

The CNIL has prepared several work papers on the issues raised by new technologies, and in particular the processing of personal data involved by the use of cyber monitoring of IT resources in corporations.

In its last yearly reports, in 2006 and 2007, the CNIL declared the necessity to regulate the development of new technologies which are increasingly intrusive.

Finally, French courts have rendered many decisions on monitoring issues in the context of employment relationship.

In addition, there are also French court decisions and CNIL decisions regarding the monitoring of networks such as Peer 2 Peer networks by collecting societies (e.g. the SACEM) for the purpose of seeking intellectual property infringements.

Germany

[65] For more information on Article 29 Data Protection Working party see also Section 4.4 Other Requirements of this document and the following address:
http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm.

[66] Opinion 1/2006 adopted on 1 February, 2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime; 00195/06/EN; WP 117; available at the following address: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

[67] The CNIL is currently very active in warning the public on the use of their personal data on social networks.

Germany's data protection legislation does not only have a long history regarding the control of automatic data production but also provides for a very structured transposition of the Directive 95/46/EC.

Germany is indeed often regarded as 'role model' for privacy matters in the sense that being compliant with German rules very likely implies also compliance with any other Member States' data protection legislation.

Many new technologies come to market at an early stage in Germany (take RFID chips for example) so that privacy issues around such technologies have also been addressed early in Germany.

Throughout Germany many data protection-related questions are examined and answered by the respective competent data protection authorities. Such practice, still enhanced by the recommendations of the "Düsseldorfer Kreis" for Germany as a whole, leads to a very rich "jurisdiction" on various kinds of data protection-related questions, which promotes a sound basis of "case law" when it comes to evaluate new questions.

Finally, technical data protection is of central importance in German privacy legislation, as it is illustrated by Section 3a Federal Data Protection Act according to which data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible.

In particular, use is to be made of the possibilities for aliasing and rendering personal data anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection.

Greece

Greece has been selected to be among the countries that their jurisdiction concerning personal data and communications protection is considered by the PRISM project for three main reasons:

First, Greece is the only European country that has two different public authorities for personal data protection: the Data Protection Authority (hereinafter, the "DPA")[68] and the Hellenic Authority for the Information and Communication Security and Privacy (hereinafter, the "ADAE")[69]. The former is the authority established in 1997 in accordance to Article 28 of the Directive 95/46/EC, while the latter has been established in 2003 in order to protect the secrecy of mailing, the free correspondence or communication in any possible way as well as the security of networks and information.

Second, Greece is the country that has been granted the highest ranking in the last year's National Privacy Ranking[70] performed by the Privacy International, the human

[68] http://www.dpa.gr/.
[69] http://www.adae.gr/.
[70] Privacy International, The 2007 International Privacy Ranking, available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597.

rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations.

Finally, Greece has been the homeland of the most serious scandal of telecommunications interception during the last few years, when in February 2006 it has been announced that for more than one year during 2004 and 2005, several cell phones have been trapped, including the ones of the Greek prime minister, several ministers, as well as other politicians[71].

Italy

Italy is one of the European Union member states that first enforced the Data Protection Directive, with Law 675 of December 31, 1996[72].

Said law has been repealed and totally replaced by Legislative Decree June 30, 2003; n. 196, in force as of January 1, 2004 and following amendments and integrations (hereinafter, the "Privacy Code"), which represents a consolidated act on privacy legislation[73], and which has also given enforcement to the ePrivacy Directive.

The Privacy Code expressly acknowledges the right to data protection as a fundamental right of the individual (Article 1 of the Privacy Code).

In respect of the previous Law 675/96, the Privacy Code has taken a more practical approach in general terms, removing all the previous requirements which resulted in mere formalities. For example the notification requirement has been limited to specific kinds of data processing that pose higher risks to the right to data protection, the consent requirement is exempted in may cases under which there is a legitimate interest of the Controller to process personal data, even though it should be outlined that said cases have to be specifically identified by operation of law, and are not left to the discretion of the Controllers.

Mr. Stefano Rodotà, who was the former President of the Italian Data Protection Authority (hereinafter, the "Garante"), has also been the President of the EU Data Protection Commissioner, and this circumstance has eased the translation into the Privacy Code of the European approach to data protection issues under many aspects.

The Privacy Code applies almost in the same way to both natural persons and legal entities, which has indeed extended its scope of application.

The Garante is very active in promoting initiatives and actions aimed at fostering and enhancing correct enforcement of the Privacy Code.

The Garante publishes on its web site[74] a weekly newsletter that takes into account the more significant data protection issues that arise, and that also reports the main

[71] cf. for example: V. Prevelakis, D. Spinellis, "The Athens Affair", *IEEE Spectrum*, Volume 44, Issue 7, pp. 26 – 33, July 2007.
[72] Published in the Official Gazette n. 5 of January 8, 1997 – Ordinary Supplement n. 3, available in the Italian version at the following web address: http://www.garanteprivacy.it/garante/doc.jsp?ID=28335.
[73] Published on the Official Gazette n. 174 of July 29, 2003 – Ordinary Supplement n. 123, available in the Italian language at the following web address: http://www.garanteprivacy.it/garante/doc.jsp?ID=1245472; an unofficial English version is also available at the following web address: http://www.garanteprivacy.it/garante/document?ID=311066.
[74] www.garanteprivacy.it.

interventions of the Garante with regard to sanctions issued for breaches of the Privacy Code.

Any individual may easily contact the Garante through its dedicated section of the web site or calling a specific public relation department.

The Garante often organizes or takes part to conferences and workshops on data protection matters[75], has issued several opinions and general provisions on the data processing activities with regards to specific sectors, and it is also promotes on a constant basis the adoption of codes of conduct jointly with the relevant trade associations and other bodies representing other categories for issuing rules and regulations aimed at peculiar data processing activities.

Switzerland

The primary laws governing data protection in Switzerland are the Swiss Federal Data Protection Act (DPA), the Swiss Federal Data Protection Ordinance (DPO) and the Swiss Federal Ordinance on Data Protection Certifications (DPCO). The latest revisions of the DPA and the DPO entered into force on January 1, 2008 and the newly created DPCO also entered into force on January 1, 2008.

We believe that Switzerland should be included in the Prism Project for the following reasons:

(i) Switzerland is not part of the EU or the European Economic Area (EEA), and therefore Switzerland is not subject to the Data Protection Directive. While the European Commission has found that Swiss data protection legislation provides an adequate level of data protection, as is required under the Data Protection Directive (Decision 2000/518/EC), it is interesting to determine if and to which extent the Swiss data protection legislation differs from the legal principles laid down in the Data Protection Directive.

(ii) Contrary to the Data Protection Directive, the definition of `Personal Data` under Swiss data protection legislation also includes personal data of legal entities. This fact raises interesting issues when assessing and interpreting the regulatory framework in daily practice. The same is true for the concept of 'Personality Profiles' which is also unique to Swiss law. Personality Profiles are dealt with under Swiss Data Protection law in the same way as Particularly Sensitive Data.

(iii) Due to rather attractive tax schemes, we have seen many multinationals re-locating their European operations to Switzerland. These re-locations regularly entail that the information technology infrastructure is also relocated.

(iv) Swiss data protection legislation provides for rather unique conflict of law principles in case of data protection violations involving more than one jurisdiction. In fact, the data subject whose data protection rights have been violated can, it his sole discretion, invoke the laws of the country in which (1) the data subject is domiciled provided that the infringer could have anticipated the results of the violation in such country, (2) the infringer has his domicile or

[75] By way of example, in the sectors of health care, public administration, and banking.

(3) the results of the infringement create an impact provided that the infringer could have anticipated the results of the violation in such country.

(vi) The Swiss Data Protection Act has been substantially amended. The amendments entered into force on January 1, 2008. Many practical questions resulting from the amendments have not been sufficiently clarified yet.

(vii) As to the principles of data processing, the Swiss Data Protection Act applies equally to electronic and manual data processing. Personal data may only be processed lawfully. The processing of personal data must be made in good faith and must be proportionate. Personal data may be used only for the purpose specified at the time of its collection and both the fact that personal data are collected and the purpose for processing it must be apparent to the data subjects. The data must be accurate. A lawful justification for data processing may be required. Data security must be ensured.

(viii) With regard to formal requirements, under certain circumstances, data files must be registered with the Federal Data Protection and Information Commissioner. Data subjects have the right to access their data and to have incorrect data corrected.

UK

The key rules regulating data protection in the UK are contained primarily in the Data Protection Act 1998 (hereinafter, the "DPA")[76], implementing the Directive 95/46/EC.

The Data Protection Act has been augmented by the Privacy and Electronic Communications (EC Directive) Regulations 2003[77] (hereinafter, the "E-Privacy Regulations'" which implements the Directive on Privacy and Electronic Communications (Directive 2002/58/EC).

The UK is a good example of "moderate" national transposition of the aforementioned Directives, with the implementing legislation remaining broadly faithful.

However, the concept of 'personal data' under the DPA has been subject to judicial consideration, significantly narrowing the scope of application of the term from the seemingly broad definition provided in the statute and the original Directive.
This interpretation has been challenged by the Commission, which considers UK law to be potentially non-compliant.

The UK Information Commissioner has issued several opinions and general guidance notes on the use of both the DPA and the E-Privacy Regulations and it is also active in promoting good practice in relation to data processing activities.

Specific guidance relating to traffic and location data requirements under the E-Privacy Regulations has been issued; while the Information Commissioner has also published an 'Employment Practices Data Protection Code', Part 3 of which is concerned with monitoring at work, including network monitoring.

[76] http://www.hmso.gov.uk/acts/acts1998/19980029.htm.
[77] http://www.hmso.gov.uk/si/si2003/20032426.htm.

5.2 Brief overview of the legal framework governing network monitoring in the selected jurisdictions

Hereinafter it follows a brief overview of the law provisions applying to network monitoring in the jurisdictions selected for the Prism project.

5.2.1 Austria

The applicable data protection law in Austria is the amended Austrian Federal Data Protection Act 2000 (*Datenschutzgesetz 2000* – hereinafter referred to as "DSG"), effective as of 1 January 2000, implementing the Data Protection Directive and lastly amended on 22 August 2006.

Legal Entities: Like in Italy and Denmark legal entities are granted protection under Austrian privacy legislation.
This is most criticised, especially by legal entities themselves.

Data Processing: Alike the Data Protection Directive, a data processing is widely defined in the DSG and covers any operation or set of operations performed, automatically or manually, on personal data including collection, recording, storing, keeping, sorting, comparing, changing, linking, reproduction, consultation, output, use, committing, blocking, erasure or destruction or any other kind of operation with data of a data application by the controller or processor except the transmission (transfer).

Data Controller and Data Processor: The DSG applies to the party responsible for the purposes for which and the manner in which any personal data is to be used.

Alike the Controller, a data processor may be a natural person or a legal entity. Irrespective of any contractual agreements, the Controller remains responsible for the data processing and the security of the personal data and the following obligations shall be imposed on the processor:

- to use the data exclusively within the scope of the orders given by the Controller; in particular any transfer of data used shall be prohibited in the absence of a relevant order by the controller;

- to provide for all data security measures required pursuant to Section 14 DSG; in particular, the processor may employ only such persons for the relevant services who have either undertaken a secrecy commitment vis-a-vis the processor or who are subject to a confidentiality obligation under law;

- to employ additional processors only with the consent of the Controller and therefore inform the controller of the intention to employ another processor in due time to enable the controller to prohibit such employment, if required;

- if possible in the view of the nature of the services, to jointly with the Controller provide for the required technical and organizational prerequisites for ensuring compliance with the Controller's obligation to give information and to effect rectifications and deletions;

- after the completion of the services, to hand over to the Controller or, at the Controller's request, to keep on the Controller's behalf or to destroy any and all results of the processing operations any and all documents containing data;

- to make available to the Controller any information required for supervising whether the obligations described above are complied with.

Territoriality: The DSG applies to:

- Data Controllers established in Austria that process personal data in Austria;

- Data Controllers established outside Austria but within an EEA Member State that process personal data in Austria through the data Controller's Austrian branch; and

- Data Controllers established outside the EEA that process personal data by using equipment located within Austria for such purposes (other than merely for the purpose of transit of data).

Sensitive Data: The DSG imposes additional requirements for the use of special categories of personal data (hereinafter, the "Sensitive Personal Data") – that is, personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life.
Specifically, the use of Sensitive Personal Data is prohibited unless certain conditions are met, especially including the following:

- the data Controller obtains the explicit consent of the data subject;

- the use is necessary to protect vital interests of the data subject or of a third party where the data subject is physically or legally incapable of giving consent;

- the use is necessary in order to assert, exercise, or defend legal claims, and there is no reason to assume that the data subject has an overriding legitimate interest in excluding the use;

- the use is required in view of the data Controller's rights and obligations in connection with labour or employment law and is admissible pursuant to special legal provisions, whereby the rights of the works council relating to the use remain unaffected.

Notification: Generally, each Controller shall, prior to commencing a data application, submit a notification to the Data Protection Commission containing the necessary information set out in Section 19 of the DSG for the purpose of a registration with the Data Processing Register. Such obligation to notify shall also apply to circumstances which subsequently cause the incorrectness and incompleteness of the notification.

No notification is required especially for data applications which

(i) only contain data already published;

(ii) are carried out by natural persons exclusively for private or family-related objectives; or

(iii) correspond to a standard application. The Federal Chancellor may by ordinance define certain categories of data applications and transmissions from these as standard applications if they are carried out by a large number of Controllers in the same way and if, in the view of the purpose of the use and the categories of data processed, it is deemed unlikely that the data subjects' interests in secrecy requiring protection will be jeopardized. Such ordinance shall for each standard application define the admissible categories of data, the categories of data subjects and of recipients and the maximum duration for which the data may be stored.

In fact there are already some standard applications i.e. for accounting matters, personnel administration, and customer administration.

Storage Term: The storage term for personal data shall be limited to the time necessary for the data processing.

Thus, once the data processing is over, the Controller shall delete all personal data from its records. However, the Controller may be entitled to store the data for an additional time period when provided by applicable laws i.e. litigation purposes or for tax reasons.

Grounds for legitimate use of data: The Austrian implementation of the Directive 95/46/EC provides for a system according to which use of personal data (including processing and transmission) shall be only admissible if permitted or prescribed by the DSG or any other legal provision or if the data subject has given its consent.

The main justifications for the use of personal data are as follows:

(i) consent;

(ii) the data being needed in accordance with the fulfilment of a contract or a quasi-contractual fiduciary relationship; or

(iii) in so far as this is necessary to safeguard the justified interests of the Controller and there is no reason to assume that the data subject has an overriding legitimate interest in its data being excluded from the use.

Consent: As above highlighted under the DSG it is not mandatory to obtain the consent of the data subject, but the consent is contemplated as a justification for the processing of personal data and it is often one of the more straightforward ways to justify said processing.

Consent must be voluntary, informed, and – highly recommended for evidence purposes – given in writing (i.e. by a handwritten signature or by a qualified electronic signature, unless the circumstances allow for a different form).

To ensure that any consent obtained from a data subject is "informed", the data subject must be provided with the following information prior to any use of personal data:

- the identity of the data Controller;
- the purposes of use of personal data;
- the intended recipients or categories and their location (to the extent the recipient is not located in Austria or in another EEA member state, the name and address and whether an adequate level of data protection exists at the location of the recipient);
- the categories of data concerned;
- any other information that might be relevant for the data subject's decision whether or not to give their consent;
- insofar as the circumstances of the individual case dictate or, at the data subject's request, the consequences of withholding consent; and
- that given consent could be withdrawn at any time without giving reasons.

Although the DSG does not contain any language requirement, the concept of "informed" consent generally requires the consent from the Austrian data subjects to be in German in order to enable them to understand without doubt what they consent to. Where the data subjects are proficient in English (or in any other language) consent also may be sought in English (or the other relevant language).

If consent is to be given in writing simultaneously with other declarations, special prominence must be given to the declaration of consent.

Austrian courts are likely to regard consent given under terms of a standard form agreement as invalid and require a separate clause and signature line.

Generally speaking consent may not be implied from an action or inaction on the part of the data subject.

Data Security Measures: For all organizational units of a Controller or processor using data, certain data security measures have to be taken.

Dependent upon the category of data used and the scope and purpose of the use, and taking into account the technical possibilities and economic feasibility, it must be ensured that the data are protected from accidental or unlawful destruction and from loss, that they are properly and are protected from access by unauthorized parties.

In particular the following steps have to be taken:

- the various tasks in connection with the use of data shall be explicitly allocated to the relevant organizational units and members of staff;
- the use of data shall be made subject to the availability of valid orders by competent organizational units and members of staff;

- each member of staff shall be informed on the obligations imposed on him under the DSG and under internal data protection regulations of the organizational unit, including data security provisions;

- the right of access of the premises of the controller or processor shall be regulated;

- authorization for access to data and programs and the protection of data carriers from unauthorized access or use shall be regulated;

- authorization for operation of the data processing equipment shall be defined and each item of equipment be protected from unauthorized operation by adequate preparation of the applied machines and programs;

- records shall be kept to allow for monitoring to the required extent the processing steps actually taken, such as, in particular, alterations, calls and transmissions, in view of their admissibility; and

- the measures taken shall be documented for facilitating supervision and the procurement of evidence.

Information, Access and Refusal: Generally, the provisions set out by the DSG are well in line with those stated in the Directive 95/46/EC.

International Data Transfers: Transfers of personal data from Austria to other EU countries are generally permitted without the need for further approval provided such transfers would be legal within Austria.

The same applies with respect to transfers to Canada, Switzerland, the Isle of Man, Argentina, and Guernsey, which are subject to European Commission findings of adequacy (subject to the fulfilment of certain pre-conditions) in relation to their data protection laws.

Transfers to the US are permitted where the recipient has registered under the Safe Harbor arrangement and provided the transfers would be legal within Austria.

Transfer to the US or any other countries outside the EU that do not provide an adequate level of data protection are legal if based on unmodified or modified versions of the relevant EU Model Clauses, always provided that transfer would be legal within Austria.
In the above mentioned cases, DPA notification and approval is required by law.

Transfers of Personal Data to countries outside the EU may further take place even without additional measures to ensure an adequate level of data protection at the recipient's end where:

- the data subject has consented to the transfer;

- the transfer is necessary for the performance of a contract between the data subject and the data Controller, or to take steps at the data Subject's request with a view to entering into a contract with him;

- the transfer is necessary for the performance of a contract between the data Controller and a third party in the interest of the data subject;

- the transfer is necessary to protect the vital interests of the data subject, or for reasons of public interest or in connection with legal proceedings, or for the purpose of establishing, exercising, or defending legal rights; or

- the personal data is available from a public register.

The general rules concerning the legality of processing must always be fulfilled (i.e., the transfer would need to be legal even within Austria).

Sanctions: A breach of privacy regulations could be subject to potential civil and criminal penalties, as well as private rights of action.

5.2.2 France

French law regulations which apply to the activity of network monitoring are the following:

- the law of August 6, 2004 (which has implemented the Directive 95/46/EC) which amended the former Data Processing, Data files and Individual Liberties Act of January 6, 1978 (hereinafter, the "Privacy Act");

- certain provisions of the law of June 21, 2004 on the confidence in the digital economy which implemented the Directive 2002/58/EC (hereinafter, the "E-commerce Law");

- articles 226-15 and 432-9 of the French penal code regarding secrecy of correspondence applicable to electronic mails (hereinafter, the "secrecy of correspondence");

- article 9 of the French civil code which establishes a right to privacy for every individual;

- the Godfrain law implemented into articles L. 323-1 and following of the penal code, concerning computer frauds, which is potentially applicable in case of illicit access to a system or network including for the purpose of monitoring.

Hereinafter is an overview of French law provisions that apply to the activity of network monitoring.

A) Preliminary conditions to the application of the French Privacy Act are

(i) the existence of a processing of personal data; and

(ii) a territorial link to France of the data processing.

(i) Processing of Personal Data:

Personal Data. The definition provided in the Privacy Act is similar to the definition set forth in the Directive 95/46/EC. Please note that the Privacy Act does not grant protection to legal entities but only to natural persons which are identified or identifiable (i.e. directly or indirectly) by an identification number or any other factor specific to the data subject. Therefore, IP addresses , logs, email addresses, names, etc. are considered personal data.

Data Processing. Alike the Directive 95/46/EC, data processing is widel y defined in the Privacy Act and covers any operation or set of operations performed, automatically or not, on personal data including collection, recording, organization, storage, adaptation, deletion, etc. Therefore, any activity performed on a network s uch as generating logs, recording of any data going through the network, etc. may be considered as data processing.

(ii) Territoriality. The Privacy Act applies to:

(a) data processing carried out by data Controllers established in France; or

(b) data processing performed by Controllers established outside the European Union through equipments located in France.

Data Controllers. The Privacy Act applies to data Controllers, i.e. any natural person, legal entity or any organization which determines the purposes and means of the data processing.

Therefore, any entity which performs network monitoring activities, and determines the purposes of the monitoring may be considered a data Controller. For example, an employer which sets up network monitoring of its IT resources, for purpose of controlling the use and security of the IT resources by its employees in the course of their employment may be considered as a Controller.

Data Processor. Alike the Controller, a data processor may either be a natural person or a legal entity.
A Controller which appoints a data processor remains responsible for the processing and the security of the personal data at stake. As a result, the Privacy Act provides that the Controller must enter into a contract with the processor setting forth the following:

(i) that the processor shall process the personal data on behalf and under the sole instructions of the Controller; and

(ii) the specific security measures which have to be implemented by the processor. For example, the subcontra ctor in charge of performing the network monitoring on behalf of the employer-Controller, remains a data processor if he acts under the sole instructions of the Controller.

The categories of the different processor must be stated in the notification to be filed with the French Data Protection Authority (hereinafter, the "CNIL").

B) Legal Requirements: In order to implement a network monitoring, the data Controller must comply with the following requirements:

a. *Prior information of the data subjects :*

Data must be collected and processed lawfully. For that purpose, before or at the time of collection of the data, the data subject must be clearly informed , through an appropriate notice of information such as a Privacy Policy, in French language, of the following:

- the **identity** of the Controller and of his representative, if any (e.g. the employer);
- the **purposes** of the processing for which the data are intended (e.g. ensuring the security of the employer's IT resources, compliance with legal obligations, prevent theft or unauthorized disclosure of employer's property or data, detect violations of employer's internal policies, prevent intrusions or malicious / unauthorized access and virus infestations, etc.) ;
- the **recipients** or categories of recipients of the data (e.g. internal services of the employer, such as HR department, legal department, supervisors of the data subjects; or sub-contractors, and other data processors for the purpose of performing the monitoring, etc.) ;
- their **right of access** to, and rectification of the data concerning them, and the practical manner to exercise such rights (including the designation of the person or service in charge of the right of access and rectification);
- the **transfer** of data to a non EU country, if any.

In addition, the data subject must be informed of his/her right to object, for legitimate reasons, to data processing.

2) Data must be relevant to the purpose stated in the notification (i.e.: all information strictly needed for the purpose of monitoring of the network).

With regard to email monitoring, the Privacy Act and together with the secrecy of correspondence rules apply, and the CNIL sets forth three principles of legitimacy, proportionality and transparency which a Controller must comply with.
Therefore, a Controller must implement email monitoring for a legitimate purpose such as security, prevention or network traffic supervision, which must be implemented in a proportional manner (i.e. not perform systematic email filtering).

In application of the transparency principle, the Controller must inform the data subjects of the monitoring and notify the processing with the CNIL .

Implementation of a data processing for the purpose of network monitoring must be proportionate.

In 2005, the CNIL delivered decisions forbidding the implementation of data processing systems enabling the automatic detection of intellectual property infringements on Peer 2 Peer (P2P) networks.
The CNIL decided that the monitoring programs were disproportionate with the purposes considered because monitoring activities were automatic and continuous, and not limited to fighting exclusively against infringements. Such processing might have lead to a massive collection of personal data on P2P networks, not necessarily in

correlation with acts of infringement. Collecting societies were therefore in position to take action against P2P users on the basis of personal data files which they could modify unilaterally at their own will to the detriment of P2P users '.

Sensitive Data prohibited: As a principle, it is prohibited to collect and process sensitive data, except with the prior and written consent of the data subject.

However, the CNIL deems that an employee's consent given within the employment environment is not valid due to the sub ordination relationship of employment.

3) *Limited storage term*: The storage term for personal data must be limited to the time necessary for the data processing.
Therefore, once the data processing is over, the Controller must delete all personal data from his records. However, the Controller may be entitled to store the data for an additional time period when provided by applicable laws e.g. for litigations purposes, etc.

The CNIL recommends specific storage term depending on the kind of personal data at stake e.g. data regarding the monitoring of employees' Internet activities should be kept for a maximum of six (6) months. Log files containing connexion data to a network, collected and processed for security measures and usage of IT resources should be kept for a maximum of six (6) months.

4) Security measures must be implemented: The Controller must guarantee the data subjects, on its behalf and on behalf of the processor if any, that all the appropriate technical and organizational measures are taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

The Controller remains liable to the data subjects in the event of a failure of the security measures taken. Neither French Privacy Act nor the CNIL provide specific information on the minimum technical requirements to be implemented.

Security measures should be specifically adapted to the kind of personal data processed and the risks identified.

Personnel in charge of the implementation of security measures should be specifically trained and informed of such measures. Indeed, under French law, such personnel must be bound by professional secrecy or held to an obligation of professional confidentiality with regard to personal data they may encounter in the performance of their mission (e.g. remote control assistance).
Therefore, they must not disclose information protected by the secrecy of correspondence, or which is protected by the Privacy Act, and which does not alter or affect the technical performance of applications, their security or the interest of the company.

5) Notification. The collection and processing of personal data performed for network monitoring must be notified by the Controller to the CNIL.

6) Specific labour law requirements apply to the collection and processing of personal data related to employees.

If a company implements new technological means in order to monitor or control its employees activities (e.g. monitoring of Internet activities, etc.) French labour law requires that the Work's Council ("Comité d'entreprise"), if any, be informed and consulted prior to the implementation of said means.
However, the Work's Council opinion is non-binding.

7) Transfer of data
A data transfer to a country which does not provide for a sufficient level of protection (including to US entities which have not adhered to Safe Harbor principles) must be justified by the purpose of the monitoring, such as centralization or reporting to a non-European entity of technical and organizational functions, for consistency and efficiency purposes.

Therefore, data transfers must in principle be secured by the execution of a data transfer agreement (hereinafter, the "DTA") between the EU entity which transfers the data (hereinafter, the "data exporter") and the non EU entity which imports the data (hereinafter, the "data importer").

Such DTA should be based on the model clauses adopted by the European Commission.

In some exceptional cases, the CNIL accepts that data subject's consent is sufficient to secure the transfer outside the EU.

C) Other remarks:

Activities which do not fall within the scope of the Privacy Act. The Privacy Act provides that the following does not fall within the scope of the Privacy Act:

(i) temporary copies made in the context of technical operations of transmission and access provision to a digital network for the purpose of automatic, intermediate and transitory storage of data and with the sole aim of allowing other recipients of the service to benefit from the best access possible to the transmitted information, provided that the data is not stored in a separate file which serves another purpose than temporary copy; and

(ii) operations of transit. The Privacy Act does not provide a definition of "transit". However, because the CNIL has a very narrow view of the term "transit" (i.e. no access to personal data by a natural person) most operations of transit will fall within the scope of the Privacy Act.

CNIL's report on network monitoring: The CNIL has issued a report concerning the monitoring of employees' activity[78].

CNIL's powers: The law dated 6 August 2004 has significantly increased the powers of the CNIL which include, without limitation, investigation powers; the issue of warning notice; the power to put fines of up to € 150,000 which may increase to € 300,000 or 5% of turnover in case of repeated infringements; the withdrawal of authorizations, etc.

[78] The report is available in French language at the following web address: http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf.

Sanctions for beach of secrecy of correspondence: penalties of up to one (1) year imprisonment and a fine of up to €45.000.

Sanctions for any breach of the Privacy Act: penalties of up to five (5) years' imprisonment and fines of up to €1.500.000 for a company. This sanction applies per infringement.

Sanctions for breach of the Godefrain law concerning computer frauds: illicit access to a system or network is punished by up to two (2) years imprisonment and a fine of up to €30000. Such penalties are raised to three (3) years imprisonment and a fine of up to € 45000 if the illicit access resulted in the deletion and or modification of data contained on the network or system.

5.2.3 Germany

The most important (i.e. the following is not an exhaustive list, it takes into accounts of the main requirements) provisions applicable to network monitoring are the following:

- **Art. 1 (1) of the German Constitution** might apply leading to the prohibition of total surveillance as violation of human dignity.

- **The Works Council Constituation Act** will most likely apply leading to information and co-determination rights for the works councils.

- **Section 4 (1) Federal Data Protection Act** ("FDPA") states as follows: "*The collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented*.".
  This provision will most likely apply since the monitoring of network traffic almost always coincides with the collection of personal data about the individual behind the corresponding static IP address inside the company.
  The same would apply for the monitoring of public networks in case the IP address is regarded as a personal information – which is a question, that is currently discussed - which appears to be correct since the so-called dynamic IP address is technically linked with an individual within the access providers' or telecom providers' systems despite the factual and legal difficulties to obtain such information from the access and telecom providers.

- **Section 4 (3) FDPA** setting forth information obligations regarding the Controller's identity, the data collected, the purposes for which such data are collected and the categories of recipients (if this is not already obvious or known to the data subject).

- **Section3a FDPA** on data reduction and data economy requiring data processing systems to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. According to Sec. 3a FDPA, in particular, use is to be made of the possibilities for aliasing and rendering persons anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection.

- **Section 33 FDPA** on notification obligations of recipients of personal data. According to Sec. 33 (1) 1st sentence FDPA if personal data are stored for the first time for one's own purposes without the data subject's knowledge, the data subject shall be notified of such storage, the type of data, the purposes of collection, processing or use and the identity of the Controller.

- **Section 4d (5) FDPA** on prior checking

- **Section 4d (4) FDPA** might apply leading to a registration obligation with the competent data protection authority if the traffic monitoring leads to an automated processing in which the controller concerned stores personal data in the course of business for the purpose of transfer or for the purpose of anonymised transfer.

- **Section 9 FDPA** on technical and organizational measures does apply.

- **Section 28 ff. FDPA** on the legality of the collection, processing and use of the data collected applies, if there is no consent of the data subject.

- **Section 4a FDPA** and if and to the extent sensitive data are concerned especially **Section. 4a (3) FDPA** (requiring that consent include explicitly the sensitive data) on the requirements for valid consent (e.g. consent must be given with free will and - as a rule - in writing) need to be respected.

- **Section 4d (4) FDPA** might apply leading to a registration obligation with the competent data protection authority if the traffic monitoring leads to an automated processing in which the controller concerned stores personal data in the course of business for the purpose of transfer or for the purpose of anonymised transfer.

- **Section 34, 35 FDPA** on information, correction, erasure and blocking does apply.

- **The provisions of the TeleMediaAct** might apply depending on what data are collected and if telemedia services are concerned.

- **Section 88 Telecommunication Act** protection telecommunication secrecy might apply due to e-mail and VoIP activities handled over the network

- It is currently unclear what final content the provisions on data retention will have and whether their applicability can be excluded in light of a recen t decision by the Federal Constitutional Court declaring parts of the provisions on data retention obligations as being anti-constitutional.

- Criminal law provisions (e.g. Sec. 206 German Criminal Code on the protection of telecommunication secrecy) and - at least as source of information - provisions of the Act on Criminal Procedure might also need to be taken into account.

5.2.4 Greece

Personal data protection constitutes a subject of the Greek Constitution. The Article 9A states that "everybody has the rig ht of being protected from the collection, processing and use of his/her personal data, especially with the use of electronic

means", while it explicitly provides for the protection of personal data the existence of an independent public authority. Additionally, the Article 19 defines as inviolable the confidentiality of telecommunications, leaving however open the possibility of intercepting communications for the purposes of national security or the investigation of serious crimes.

Regarding the adaptation of the European law and regulatory framework in the national jurisdiction, Greece has implemented the Directive 95/46/EC with the Law 2472/1997, put into force in April 1997 "for the protection of natural persons regarding personal data processing". The EU Directive 97/66/EC had been implemented with the Law 2474/1999 which has been substituted in July 2006 by the Law 3471/2006 that implements the Directive 2002/58/EC. The Law 3471/2006 amends the former 2472/1997 and determines the competences of the two afore-mentioned Authorities, that is, the Data Protection Authority (hereinafter, the "DPA")[79] and the Hellenic Authority for the Information and Communication Security and Privacy (hereinafter, the "ADAE")[80]. In the following, the Greek framework is briefly described.

Data Processor. The law provides that for each specific data basis there is a specific Controller who is ultimately responsible for any aspect of the data processing. Processing is defined in virtually the same wording that is used in the Directive 95/46/EC. The same applies to the definition of Controller and the definition of Processor. Finally the same applies for a "third" person that may be processing data. In all cases the Controller is responsible towards the person that data of whom are processed along with the data processor or the third person and in whole with that person. In case that the data processor or "third" person has acted without the knowledge of the Controller, the Controller can demand then compensation from them. Their relationship may further be governed from their contractual relationship. A "third" person can process personal data only following a written authorization to that effect from the Controller.

Consent. In line with the Directive 95/46/EC, the Greek law provides that the consent of the data subject is a necessary prerequisite for a legitimate data processing. The Greek law uses the same wording of the Directive 95/46/EC. In addition, however, to that it specifically states that the person must have full knowledge of all the details related to the data basis and the data processing. This does not constitute an additional factor to those described in the Directive 95/46/EC as said Directive covers it. The wording of the law simply stresses this. However, this seems to have led the courts to accept that simply signing General Terms and Conditions that are not negotiated does not constitute consent in the context of the Greek data protection law. The Appeal Court in the same decision did not accept a reference in the General Terms and Conditions stating that the person should read the document well and diligently before signing it as this would not suffice. A general consent will also not suffice but a specific consent for specific use and processing is needed. The DPA has further ruled that the fact that the person has not responded to a call for consent cannot be taken to be consent in the context of the law. It is further prohibited to set the consent as a prerequisite for providing services or goods or to treat the purchase of the services or goods as an implied consent. It should be additionally noted that the Greek DPA maintains a list of data subjects, the so-called "Article 13 list" referring to the Article 13 of the Law 2472/1997, entitled "Objection Right". All natural persons have the

[79] http://www.dpa.gr/.
[80] http://www.adae.gr/.

right to be included in this list through a very simple procedure. The data subjects that are members of the list are excluded from any products' promotion campaign and other similar services. The data controllers and process ors are obliged to refer to this list and delete its members from their corresponding catalogues of recipients.

Consent: Exemptions from the rule. The Greek law uses the same wording of the Directive 95/46/EC in regard with the exceptions in which no cons ent is needed for the processing of the data. Article 5 of the Law 2472/1997 however, by which Article 7 of the Directive is implemented, further provides that the DPA can issue regulations that cover cases in which the rights of the persons are obviously not infringed. Such regulations must be ratified by Presidential Decrees and acquire in that manner more authority.

Employment agreements constitute one of the kind of agreements for which the law provides that no consent is needed and no prior notific ation to the DPA is needed. The DPA has issued a Directive in respect with employees' data [81]. The DPA made it clear that the Directive does not constitute a legally binding document and simply gives directions as to how the DPA should be expected to react in cases that may be brought before it.

Any data in addition to the data that can be used for such purpose as mentioned above, or the processing of data that are collected for the purpose of the performance of the employment agreement, for purposes other than the performance of the employment agreement, is prohibited. The DPA in the above Directive adopts the very strict view that despite the principle of freedom of contract, the employee is not really in a position to react due to the obvious inequality of his negotiating position against the employer. Video surveillance in the work can only be used if this is absolutely necessary for the protection of the health and security of the employees. The employees must be previously informed of the video surveil lance. The assessment of the performance of the employee cannot be based solely on data collected in this manner. Finally the employer cannot process data concerning the use of the Internet or the telephone from the employee unless again this is absolutely necessary in accordance with the principle of proportionality from the kind of work performed and on a case by case basis.

Notification. The Controller must notify the existence and processing of any data basis to the DPA. The Controller must notify his name, title and address. In case that the Controller is not a resident of Greece or of a place where Greek law will be applicable, he must also give the above information in regard with his representative in Greece. The place where the data basis is establ ished, the purpose of the processing, the kind of the data that are processed, the entities that will have access to the data, the possible transfer of the data to another country, the basic technical characteristics of the data basis system and the securi ty measures that are taken for the data basis. Any change to the above must also be notified.

Sensitive data. The Greek legislation follows the wording of the Directive 95/46/EC in regard with the definition of sensitive data and lists the same exclusive list of sensitive data that may be processed. The processing of such data presupposes not only notification to the DPA, but also an authorization by it to that extent. Otherwise the processing of such data is considered illegal. The DPA must be satisfied that the

[81] Directive 115/2001.

processing will be made strictly for reasons that fall within the exclusive list of the Act and that the data used are the absolutely necessary for that purpose. The DPA may grant authorization under additional conditions and terms. The data of all the recipients of the sensitive data must be notified to the DPA, the moment that they acquire knowledge of the sensitive data. The DPA has been very strict and diligent in applying these provisions. The data subject must consent freely and in writing to the processing of his data. The Controller must in all cases decide whether in accordance with the principle of proportionality the data used that may be requested from a third person are those absolutely necessary for the reason that allows such processing in accordance with the Law 2472/1997. The DPA has rejected the circulation of sensitive data to a third person that was proposing to use them at the court, without having already taken action for that purpose. Data collected for research purposes from the National Research Center or the Academy of Sciences and Arts in Athens, is only allowed if the identity of the persons is covered. Finally, law case reports must not refer to data that help uncover the identity of the persons participating in the case.

Exemptions form the rule of prior notification and authorization. Article 7^{A} of the Law 2472/1997 lists in an exclusive manner all the cases that are exempted. These include data concerning the performance of an employment agreement, as described above, data concerning suppliers or customers to the extent that they are not notified to third persons. This exemption does not apply to insurance companies, pharmaceutical companies, financial institutions and companies providing commercial information. Legal entities of a non-profit purpose are exempted to the extent that the data processing concerns their members, they have consented and no third party has access to such information. For medical information processed by medical staff, under the condition that the Controller is bound from an obligation of secrecy or an ethical code and no third person has access. This does not include the administration of a hospital and insurance companies. Under the same conditions data can be processed from lawyers, public notaries and bailiffs in regard with their clients. Finally the processing of data from Courts in the context of administering justice is exempted.

Information, Access and Refusal. The data subjects are given the above rights in order to be able to safeguard their privacy. The data subjects can request all necessary information in order to be able to have full knowledge of the function of a data basis and in addition knowledge of the third persons that have access to the data. The Controller must have written agreements with all persons that may be involved with the processing of the data, for example in the context of an outsourcing agreement. The Controller is obliged to provide access to any information required by the data subject in regard with the location, the kind and purpose of processing, the development of processing, and the persons that have access to the data, within 15 days as from such an application. In doing so the data subject may have the assistance of any person he feels appropriate.

Sanctions. The Greek Law provides for extensive both criminal and administrative sanctions. The penalties that can be imposed by the DPA may reach 150.000 Euro. Other sanctions include the non-permanent and the permanent withdrawal of the authorization by the PDA and the destruction of the data basis. The criminal penalties to the persons who commit a crime related to processing of data may reach 10 years of imprisonment. In case of a legal entity such criminal penalties are imposed on the legal representatives of the legal entities. Similar provisions apply in case the crime is committed from a public entity. The sanctions can be stricter if applied by the ADAE.

For example, Vodafone Greece was fined 76 million Euros for the afore-mentioned illegal wiretapping[82].

Data and communications security. Greece has been the first European country to enact specific regulations regarding the enforcement of acceptable security policies by the telecommunications providers of mobile, fixed and wireless networks, providing telecommunication services, as well as the Internet Service Providers (fixed, wireless and mobile ISPs), Internet Application Service Providers and Internet Providers of Value-added Services. According to the regulations[83], all the afore-mentioned providers must have implemented a security policy and the consequent operational procedures and put in place the corresponding technical means in order to provide for the data and communications confidentiality and security. It should be noted here that these security policies must be submitted to the ADAE and be approved. The ADAE regulations set high standards at a national level and are equivalent to well-respected international standards, such as the ISO/IEC 17799[84].

Lawful Interception of communications. The procedures, as well as the technical and administrative/operational guarantees for the performance of Lawful Interception are defined by the Presidential Decree 47/2005, enacted in March 2005. The Presidential Decree 47/2005 defines in detail the types of communications and the types of data that are subject to Lawful Interception. It sets obligations to the providers to have the appropriate equipment for performing the interception, which must only be activated after a related request by the National Authorities. In any case, the ADAE must be informed and provide consent for the performance of the Lawful Interception.

5.2.5 Italy

Hereinafter it follows a brief highlight of the main principles that might be applicable to the activity of network monitoring under Legislative Decree June 30, 2003 n. 196 and following amendments and integrations (hereinafter, the " Privacy Code").

Legal entities as data subjects. The Privacy Code considers as data subjects not only natural persons, but also legal entities, which are granted almost the same degree of protection than natural persons.

It should be noted that except for specific and limited law provisions, for example the fact that data relating to legal entities may be transferred out of the safe boundaries of the European Union without any formality to be accomplished, the mechanism and rules provided under the Privacy Code are more or less the same for both natural persons and legal entities.

Data Processor. The role and regulation relating to the data processor are peculiar under the Privacy Code if compared with the generality of the other European Union member states.

The Privacy Code provides that the Controller may appoint as data processor both a natural person and a legal entity that basically processes personal data on behalf and under the instructions of the Controller.

[82] cf. for example: V. Prevelakis, D. Spinellis, "The Athens Affair", *IEEE Spectrum*, Volume 44, Issue 7, pp. 26 – 33, July 2007.
[83] Secrecy Assurance Regulations for Telecommunication Services (FEK 87/2008); Secrecy Assurance Regulations for Internet Telecommunications (FEK 88/2008)
[84] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Code of practice for information security management", International Standard ISO/IEC 17799, Dec. 2000.

The Controller does not have a specific obligation of appointing a data processor, but the appointment is almost due when the Controller delegates to third parties the whole or part of the processing activities that it performs.

The appointment must be made by written instrument, notably a formal appointment deed that is executed by the Controller and also the processor for express acceptance. The content of the appointment deed is not ruled, so it varies depending upon the degree of authorities and correspondent liabilities that the Controller wishes to delegate to the processor.

The Controller may appoint as its processor either a subject internal or external to its organization, hence in Italy there is the possibility to have internal processors (usually natural persons) that are appointed in the majority of cases within the personnel of the Controller's organization and who are in charge of all or some aspects of the processing that is under the authority of the Controller, and external processors, that are appointed when the Controller assigns all or some of its processing activities to a third party, or when the Controller reverts to a third party service provider for the performance of services that imply processing of data that are under the authority of the Controller.

The Controller has a specific and stringent duty to select as data processor a subject that provides appropriate guarantees of compliance with the Privacy Code, and has also a duty to constantly monitor the data processor and to verify that it complies with the instructions received by the Controller and with the Privacy Code.

Minimum data security measures. Annex B to the Privacy Code (Technical specifications on minimum data security measures) contains a detailed list of the minimum data security measures that any Controller has to implement for a lawful data processing.

The security measures are split in two main categories under the Privacy Code: minimum and adequate data security measures.

The minimum data security measures are a minimum security standard considered as precondition for any kind of lawful data processing. Failure to implement minimum data security measures may result in criminal sanctions.

The Privacy Code in contrast does not specifically define the adequate data security measures to be implemented by the Controller, and same as the Data Protection Directive, the Privacy Code limits saying that the Controller should determine itself what are the security measures that are adequate with regards to the specific data processing activities to be protected with regard to the aim of reducing to the minimum any possible risk that may jeopardize the personal data or that may harm the data subject, and the Controller should then implement said security measures.

The Privacy Code only provides for the general criteria that the Controller has to follow for determining what the adequate security measures are for the specific relevant case. The rule is that personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimize, by means of suitable preventative security measures, the risk of their destruction or loss, whether by

accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Tighter security measures are provided under articles 123 and 126 of the Privacy Code for the processing of traffic data (article 123) and of location data (article 126), with provisions that impose limitation to the possibility of access to the data, the necessity to have in place appropriate safeguards to the identification and monitoring of the data access, the compliance with the necessity, proportionality and data storage principles.

Security Policy Document. A peculiar minimum data security measure provided for by Annex B to the Privacy Code in case of processing of sensitive data through electronic means is the drafting of a document named security policy document.

The content of this document is detailed in Annex B to the Privacy Code .
In brief, it represents a picture of the features and modalities of the processing carried out by the Controller, with specific focus on the security issue s[85].

The document must be updated at least within the 31st of March of each year; notice of the fact that the security policy document has been drafted/renewed has to be reported in the management report of the balance sheet of the company , if applicable.

Codes of conduct. The codes of conduct are regulations that are issued with regard to specific areas that need detailed rules in addition to the general ones set forth under the Privacy Code.

The codes of conduct are published in the Italian Official Gazette and they are an integral part to the Privacy Code, to which they are attached under Annex A with progressive numbering (e.g. Annex I, Annex II, etc.).

So far, the following codes of conduct have been adopted:

- code of conduct applying to the processing of personal data in press activities [86];
- code of conduct and professional practice applying to the processing of personal data for historical purposes[87];
- code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes carried out within the national statistical system[88];

[85] Under point 19 of Annex B to the Privacy Code, the security policy document must contain appropriate information with regard to: the list of data processing operations carried out; the distribution of tasks and responsibilities among the departments/divisions in charge of processing data; an analysis of the risks applying to the data; the measures to be taken in order to ensure data integrity and availability as well as protection of areas and premises; a description of the criteria and mechanisms to restore data availab ility following destruction and/or damage; a schedule of training activities of the persons in charge of the processing; a description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operat ions concerning personal data are externalized in accordance with the Privacy Code; as for the personal data disclosing health and sex life under certain circumstances, the specification of the criteria to be impl emented in order to either encrypt such data or keep them separate from other personal data concerning the same data subject.
[86] Decision of the Italian Data Protection Authority of July 29, 1998 - Official Gazette of August 3, 1998 n. 179.
[87] Decision of the Italian Data Protection Authority of Mar ch 14, 2001; n. 8/P/2001 - Official Gazette of April 5, 2001 n. 80.

- code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments[89].

Territoriality. With regard to the extent of application of the Privacy Code, the same applies to the processing of personal data, including data that are held abroad, under the following circumstances:

- when the processing is performed by entities established in Italy; and

- when the processing is performed by entities established in the territory of a country outside the European Union, provided that said entities make use in connection with the relevant data processing of equipment – whether electronic or otherwise – located within the Italian territory; unless such equipment is used only for purposes of transit through the territory of the European Union.

Notification. As above recalled, the Privacy Code has significantly simplified the notification requirement, if compared with the previous Law 675/96.

The notification requirement is indeed limited to some data processing activities that are deemed to present specific risks and of which the Garante wants to be informed[90]. The notification is filed only once, in telematic form (through the web site of the Garante[91]). The register of notifications is publicly available and may be interrogated free of charge via electronic networks on the web site of the Garante.

With regard to the activity of network monitoring, this activity as such may be subject to the notification obligation if it is ascertained as involving the processing of other data that allow the disclosing of the geographic location of individuals or objects by means of an electronic communications network (article 37, letter a) of the Privacy Code).

---

[88] Decision of the Italian Data Protection Authority of July 31, 2002; n. 13 - Official Gazette of October 1, 2002 n. 230.

[89] Decision of the Italian Data Protection Authority of November 16, 2004; n. 8 - Official Gazette of December 23, 2004 n. 300.

[90] The data processing subject to the obligation of notification are the following: a) genetic data, biometric data, or other data disclosing geographic location of individuals or objects by means of an electronic communications network; b) data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure; c) data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade-union character; d) data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users; e) sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys; f) data stored in ad-hoc data banks managed by electronic means in connection with creditworthiness, as sets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.
The Italian Data Protection Authority may specify additional processing operations that are liable to affect the data subjects' rights and freedoms on account of the relevant mechanisms and/or the nature of the personal data at stake. By means of a similar decision to be published in the Official Journal of the Italian Republic, the Italian Data Protection Authority may also specify the processing operations among those above referenced that are not liable to be prejudicial and are therefore exempted from notification.

[91] The notification may be filed with the Italian Data Protection Authority at the following web address: https://web.garanteprivacy.it/rgt/NotificaTelematica.php?h_mnu=NotificaTelematica.

It is understood that if the Controller intends to use the data gathered for network monitoring reasons for other processing purposes falling within the list of data processing that are subject to the notification obligation under article 37 of the Privacy Code, the notification would be necessary.

Information statement. The information statement represents the principal instrument through which the Controller informs the data subject on the data processing that the Controller intends to perform on the data subject's data. The information statement may be given to the data subject orally or in writing; the usual practice is to provide the data subject with a written information statement for evidence purposes, save for specific cases in which it proves problematic to revert to the written form.

Article 13 of the Privacy Code sets forth the amount of mandatory information that the Controller must provide to the data subject, which is larger than what provided under the Data Protection Directive. This mandatory information may be summarized as follows:

(i) the purposes and modalities of the processing for which the data are intended;

(ii) the mandatory or voluntary nature of providing the requested data;

(iii) the consequences if the data subject does not provide the data;

(iv) the extent of data communication and access, notably the entities or categories of entity to which the data may be communicated, or who may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data;

(v) the rights of the data subject as per article 7 of the Privacy Code [92];

(vi) the identification data of the Controller and, where designated, the data processor. If the Controller has appointed several data processors, at least one among them should be referred to and either the site on the communications network or the mechanisms for easily accessing the updated list of data processors shall be specified. If the Controller has designated a data processor with the specific duty to handle the data subject's requests in case of enforcement by the data subject of the rights acknowledged under article 7 of the Privacy Code, this data processor should be mentioned in the information statement.

[92] Article 7 of the Privacy Code provides that a data subject shall have the right to obtain confirmation as to whether or not personal data concerning the data subject exist, regardless of their being already recorded, and communication of such data in intelligible form. A data subject shall further have the right to be informed a) of the source of the personal data; b) of the purposes and methods of the processing; c) of the logic applied to the processing, if the latter is carried out with the help of electronic means; d) of the identification data concerning data controller, data processors and the representative designated; e) of the entities or categories of entity to which the data may be communicated and which may get to know said data in their capacity as designated representative(s) in the State's territory, data processor(s) or person(s) in charge of the processing. Moreover, a data subject shall have the right to obtain a) updating, rectification or integration of the data; b) erasure, anonymization or blocking of data that have been processed unlawfully; c) certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected. Furthermore, a data subject shall have the right to object, in whole or in part, a) on legitimate grounds, to the processing of personal data concerning the data subject, even though they are relevant to the purpose of the collection; b) to the processing of personal data concerning the data subject, where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communication surveys.

Moreover, articles 123 and 126 of the Privacy Code set forth that for the processing of traffic data (article 123) and of location data (article 126) some further information is to be added, notably specific details on the nature of traffic and location data that are processed, the specific purpose of the processing, the duration of the data processing, and clear indications as to the possible communication of said data to third parties.

Whenever personal data are not collected directly from the data subject, yet for example from third parties, the above reported information should be provided to the data subject at the time of recording such data or, if their communication is envisaged, no later than when the data are first communicated.

The Privacy Code provides for a limited set of circumstances under which the Controller is exempted from the obligation of giving the information statement to the data subject if data are not collected directly by the data subjects. Said exemptions have regard to the following cases:

(i) if the data are processed in compliance with an obligation imposed by a law, regulations or Community legislation;

(ii) if the data are processed either for carrying out the investigations by the defense counsel or to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary there for; and

(iii) if the provision of information to the data subject involves an effort that is declared by the Garante to be manifestly disproportionate compared with the right to be protected, in which case the Garante shall lay down suitable measures, if any, or if it proves impossible in the opinion of the Garante.

Consent. The Privacy Code states that for the processing of personal data it is necessary to obtain the data subject's consent except for specific circumstances specifically listed under Section 24 of the Privacy Code [93].

Moreover, the Privacy Code specifies the features that the data subject's consent should have in order to be valid.

The consent of the data subject to the processing must be as follows:

- express: no implied consent is envisaged under the Privacy Code;

[93] The consent is not required if the relevant data processing a) is necessary to comply with an obligation imposed by a law, regulations or Community legislation; b) is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract; c) concerns data taken from public registers, lists, documents or records that are publicly available; d) concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy; e) is necessary to safeguard life or bodily integrity of a third party; f) is necessary for carrying out the investigations by the defense counsel, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary there for by complying with the legislation in force concerning business and industrial secrecy, dissemination of the data being ruled out; g) is necessary to pursue a legitimate interest of either the data Controller or a third party recipient in the cases specified by the Garante; h) except for external communication and dissemination, is carried out by no-profit associations, bodies or organizations according to specific provisions; i) is necessary exclusively for scientific and statistical purposes in compliance with the respective codes of professional practice, or else exclusively for historical purposes pursuant to applicable regulation.

- free: the result of the free will of the data subject;

- specific: a specific consent is necessary for each data processing purpose sought by the Controller;

- informed: the consent must follow an information statement drafted pursuant to the Privacy Code;

- given in advance: the consent must be obtained by the Controller before the latest starts processing personal data; and

- documented in writing in case of processing of personal data: the consent for personal data may be given also orally, but the relevant providing must be reported on a paper medium, while the consent for sensitive data must be given through written instrument.

With regard to the activity of network monitoring, the necessity to obtain the data subject's consent depends upon the specific purpose for which the network monitoring activity is performed. So for example if the processing purpose is to guarantee efficiency and proper functioning if the network of the Controller or proper performance of the services offered by the Controller, the consent would not be necessary.

However, articles 123 and 126 of the Privacy Code set forth that for the processing of traffic data (article 123) and of location data (article 126) the consent is usually always required, also for performance of value added services. The specific circumstances have to be ascertained on a case by case basis.

Sensitive data. For the processing of sensitive data it is necessary an authorization issued by the Garante and, save for limited and specified exemptions, the written consent of the data subject.

The written consent of the data subject is not required when it is concerned with the following processing activities:

a) processing of the data concerning members of religious denominations provided some specific conditions are met;

b) processing of the data concerning affiliation of trade unions and/or trade associations or organizations to other trade unions and/or trade associations, organizations or confederations;

c) data processing carried out for specific, lawful purposes as set out in the relevant articles of association or collective agreements by not-for-profit associations, organizations of political, philosophical, religious or trade-unionist nature, for personal data concerning relevant members, provided that data are not communicated or disclosed;

d) data processing that is necessary to protect a third party's life or bodily integrity;

e) necessary for carrying out the investigations by defense counsel, or else to establish or defend a legal claim;

f) is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context.

The written consent of the data subject would be mandatory for the processing of network monitoring activity whether sensitive data are collected and processed.

Principles of lawfulness of the processing and of data quality. Article 11 of the Privacy Code states the data quality principles and the principles for a lawful processing. Any kind of data processing activity, and thus also network monitoring, should comply with the requirements hereinafter set forth.

Personal data undergoing processing shall be:

a) processed lawfully and fairly;

b) collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes;

c) accurate and, when necessary, kept up to date;

d) relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;

e) kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

Any personal data that is processed in breach of the relevant provisions concerning the aforementioned principles may not be used.

Moreover, under article 3 of the Privacy Code the information systems and software in place at the Controller should be configured by minimizing the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively.

Transfer of data. Transfer of data within the EU is allowed due to the circumstance that all EU member states are bound by the Directive 95/46/EC on the professing of personal data, which basically sets forth a common benchmark of principles that are applied in all member states and that guarantee an adequate level of data protection. It follows that transfer of data within the EU is regarded as a mere data communication and the general requirements set forth for the data processing within the member states apply.

In contrast, transfer of data towards third countries that do not allow an adequate level of data protection is in principle prohibited. The data transfer is allowed only provided that the specific requirements set forth by the Privacy Code are complied with. The transfer of data is allowed on the basis of one of the following conditions [94]:

[94] Section 43 of the Privacy Code.

(i) if the data subject has consented to said transfer either expressly or, where the transfer concerns sensitive data, in writing;

(ii) if the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject;

(iii) if the transfer is necessary for safeguarding a substantial public interest or a third party's life or bodily integrity;

(iv) if the transfer is necessary for carrying out the investigations by the defence counsel, or else to establish or defend a legal claim, provided that the data are transferred exclusively for said purposes and for no longer than is necessary therefore in compliance with the legislation in force applying to business and industrial secrecy;

(v) if the transfer is carried out in response to a request for access to information contained in a publicly available register, list, record or document, in compliance with relevant applicable provisions;

(vi) if the transfer is necessary exclusively for scientific or statistical purposes, or else exclusively for historical purposes min compliance with relevant codes of conduct;

(vii) if the processing concerns data relating to legal entities, bodies or associations.

Moreover, the transfer of data out of the EU may be authorized by the Garante on the basis of adequate safeguards for data subjects' rights [95]. The Garante may give its authorization in connection with guarantees and also contractual safeguards that the data exporter and importer undertake to abide by, and also following a decision of the European Commission that finds that a non-EU member state affords an adequate level of protection, or else that certain contractual clauses afford sufficient safeguards.

It should be noted that at a European and also Italian level the view taken by the Data Protection Authorities is that when the data transfer happens on a constant basis and has regard to a large amount of personal data, the Controller should not opt for the consent solution, but for other options that allow the transfer without reverting to the data subject's consent, in light of the circumstance that the consent may be either denied or further revoked at any time by the data subject.

In case of network monitoring activities that involve the transfer of personal data out of the European Union, the Controller should carefully verify the situation and take the appropriate solution.

Sanctions. The Privacy Code sets forth a severe system of penalties. Indeed, on the one hand breach of some provisions of the Privacy Code [96] entail criminal sanctions; on the other hand, also administrative [97] and civil sanctions have been provided for.

[95] Section 44 of the Privacy Code.

[96] Criminal sanctions are provided, for example, in case of unlawful data processing; failure to implement minimum data security measures; false statement to the Italian Data Protection Authority or false notification.

Among the civil liabilities that may result from an illegitimate data processing, it should be noted that the infringer has to compensate not only monetary, but also moral damages.

Moreover, the legislative mechanism provides for an inversion of the burden of proof. The general rule on extra-contractual liability is that the allegedly damaged party has to prove the causal relationship between the acts of the alleged damaging party and the damages suffered. In contrast, for damages caused by unlawful data processing, the damaged party must only indicate the damages suffered and the action of the alleged damaging party, while it is the alleged damaging party that must prove to have done every thing that would have been necessary to avoid the occurring of the damages. This probation is usually named *probatio diabolica* as it is difficult to prove to have taken all necessary steps to avoid damages, especially in light of the fact that damages did occur.

Data retention. As to the issue of data retention, Italy has enacted a data retention law before the Data Retention Directive entered into force, notably Law 155/2005[98] and following amendments and integrations[99].

Further to said legislative provisions, Italy has ratified and executed the Council of Europe Convention on cybercrime[100] with Law 48/2008[101].

Lastly, with Legislative Decree n. 109 of May 30, 2008 Italy Has formally ratified the Data retention Directive[102].

The result is a legislative framework fairly complex, to which they should be added the provisions issued by the Garante with regard to the storage and processing of traffic and telematic data for data retention purposes, that are hereinafter reported.

The legislative scenario in Italy before enactment of the Data Retention Directive could be summarized as follows.

(i) Retention for a period of 6 months of telephonic and telematic data for purposes of evidence in case of claims relating to invoicing or demand of payment, save further specific retention of data that is necessary in relation to claims, also judicial claims in order to provide evidence in

[97] Administrative sanctions are provided, for example, for inadequate or lack of the information statement to the data subject; failure to submit the notification or incomplete notification submitted; failure to provide information or produce documents to the Garante.

[98] Law n. 155 of July 31, 2005, published on the Official Gazette n. 177 of August 1, 2005, and available in the Italian language at the following web address: http://www.parlamento.it/leggi/05155l.htm.

[99] Legislative Decree n. 248 of December 31, 2007, article 34, published on the Official Gazette n. 302 of December 31, 2007, and available in the Italian language at the following web address: http://www.camera.it/parlam/leggi/decreti/07248d.htm.

[100] The Council of Europe Convention on cybercrime is available in the English version at the following web address: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=6/11/2008&CL=ENG.

[101] Law n. 48 of March 18, 2008, published on the Official Gazette n. 80 of April 4, 2008, Ordinary Supplement n. 79, and available in the Italian language at the following web address: http://www.parlamento.it/parlam/leggi/08048l.htm.

[102] Legislative Decree May 30, 2008, n. 109 – Implementation of the Directive 2006/24/EC relating to the storage of data generated or processed within the provision of electronic communications services available to the public or public communications networks and that amends Directive 2002/58/EC, published on the Official Gazette n. 141 of June 18, 2008, and available at the following web address: http://www.penale.it/page.asp?mode=1&IDPag=638.

case the bill is challenged or payment is to be pursued, subject to such additional retention as may be specifically necessary on account of a claim also lodged with judicial authorities (article 123, paragraph 2 of the Privacy Code);

(ii) Retention for a period of 24 months of telephonic data (including unanswered calls and hence even if data are not subject to invoicing) and of 6 months for telematic data for purposes of detecting and suppressing criminal offences (article 132, paragraph 1 of the Privacy Code);

(iii) Retention for a period of 48 months of telephonic data (including unanswered calls and hence even if data are not subject to invoicing) and of 12 months for telematic data for purposes of detecting and suppressing some specific crimes as well as any offences against information or telematics systems (article 132, paragraph 2 of the Privacy Code);

(iv) Retention until December 31, 2008 of telephonic and telematic data for purposes of combating international terrorism, save enforcement of criminal proceedings for crimes that are in any case to be prosecuted, and without prejudice to other applicable law provisions setting forth additional data storage periods (article 6, paragraph 1 of Law 155/2005 as amended by Legislative Decree 248/2007);

(v) Retention from 3 to 6 months of telematic data for purposes of carrying out of some specific preventive investigations, or for purposes of detecting and suppressing of specific crimes as set forth under the Council of Europe Convention on cybercrime (Law 48/2008).

In general terms, the data to be retained are phone numbers of incoming and outgoing calls (in some cases also unanswered calls), duration of phone calls, IP addresses in relation to log-in and log-off times and also details of e-mail activities. The content of the communications is excluded from data retention obligations.

There is no provision of reimbursement for the companies subject to the aforementioned data retention obligations.
The most relevant category of addresses of data retention obligations are providers of electronic communication services available to the public on public communications networks, and providers or operators of informatic or telematic services [103].

As above outlined, Legislative Decree 30/5/2008 has executed in Italy the Data Retention Directive, partially modifying the above depicted scenario.

The Garante has issued a favourable opinion on the scheme of the above referenced Legislative Decree, which has been submitted to the Garante before issuance for its opinion[104].

[103] Please note that at the time this document is being drafted there are discussions among the exact definition of the addressees of data retention obligations.
[104] Opinion of the Garante issued on March 5, 2008, published in Bulletin n. 93 of March 2008, available in the Italian version at the following web address: http://www.garanteprivacy.it/garante/doc.jsp?ID=1523089 .

The current legislative framework on data retention, after enforcement of Legislative Decree 30/5/2008, allows a maximum period of 24 months for retention of telephone data, 12 months for sms data (excluding relevant content), and only 30 days for unanswered calls.
The latest time storage limit (30 days instead of 12 months), has been evaluated as adequate for the purpose of possible judicial investigations.

The reason to keep inclusion of data relating to unanswered calls within the data retention obligations is that also if there is no real communication, the mere calling of a number may used for terrorism activities such as for example activating an explosive device at distance.

For telephone communications the data to be retained are time of the conversation, telephone numbers involved in the conversation, place of departure and arrival of the telephone call.

With regard to conversations over the network, the data to be retained are IP addresses, name of the subscriber to the service, e-mail address and place of departure of the request.

Legislative Decree 30/5/2008 has also introduced amendments with regard to the mechanism provided for sanctioning the breaches by the telecommunications operators of the data retention provisions.
The Garante is indeed provided with the authority of issuing administrative fines of an amount ranging from € 10.000 to € 150.000, the amount of the administrative fine to be increased up to the maximum in consideration of the increasing seriousness of the breach and the dimension of the infringing entity.

The Garante has recently issued (January 17, 2008) a General Regulation on Security In Telephone And Internet Traffic Data[105], in which the Garante has detailed the physical, organizational and technical data security measures that have to be implemented with regard to the processing and storage of personal data to which the data retention obligations apply.

The mandatory security measures identified by the Garante with the aforementioned General Regulation should be implemented within October 31, 2008, and may be summarized as follows.

(i) Access to data. Access to data is allowed only to persons specifically authorized to process data through advanced systems of information authentication, also making use of biometric data such as fingerprints. Save for limited cases of necessity, the foregoing provisions are to be applied also to system administrators;

(ii) Access to places. Places where are located the elaboration systems that process data relating to telephonic traffic for exclusive purposes of justice should be provided with biometric systems to control access to said places. In any case, the systems that process traffic data of any nature should be located in places of selected access;

[105] General Regulation of the Garante on Security In Telephone And Internet Traffic Data, issue on January 17, 2008, and available in English version at the following web address: http://www.garanteprivacy.it/garante/doc.jsp?ID=1502599.

(iii) Authorization systems. The functions between the persons who assign the authentication credentials and the persons who access the data should be kept strictly separated. The authorization profiles to be assigned to the persons that access and process data should be differentiated on the basis of the purposes for which traffic data are processed, notably ordinary management or detection and suppression of crimes;

(iv) Tracking of the activity of the authorized personnel. Every access that takes place and every operation that is performed by the persons who are specifically authorized to access and process data and also by the system administrators should be registered in a specifically dedicated audit log register;

(v) Separate storage. Data that are stored for exclusive purposes of detection and suppression of crimes should be stored separately from the data used for company business purposes such as for example invoicing, marketing, prevention of frauds, statistics. Moreover, the elaboration systems that process the data stored for exclusive purposes of detection and suppression of crimes should undergo tight physical security measures and access controls;

(vi) Deletion of data. Data should be promptly deleted or made anonymous upon expiry of the data retention period set forth by applicable laws and regulations, also deleting said data from backup copies created to save the data;

(vii) Internal controls. Periodic controls should be carried out on the legitimacy of the access to the data by the persons specifically authorized to access and process the data, on compliance with applicable laws and regulations, on fulfilment of the technical organizational and security measures set forth by the Garante, and on real deletion of data upon expiry of the data retention periods.

(viii) Coding systems. Traffic data processed for exclusive purposes of justice should be protected with cryptographic techniques against the risks of unauthorized acquisition, also accidental, of the information registered by the persons specifically authorized to access and process the data, such as system administrators, data base administrators, hardware and software maintenance persons.

5.2.6 Switzerland

(i) General Data Protection Principles

The DPA sets out a number of "principles" for processing personal data. The principles apply to any person processing personal data. The violation of such principles is considered a violation of the data protection law. The principles are the following:

- Personal data shall only be processed lawfully and accordin g to the principle of good faith.

- Personal data shall be collected in a manner that its collection and, in particular, the intended purpose of processing is recognizable by the data subject.

- Personal data shall only be processed for the purpose (i) i ndicated at the time of collection; (ii) that is evident from the circumstances at the time of collection; or (iii) as provided for by law.

- Personal data shall not be processed excessively. That is, it must only be processed to the extent needed for the purpose of processing and without unduly harming the data subject.

- Whoever processes personal data shall ensure that it is accurate (to the extent this is necessary in view of the purpose for which such data is processed).

- Personal data shall not be transferred abroad if the privacy of the data subjects may seriously be jeopardized;

- Particularly sensitive personal data or personality files must not be disclosed to a third party without any sufficient justification.

- Personal data shall not be processed against the explicit will of the data subject without a sufficient justification.

Any violation of the principles set out above can be justified by:

- obtaining the data subject's consent;

- relying on an overriding private interest;

- relying on an overriding public interest.

(ii) Registration Requirements

Owners of data collections that regularly process sensitive personal data or personality profiles, or regularly disclose personal data to third parties (including affiliated companies) must register their data collections with the Swiss Data Protection Commissioner.

Non-compliance with this requirement may be subject to fines. There are several exemptions to the aforementioned rule. For example, registration is not required where:

- the personal data is being processed based on an obligation imposed by law;

- the controller has its own independent data protection officer monitoring the controller's data protection compliance;

- the content of the data collection is public;

- the processing serves bookkeeping purposes.

(iii) Security Requirements

Personal data must be protected by appropriate technical and organizational measures against unauthorized processing. Systems and procedures for processing or transmitting personal data must ensure the confidentiality, integrity and accessibility of such data.

In particular, the data protection legislation provides that personal data must be protected against: unauthorized or accidental destruction, accidental loss, technical faults, forgery, theft, unlawful use, unauthorized alteration, unauthorized copying, unauthorized access and other unauthorized processing.

Technical measures must be assessed periodically and must take into account the purpose, manner and extent of data processing, the risk for the data subjects and the technology available.

(iv) Cross-border Data Transfers

Personal data can only be transferred outside Switzerland if the country of the data recipient provides for an equivalent level of protection. In order to ensure an equivalent of protection, the data controller may do the following:

- implement "sufficient safeguards" ensuring an equivalent level of protection, such as data transfer agreements.

- adopt binding corporate rules that ensure data protection in cross-border data transfers within a single legal entity or a group of companies.

- procure the data subject consents to the particular data transfer.

- maintain that the transfer the personal data is required for the conclusion or performance of a contract with the data subject.

- maintain that the transfer is necessary to maintain overriding public interests or to establish, execute or enforce legal rights in court proceedings .

- maintain that the transfer is necessary to protect the life or physical integrity of the data subject.

- maintain that the data subject has made the personal data publicly available and has not expressly prohibited the processing of such data.

Approval of the data transfer agreement by the Data Protection Commissioner is not required. However, the Data Protection Commissioner may review and comment on the data transfer agreement.

5.2.7 UK

In general terms, network monitoring is governed by the Regulation of Investigatory Powers Act 2000 ('RIPA') and regulations issued under it.

To the extent that network monitoring consists of the processing of personal data, the Data Protection Act 1998 (hereinafter, the "DPA"), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (hereinafter, the "E-Privacy Regulations") and the Data Retention (EC Directive) Regulations 2007 (hereinafter, the "Retention Regulations'") will be applicable.

Regulation of Investigatory Powers Act

In terms of network monitoring, the Regulation of Investigatory Powers, (hereinafter, the "RIPA") addresses both the interception of the content of communications (Part I, Chapter I) and the obtaining of access to communications data (Part I, Chapter II), which includes traffic data detailing the attributes of a person's communications activity.

The general position under RIPA is that the interception of communication content is unlawful, either as a criminal offence or as a statutory tort, if carried out by, or under the authority of, the 'system controller', i.e. the person having the right to control th e operation or use of a private telecommunication system.

Despite the general prohibition, RIPA provides for a range of circumstances that authorise the carrying out of an interception.

For the purposes of this project, the most important of these are detailed in a regulation made under RIPA: The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 [106].

These regulations permit a system controller, of a private or public telecommunication system, to monitor and record the content of a person's communications for a number of purposes, including for the investigation and detection of the unauthorised use of the telecommunications system

Part I, Chapter II of RIPA provides for ways in which designated persons withi n certain public authorities carrying out law enforcement functions can access 'communications data' (ie. traffic data, location data, routing data and subscriber data).

To the extent that any interception relates to 'communications data' rather than the content of 'communications', no interception will occur and no civil or criminal liability will arise under RIPA.

Section 22(2) of RIPA lists a number of purposes for which those designated under the DPA may obtain access to communications data held by communication service providers, such as where it is in the interests of national security or in the interests of public safety for the purpose of protecting public health.

Data Protection Act (DPA)

[106] http://www.opsi.gov.uk/si/si2000/uksi_20002699_en.pdf

Under the DPA, all businesses operating in the UK which process data relating to individuals, whether employees, customers or any other person are subject to the provisions of the DPA.

Essentially, the DPA imposes obligations on entities controlling data processing activities (controllers), and grants rights to individuals in respect of whom data is held (data subjects). The DPA contains a number of broad definitions, such as that relating to 'personal data'.

In relation to network monitoring, the UK Information Commissioner's view is that an IP address may fall within the definition of personal data under the DPA where it can be linked to an individual user perhaps through other information held or from information that is publicly available on the internet

E-Privacy Regulations

In addition to the DPA, the rules enshrined in the E-Privacy Regulations apply to providers of electronic communications networks and services and associated services who carry out network monitoring, as well as other persons who make use of such networks and services.

Application

The obligations under the DPA apply to controllers only. Where a controller uses a third party or third parties to process data on his behalf (data processor), it will be legally responsible under the DPA for the actions of its data processors.

The controller is obliged, under the DPA, to put in place written contracts with all data processors, requiring his data processors to process data in accordance with his instructions and to implement security measures, equivalent to those required to the controller under the DPA, to safeguard the data.

The obligations under the E-Privacy Regulations apply mainly to telecommunication network and service providers.

Grounds for legitimate data processing

The DPA provides that all information must be fairly and lawfully processed. This requirement is amplified by a number of rules, most importantly rules prescribing criteria as pre-conditions to legitimate processing.

Processing will be legitimate only if one or more of the following conditions is satisfied:

(1) the data subject has consented to the processing;

(2) the processing is necessary to perform a contract with, or comply with a request made by, the data subject;

(3) the processing is necessary to comply with a legal obligation of the controller (other than a contractual obligation);

(4) the processing is necessary to protect the vital interests of the data subject;

(5) the processing is necessary for the administration of justice, or for the exercise of any function conferred by statute;

(6) the processing is necessary for the legitimate interests of the controller or a third party to whom the data is disclosed, except where it is unwarranted because it is prejudicial to the interests of the data subject.

Notice to individuals

Compliance with the first principle of the DPA also requires compliance with rules relating to the provision of information to individuals.

The DPA requires controllers to provide individuals with information prior to the processing of their personal data (or within a specified period thereafter where data is obtained from a third party).

The information is to include: the name of the controller; the purposes for which the data is intended to be processed; and any additional information which is necessary to ensure that the processing is fair in the circumstances.

Where data is obtained from a third party, the controller will not have to provide this information where to do so would involve "disproportionate effort" or where collection or disclosure of the data is necessary for the controller's compliance with a legal obligation.

There are additional requirements under the DPA for the processing of sensitive data.

Communications Services

Communications network and service providers (operators of networks and services for distance communication to users via data, text, graphics, voice, video and other media) are subject to additional rules relating to the monitoring of location, traffic and billing data.

Traffic Data

The E-Privacy Regulations allow for the monitoring of traffic data by a public communications provider in the course of its business for the following purposes:

- to manage billing or traffic;
- for customer enquiries;
- to prevent and detect fraud;
- to provide value added services to the subscriber or user; and
- to market the service provider's own electronic communications services .

The processing of traffic data for the last two purposes, the provision of value added services and the marketing of services, is permissible only if the subscriber or user has given his prior consent.

The Regulations do not set out how service providers should obtain this consent.

The UK Information Commissioner's view is that in order to obtain valid informed consent, the subscriber or user should be given sufficiently clear information for them to have a broad appreciation of how the data is going to be used and the consequences of consenting to such use.

The Information Commissioner's guidance states that the service provider will not be able to rely on a blanket statement on a bill or a website but rather will need to obtain specific consent for each value added service requested and to market their own electronic communications services. If, for example, a communications provider uses a third party to provide a value added service then consent should be obtained to process for this purpose.

The E-Privacy Regulations also specifically require that the subscriber or user is provided with information regarding the types of traffic data which are to be monitored and the duration of such processing.

Location Data

Location data relating to a subscriber or user of a public electronic communications network may only be processed where the subscriber or user cannot be identified from that data, or where it is necessary to provide a value added service with the consent of the relevant user or subscriber.

Where the processing of the location data is carried out for the provision of a value added service the processing of location data should be restricted to what is necessary for those purposes.

Information that must be provided includes the name of the data controller, the types of location data that will be processed, the purpose and duration of the processing and whether the data will be transferred to a third party for the purpose of providing a value added service.

As with the processing of traffic data, the E-Privacy Regulations do not prescribe how service providers should obtain consent from users and subscribers, however relevant guidance issued by the Information Commissioner states that they should be given clear enough information for them to have a broad appreciation of how the data is going to be used and the consequences of consenting to such use.

The user or subscriber must be able to withdraw their consent at any time and the communications provider should make the user or subscriber aware of that fact. They should also be provided with an opportunity to withdraw their consent on the occasion of each connection to the network or on the transmission of a communication.

In addition, there is a self-regulatory 'Code of Practice For The Use Of Passive Location Services' in the UK developed by location service providers and mobile operators in 2004 which recommends that this information should include the contact details of the location service provider, as well as instructions on how to stop or suspend any location service offered.

Exemptions under the DPA

The DPA provides a number of exemptions from certain parts of the DPA, such as obligations to provide subject access and the non-disclosure provisions.

Key exemptions include circumstances where national security is required to be safeguarded and the prevention and detection of crime.

Retention of personal data

Under the DPA, any personal data processed for any purpose, must not be kept for longer than is necessary for that purpose.

In addition, any personal data held must be adequate, relevant and not excessive in relation to the purposes for which it is held.

Under the E-Privacy Regulations, where such data is no longer needed to transmit a communication, when the communication is terminated, that data must be erased or dealt with in such a way that it is no longer personal data.

Data required by the communications network or service provider to calculate the subscriber's bill or for interconnection charges can only be retained until the end of the period during which the bill may lawfully be challenged or payment pursued. This would usually mean a maximum period of six years plus appeals .

However, the Commissioner's view is that this provision in the Regulations merely permits the retention of such data where circumstances require it, for example, where a challenge is made to the bill during the time a communications network would normally retain the data for their own billing purposes. It does not permit the wholesale retention of such traffic data in every case.

The recently enacted Data Retention (EC Directive) Regulations 2007, implementing the Data Retention Directive, requires providers of public electronic services or networks (fixed network telephony and mobile telephony only) to retain traffic data and location data for a period of 12 months from the date of communication.

Notification

The DPA requires notification by controllers to the Information Commissioner prior to processing (save in limited cases of exemption).

The notification must include the following information:

(i) the identity of the controller;

(ii) the purposes for which data is processed, which could include monitoring;

(iii) the classes of individuals about whom information is processed;

(iv) the type of information processed (specifically highlighting sensitive data); and

(v) countries outside of the European Union to which information is to be transferred.

Notification is effective for 1 year and must be renewed annually. Failure to notify where required is an offence under the DPA.

Enforcement
Under the DPA, individuals are given the right to enforce certain obligations upon the controller and can prevent further processing in certain limited circumstances.

In addition, the Information Commissioner has broad enforcement powers under the DPA. The Information Commissioner may (with a warrant) exercise powers of entry, inspection, and seizure of documents and equipment. The Information Commissioner may also serve notices on controllers requiring compliance with the rules, including an information notice requiring the controller to provide information about his processing operations.

In May 2008, the Criminal Justice and Immigration Act 2008 amended the DPA to provide the Commissioner with the power to impose monetary penalties on data controllers for the most serious breaches of the DPA.

Sanctions and Remedies
The DPA gives the data subject a right to compensation for damage caused by any breach of the rules by the controller.

Compensation is also available in certain cases, where the data subject suffers distress as a result of the breach.

Data subjects are also able to obtain a court order for rectification, blocking, erasure or destruction of inaccurate data.

Breaches of certain rules constitute a criminal offence, for example, breach of the obligation to notify. The knowing or reckless obtaining or disclosure of personal data without consent of the controller is, subject to certain limited defences, an offence, as is offering to sell data so obtained or disclosed.

Officers of companies which have committed an offence may also be liable to prosecution. Offenders are liable to a fine of a maximum of £5,000 if convicted summarily, and an unlimited fine if convicted on indictment.

6 Conclusions

6.1 Network monitoring as a *data processing activity*

From the considerations expressed in the above section 3 of this deliverable it stems that the activity of network monitoring does represent an activity of *processing* of *personal data*.

Network monitoring is therefore subject to application of data protection legislation, and also to laws that rule on data retention. This has regard to both the European Union and also the member states' national legislations.

Having ascertained that the activity of network monitoring falls within application of data protection and also data retention law requirements, in order to assess what are the specific rules to be applied the attention should focus on the purposes for which network monitoring is performed and also on the specific features and conditions of the data processing that is considered.

As above highlighted, depending on the reasons for which the data are ga thered for network monitoring activities, different requirements may be imposed by applicable data protection legislation.

So for example a service provider performing network monitoring activities in order to guarantee security and proper functioning of its network, and so in the end in order to provide a better service to its customers, would be pursuing an interest that is considered as legitimate under data protection legislation.

Moreover, the specific features and conditions of the network monitori ng activities trigger further requirements. For example, the mere collection and processing of traffic data and location data other than traffic data, in general would determine the requirement of obtaining the data subject's consent.

As essential prerequisite, it is necessary to clearly identify the data Controller and possible third parties involved in the data processing. This is fundamental since the data Controller is the entity that should provide for compliance with data protection and also data retention applicable legislation.

6.2 The PRISM approach

The importance of the activity of traffic network monitoring from the twofold perspective of research and scientist purposes, and the commercial purposes of enhancing network and communications services, has been tackled in the above section 2 of this deliverable.

Having ascertained that the activity of network monitoring is subject to application of data protection and also data retention legislation, it seems appropriate at this point to briefly recall the main reasons, goal and rationale of the Prism project.

The first consideration to be made is that the activity of traffic network monitoring involves the gathering of a massive amount of data.

From a data protection law perspective, the mere circum stance of being enabled to collect a large number of information as such is considered as triggering data protection concerns. Indeed, deployment of data mining algorithms and specific data elaboration techniques allow the holder of the data to build preci se profile on the subjects whose data are processed.

Moreover, it is very likely that network traffic monitoring activities would involve the processing of traffic data, location data, and also sensitive data relating to data subjects; these data as above reported are considered as deserving a specific high level of protection, and thus their processing poses concerns from a data protection law perspective.

It should also be considered the circumstance that when it comes to the use of electronic services and electronic communications, the data subject is very often totally or almost totally unaware of what it is done with his data.

Indeed, the technical means may allow for the invisible collection and processing of personal data. Nor being aware of what happens to his data, the data subject is deprived of the possibility to enforce the privacy rights acknowledged by the applicable legislation.

Lastly, it is necessary that the Controller does implement the security measures set forth by applicable data protection legislation, and also the security precautions that the legislator requires in relation to the data retention requirements. The security measures serve indeed the twofold purpose of protecting the personal data from external intruders that act from the outside of the controller's organization, as well as from malicious subjects that act from within the Controller's organization (for example, malicious employees of the Controller).

The European Union and also national data protection authorities have acknowledged in several occasions[107] the importance of the technical means as an effective and important tool to guarantee proper enforcement of applicable data protection law requirements.

Art. 29 Data Protection Working Party, on the section of its web site devoted to the issue of privacy enhancing technologies, expressly states as follows: "*Though technology can be used to invade our privacy, it also provides the far most effective means to protect it.*"[108]

Moreover, the deep link existing between technology solutions and the right to data protection has been highlighted into a very recent communication of the European Union Commission on Promoting Data Protection by Privacy Enhancing Technologies (PETs)[109].

Technological solutions have been recognized by the Commission as a vital tool to make it *technically more difficult to breach data protection legislation and to violate individual's rights*[110]*;* and their deployment is also fostered with regard to detection of regulatory breaches.

In order to enhance the degree of data protection within the Community, the Commission has evaluated and determined a set of steps to be taken that are focused on fostering the widespread enforcement an development of the Privacy Enhancement Technologies, also with a view to enhance the trust of individuals in on-line services.

To the latest regards, Viviane Reding, Commissioner for Information Society and Media, has stated the following: "*People must have sufficient confidence that their personal privacy and legitimate business interests are being properly safeguarded*".

Acknowledgement of the circumstance that technology can perform a task of the utmost importance with regard to compliance with data retention law requirements is the rational that drives the Prism project, together with the consideration that traffic

[107] See for example the following documents adopted by Art. 29 Data Protection Working Party: "Privacy - enhancing technologies", adopted on October 1997, available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/petgen_en.pdf ; and Working document "Privacy Enhancing Technologies in Telecommunications", adopted on October 1997, available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/pettel_en.pdf.

[108] Please see the section of the web site of Art, 29 Data Protection Working Party devoted to the issue pf privacy enhancing technology at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/studies/priv - enhancing_en.htm.

[109] Communication IP/07/598 dated May 2, 2007, available at the following web address: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/598. This Communication follows from the First Report on the implementation of the Directive 95/46/EC - COM (2003) 265(01), 15.5.2003, available at the following web address: http://eurlex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf.

[110] As stated by Vice-President Frattini, Commissioner responsible for Justice, Freedom and Security.

network monitoring for the reasons above outlined poses severe concerns to the enforcement of data protection rights, and poses also issues with regard to the data retention issue.

The Prism project is indeed aimed at providing technical solutions and functions that allow the activity of traffic network monitoring to take place in compliance with applicable data protection legislation, and also in line with applicable data retention law requirements.