www.euro6ix.net

Title:	Document Version:
Deliverable D4.5 **Legal Position in Relation to the System /ISP and Data Protection and its Relation the Processing of Personal Data**	4.1

Project Number:	Project Acronym:	Project Title:
IST-2001-32161	Euro6IX	European IPv6 Internet Exchanges Backbone

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
30/04/2004	03/06/2004	R – PU

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author:	Organization:	Contributing WP:
Jennifer Gil	E&A	WP4

Authors (organizations):

Jordi Palet (Consulintel).

Abstract:

Deliverable 4.5 analyses the personal data issues that the deployment and use of IPv6 may involve in the information society by means of the precise analysis of different cases to which this protocol shall be applicable.

In particular, we analyze legal issues arising out of the use of this protocol in mobile telephony, personal computers and household appliances.

After the analysis of these matters, we suggest certain alternatives or proposals with the purpose of sorting out or, if applicable, minimizing the legal issues explained throughout this Deliverable.

Keywords:

Consent, Data Protection, Data quality, Data Subject, Directives, Duty of Information, Extraterritoriality, Household Appliances, Internet, IP Address, Location Data, Mobility, Privacy, Public Directories, RFC 3041, Security Measures, Self-Regulation, Traffic Data, Unique Identifier.

© Euro6IX Consortium

Revision History

The following table describes the main changes done in the document since created.

Revision	Date	Description	Author (Organization)
v1.0	20/12/2003	First draft of Index	Jennifer Gil (E&A)
v2.0	29/04/2004	Deliverable 4.5	Jennifer Gil (E&A)
v3.0	05/05/2004	Deliverable updated to match Project Deliverable Template	Jennifer Gil (E&A)
v4.0	30/05/2004	Overall review and technical accuracies added	Jordi Palet (Consulintel)
v4.1	03/06/2004	PSC Review	Jordi Palet (Consulintel)

Executive Summary

The widespread use of IPv6 could have legal consequences that have been taken into account whilst developing the Protocol. Some of these legal consequences are the implications that IPv6 might have on the right to privacy and data protection.

These matters are based on the fact that, under some circumstances, an IP address based on the Internet Protocol version 6 could be considered personal data because it could contain in its configuration a Unique Identifier which could be linked directly to the interface of the terminal that is using this IP and indirectly to its user, whom might be an individual.

One of the main scopes of this document is to analyze the current legislation on data protection adopted by the different Member States of the European Union with the purpose of determining if it might be applied initially to IPv6 or, on the other hand, if it would be necessary to adopt a specific legal legislation for IPv6.

Therefore, there are two Directives which are going to be analyzed by this Deliverable: 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, and the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Also, the implementation of IPv6 has some important consequences regarding the processing of personal data. First of all, the IP address itself is considered personal data and, therefore, its processing is bound by this legislation.

Secondly, all the information that could be related by a third party to an IP address based on an Unique Identifier, for example the information obtained by this third party about the Internet use or the results of surfing the Net by a specific user, might also be considered as personal data because at the end, it could be linked, using certain means, to its owner or data subject.

There are some means that could be used by a company or individual to link an IP address to its holder, for example, a contract or using public directories. The creation and use of these means will be analyzed in detail in this document.

To conclude, this Deliverable aims to provide a wide perspective concerning the implications, problems and advantages that the implementation of IPv6 would have regarding the privacy and data protection of its users.

Table of Contents

1. Introduction *7*

1.1 Principal Aims of the Deliverable **7**

1.2 Need of the Present Legal Study on IPv6 ..... **7**

2. What is Data Protection? *9*

2.1 Definition of Data Protection **9**

2.2 Consideration of the IP Address as Personal Data **9**

2.2.1 In all cases, could an IP address based on a Unique Identifier be considered personal data? 10

2.2.2 Could the IP addresses based on a Unique Identifier corresponding to the workplace be considered personal data? 11

3. Data Protection Legislation *12*

3.1 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of the European Council, adopted the 28th January, 1981 ..... **12**

3.2 Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data **12**

3.3 Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector **13**

3.4 Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector **13**

3.5 Domestic Legal Systems on Data Protection Adopted by the Member States **14**

4. Data Protection Legislation with Regard to the Use of IPv6 ..... *15*

4.1 Directive 95/46/EC **15**

4.1.1 Collection of IP addresses data 15

4.1.2 IP data processing 17

4.1.3 Cancellation or conservation of the information of IP address 18

4.1.4 Must Directive 95/46 be modified because of the implementation of IPv6? 18

4.2 Directive 2002/58/EC **18**

4.2.1 Consideration of IP addresses as Traffic Data 19

4.2.1.1 General considerations about Traffic Data 19

4.2.1.2 What is the conservation period for Traffic Data? 20

4.2.2 When does the Directive require the obtaining of the users/subscribers´ consent for the processing of their personal data? 21

4.2.3 Presentation and restriction of the calling and connected line identification 21

4.2.4 Consideration of IP addresses as Location Data 22

4.2.5 Regulation for the guides of subscribers 22

4.2.6 Must the Directive 2002/58/EC be modified because of IPv6? 23

4.3 Normative Developments on Data Protection Adopted by the Member States **23**

4.3.1 Germany 24

4.3.1.1 Main aspects 24
4.3.2 Austria 24
4.3.2.1 Main aspects 25
4.3.3 Belgium 25
4.3.3.1 Main aspects 25
4.3.4 Denmark 25
4.3.4.1 Main aspects 25
4.3.5 Spain 26
4.3.5.1 Main aspects 26
4.3.6 Finland 26
4.3.6.1 Main aspects 27
4.3.7 France 27
4.3.7.1 Main aspects 27
4.3.8 Great Britain 28
4.3.8.1 Main aspects 28
4.3.9 Greece 28
4.3.9.1 Main aspects 28
4.3.10 Holland 29
4.3.10.1 Main aspects 29
4.3.11 Ireland 29
4.3.11.1 Main aspects 29
4.3.12 Italy 30
4.3.12.1 Main aspects 30
4.3.13 Luxembourg 30
4.3.13.1 Main aspects 30
4.3.14 Portugal 31
4.3.14.1 Main aspects 31
4.3.15 Sweden 31
4.3.15.1 Main aspects 31

5. Practical Problems 32

5.1 New Processing of Personal Data as Consequence of the Use of IPv6 32

5.2 Obtaining Information about IP Addresses by the Processing Agents 33

5.3 Means to Consider an IP Address as Personal Data 33
5.3.1 The use of public guides or directories 33
5.3.1.1 Nature of public directories 34
5.3.1.2 Incorporation of information in the public directories 35
5.3.1.3 Some assumptions to be regulated 35
5.3.1.4 The use of Reverse Directories 36
5.3.2 Contracting of services 37

5.4 Possibility of Maintaining IP Addresses based on an Unique Identifier 37

5.5 Possibility of Tracing the User's Activities 38

5.6 What Means can exist to Comply with the Duty of Information by the Personal Data Processing Agencies? 38

5.7 Mobility in IPv6 39

5.8 IPv6 in Household Appliances 40

5.9 Security Measures to be Adopted in the Processing of IP Addresses 40

6. The Use of RFC 3041 42

6.1 Brief Explanation of How it Operates 42

6.2 Implications of its Adoption from the Data Protection Point of View 42

6.3 The Use of RFC 3041 by the Manufacturers of Hardware and Software 42

6.4 Other Relevant Considerations 43

7. The Problem of the Extraterritoriality 44

7.1 Some Problematic Cases 44

7.2 General Aspects to be Considered 44

7.3 The Power of Self-Regulation 45

8. Summary and Conclusions 47

1. INTRODUCTION

1.1 Principal Aims of the Deliverable

As a consequence of the deployment of the Internet Protocol version 6 (IPv6), there are numerous projects dedicated to the study of its development, although the vast majority of them are from a purely technical perspective.

We advocate that it is necessary to bear in mind that the widespread use of IPv6 has legal consequences that have to be taken in account whilst implementing the Protocol. These legal consequences are focused, principally, on the implications that IPv6 might have on the right to privacy and data protection.

With regard to the implications of IPv6 on the right to privacy, the Euro6IX project has already provided Deliverable 4.2 entitled "Civil Privacy and Liberty concerns in relation to IPv6", which analyzes how the adoption of the Protocol might affect the privacy of its users.

The purpose of Deliverable 4.5, though it is closely linked to right to privacy, is to analyze the possible implications that IPv6 might have on data protection, as consequence of the possible consideration of IP addresses as personal data on certain occasions.

In this respect, it is necessary to explain that although data protection is normally included inside the wider sphere that constitutes the right to privacy, it is a specific legal branch of this area that focuses on ensuring that the processing or use of personal data in respect of a natural person (called data subject) should be carried out in conformity with the existing laws.

Therefore, this Deliverable centers, first of all, on analyzing the current European legislation on data protection with the purpose of deciding if it contemplates and regulates the possible problems from the implementation of IPv6 or if, on the contrary, some modification or adjustment to the data protection legislation is necessary.

Secondly, another purpose of this Deliverable is to identify some possible problems caused by the introduction of IPv6 in relation to data protection legislation, as well as the adoption of certain technical solutions that have been developed in order to preserve the privacy of the users of this Protocol, specially, based on the RFC 3041.

Finally, a brief reference will be presented concerning the problem of the extraterritoriality and the difficulty of adopting a unique legislation that solves the problems that arise in the Internet, regulates certain "offences" and unifies useful criteria on data protection legislation.

1.2 Need of the Present Legal Study on IPv6

Though most of the studies about IPv6 focus on the development, analysis, implementation and valuation of this Protocol and, therefore, they are mainly technical studies, as it will be verified in the present Deliverable, there are certain aspects that have to be taken into account from a legal perspective.

Thus, before the definitive introduction of IPv6, the legal problems that this Protocol might have should be analyzed to find possible solutions to ensure that both, the technical approach and the legal one, are linked closely in the development and implementation of IPv6.

In this respect, the Article 29 Data Protection Working Party, an independent advisory body on data protection and privacy, established under the Directive 95/46/EC, declared its concern for the implications that this Protocol might have on the privacy of its users and their right to data protection in its "*Opinion 2/2002 on the Use of unique identifiers in telecommunication terminal equipment: The example of IPv6"*, adopted the 30th of May, 2002.

Therefore this Deliverable tries to centre on the implications of IPv6 on data protection. For this reason, one of the first sections of this Deliverable tries to explain briefly why an IP address, under some circumstances, could be considered personal data, which implies that the processing of this kind of information is governed by data protection legislation.

Also, another reason for this study is the fact that the current data protection legislation is being consolidated and it is becoming known by companies, organizations and citizens who are acquiring a wide knowledge about their rights and obligations according to this data protection legal framework.

This fact, undoubtedly, is one of the principal reasons to closely study any aspect concerning the implementation and use of IPv6 so that this Protocol can be promoted as a safe option which guarantees the confidentiality of its potential user's personal information, the only way for its implementation to be deemed successful.

2. WHAT IS DATA PROTECTION?

2.1 Definition of Data Protection

Nowadays, the concept "Data Protection" is a fundamental right of every natural person, also known as the "right to self-determination of information".

This right refers to the protection that must be offered and guaranteed to the citizens (natural persons) as consequence of the processing of their personal information (personal data) carried out by a third party in an unauthorized way. This concept is also defined as "*the legal protection offered to a natural person regarding the automatic processing of his personal information"*.

The need for the adoption of some measures to guarantee this protection has been promoted as a consequence of the advance of new technologies that allow the processing of any kind of personal data, by different agents and in a multitude of different situations, thus creating certain insecurity for the data subjects.

The right to data protection allows data subjects to decide what can be done with their personal information and to obtain the sufficient guarantees that the processing of their personal data will be carried out under the data protection legal framework.

In this respect, article 8 of the EU Charter on Fundamental Rights, adopted on December 8th, 2000, recognizes the right of all citizens to the protection of their personal information so that processing this information must be done stating specified motives and always based on the previous consent of the data subject or in compliance with data protection legality.

2.2 Consideration of the IP Address as Personal Data

The purpose of this section is to determine if an IP address can be considered as personal data. In order to do this, various basic concepts need to be observed.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted on 28th January, 1981 of the Council of Europe (known as the Convention 108) defines "personal data" as follows: "any information relating to an identified or identifiable individual (data subject)".

In the same way, the Directive 95/46/EC of the European Parliament and of the Council adopted October 24th, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, considers "personal data" as "*any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an <u>identification number</u> or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*.

Therefore, there are two essential elements that must exist in order to consider certain information as personal data:

- The data subject must be a natural person, not a legal person.

- The possibility of associating the information with the natural person who is the owner of that information, directly or indirectly.

Next, it is necessary to deduce if it is possible to link this provided information with a natural person who is already identified or who could be identified in the future (by reasonable means). Then, it could be understood that the above mentioned information is personal data and, therefore, its processing has to be carried out in conformity with the requirements determined by the current legislation on data protection.

Likewise, another essential concept which helps to understand this regulation is the concept of "processing of personal data". It is important to highlight that what is being regulated by this legislation is the processing of personal information. The mere fact of being a data subject, in principle, does not oblige the subject in any way but rather grants a series of rights relating to his personal data. Nevertheless, when a third party processes this kind of information belonging to a data subject, it becomes a situation relevant for regulation by the previously mentioned legislation.

In that case, Directive 95/46/EC explains in article 2 b), the meaning of the concept "processing of personal data" as *"any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."*

Bearing these considerations in mind, an IP address might be considered personal data because of its numerical nature, which the entity or person who is processing might potentially relate it to a certain user who might be a natural person. For example, an Internet access provider might relate an IP address to one of its users receiving one of its services.

The possibility of associating personal data and a concrete person has increased with the use of IPv6 due to the following situation. Some IP addresses created on the basis of this version 6 of the Protocol possibly including an identifying part (Interface ID or Unique Identifier: 64 bits) would identify unequivocally an interface on its terminal (PC, portable computer, PDA's, etc) which, at the same time, might end up being associated with a certain user using different mechanisms (i.e. public guides, public databases like the Whois Database).

It is important to highlight that the implications on data protection that might exist from using IPv6 do not arise exclusively because of the fact that the IP address could be associated with an individual but because it can also be considered as a "record of personal identification" of the individual and the work or activities that he carries out. In this respect, there might exist a large quantity of information that could be associated to an IP address, for example, information about: A user´s purchases, conduct, personal information, etc.

2.2.1 In all cases, could an IP address based on a Unique Identifier be considered personal data?

In general terms, if IP addresses are based on the new version 6 of the Protocol and contain in their configuration a Unique Identifier, it is important to highlight that not in all cases do they have to be considered as personal data. In order to verify this possibility, it is necessary to associate the IP address with a certain natural person. This option will be explained later in this Deliverable.

The following situation is an example of a likely connection between IP address and user. A personal computer is connected to the Internet using the Protocol IPv6. In this respect, the user, using his terminal, would access the Net only with his IP address and its Unique Identifier, which forms part of that address. In this case, the IP address would be directly linked to his terminal and could possibly be linked, indirectly, to the user.

Given that the Internet Service Provider has the possibility of associating the IP address with the holder of this address due to his contract with this services provider, there exists the probable connection of service to user, by fault of the provider, and thus the IP address of the user would be clearly considered as personal data.

On the contrary, the same example shows a situation where the computer used to access to the Net belongs to a Cybercafe, thus the user, who accesses using the above mentioned IP address, changes frequently. In this second situation, the Internet Service Provider might not be able to associate the IP address with the concrete user who is surfing the Net. Therefore, the IP address would not be regarded as personal data.

2.2.2 Could the IP addresses based on a Unique Identifier corresponding to the workplace be considered personal data?

There exist the doubt to whether an IP address that identifies a certain working device or computer in a company might be categorized as personal data or not. This doubt is based on the supposition that the activities undertaken whilst using this IP address will not be included in the private sphere of it's user. In other words, it is assumed that an IP address which belongs to a person and is used for private purposes *must* be considered as personal data. On the other hand, the IP of a workplace is not included in this category of data because it does not belong to the private sphere of the user.

This assessment is not adequate from the point of view of the data protection legislation since the only valid criteria to determine if an IP address is personal data or not is its connection with the natural person who directs the node or the terminal that is accessing the Net.

With regard to the likelihood of relating an IP address to a concrete natural person, it is necessary to examine the further limitations to this aspect of IP addresses, presented in later sections of this Deliverable. This is because certain providers (in forward, agents, providers or actors) could be making this relation of IP address and user directly, whereas other providers would not have this option or would have to come to alternative means of achieving this association.

3. DATA PROTECTION LEGISLATION

The aim of this section is to give a brief analysis of the Directives and more important European agreements and conventions on data protection which might be applied initially to IPv6.

However, it appears repetitive to address this analysis and others regarding the progression of the different existing legal frameworks on this matter and previous studies on data protection conducted in different States, since this information was already provided by Deliverable 4.2.

That being said, the principal purpose put forth in the following sections (3 and 4), is to analyze the current legislation on data protection, examining the three following elements:

- To study the current processing and regulation of personal data in Europe by the analysis of the most important legislation on this matter.
- To observe how the Member States have included this framework in their legal systems, highlighting those which should be considered most important.
- To conclude if IPv6 is perfectly regularized by the current legislation or if there are some specifics that would have to be considered by this legislation.

3.1 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of the European Council, adopted the 28th January, 1981

This Convention, also known as Convention 108, is a representation of one of the first efforts carried out for the creation and expansion of the legislations on data protection, inclined to regularize the processing of personal information. According to this Convention, the signatory States were required to include in their legal systems the necessary measures and guarantees to concrete the basic principles on data protection.

In few words, the purpose of this Convention is *"to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him"*.

3.2 Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 95/46/EC was enforced in 1995, some years after the signature of Convention 108, with the aim to establish the basic principles on data protection which each Member State must incorporate into their domestic legal system. Thereby, it was created as a common and homogeneous legal framework for the European Union relating to this matter. As it states in the Preliminary Consideration Number 25, its purpose is to guarantee the protection of all the personal data, automatic processed by public or private entities and organizations.

As its principle goal, it establishes the following: *"the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom the subject of processing are, to be informed that processing in taking place, to consult the data, to request corrections and even to object to processing, in certain circumstances"*.

3.3 Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Keeping in mind the multitude of new digital public telecommunications networks and the important processing of personal data carried out by these telecommunications companies, this Directive was published in order to define the basic principles that should govern the specific data processing taking place in this sector.

In effect, some of these aspects include the following:

- The processing of traffic and billing data.
- Itemized billing.
- Presentation and limitation of the identification of the calling and connected line.
- Public directories.

As can be seen, Directive 97/66´s main objective is detailed more specific in comparison to that of Directive 95/46, which puts forth a more general legal framework. Directive 97/66 aims to solve *concrete* problems of this sector which, in numerous occasions, might serve as criteria to resolve possible problems detected in relation to IPv6. An example may be regulating the limitation of the identification of the calling line or the regulation of public directories in general.

Nevertheless, this Directive has been repealed by the recent Directive 2002/58/EC. In spite of this latter Directive extending its legislation to the whole frame of data protection in relation with new technologies (telecommunications and electronic communications, in general), it supports part of the legislation already established in the Directive 97/66/EC.

3.4 Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector

As previously mentioned, Directive 2002/58/EC repealed Directive 97/66, further intending to specify the legislation given by the Directive 95/46 for the particular sector of the electronic communications according to its articles.

This legal framework aims to protect and safeguard the privacy of the subscribers and users of services of electronic communications. Principally, this Directive regulates the following aspects:

- Technical and organizational safety measures that must be adopted by the providers of electronic communications services.
- Confidentiality of the communications.

- Processing of traffic data.
- Itemized billing.
- Presentation and restriction of calling and connected line identification.
- Processing of location data.
- Directories of subscribers, etc.

3.5 Domestic Legal Systems on Data Protection Adopted by the Member States

As a result of the Preliminary Consideration Number 22 and article 32 of the Directive 95/46/EC, the Member States were bound to adapt their domestic legislations to the principles and obligations regarding the processing of personal data, taken under this Directive. In compliance of this duty, the different Member States have been adopting their own domestic regulations tending to regulate these aspects. Some of these domestic legislations will be analyzed in Section 4.3 of this Deliverable.

4. DATA PROTECTION LEGISLATION WITH REGARD TO THE USE OF IPV6

This section focuses on analyzing the adequacy of the previously mentioned Directives at the moment of using IPv6 to determine the effectiveness of these Directives in terms of detecting new aspects that may develop as a consequence of implementing IPv6 or, if lacking effectiveness, there should be modifications to the Directives.

In particular, this analysis will focus on two specific Directives: 1) Directive 95/46 as it is considered the principal legislation on data protection and 2) Directive 2002/58/EC because of its significant contribution to the electronic communications sector, precisely where the new Internet Protocol, version 6, can be categorized. Finally, some brief considerations will be gathered about the adequacy of the domestic regulations on data protection adopted by the different Member States.

4.1 Directive 95/46/EC

The analysis of this Directive will centre on three fundamental existing aspects on the processing of personal data and, thus, on the processing of IP addresses data:

- Obtaining the IP address data.
- Processing of this data by the agents being capable of associating IP address data with a machine and even a user.
- Cancellation and suppression of the IP address information.

Regarding each of these steps for the general act of processing personal information, the legislation for such an act requires certain principles and obligations that any processing agent would have to fulfill.

That being said, this section examines whether the processing of the information of IP addresses could be done in conformity with the legislation provided by the Directive, keeping in mind the above three aspects, and if so, whether it is possible to achieve such an aim under the existing IPv6.

4.1.1 Collection of IP addresses data

The following are the three main principles stated in the legislation which have to be considered when someone (the agent or the collector) proceeds to obtain personal information from any other person: Quality of the information; duty of information and obtaining the appropriate data subject's consent.

1. Regarding the **principle of data quality**, article 6 establishes the obligation that personal data must be collected and processed as follows:

- Processed fairly and lawfully.
- Collected for specified, explicit and legitimate purposes.
- Not to be further processed in an incompatible way with those purposes.
- Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

- Data must be accurate and kept current.
- Data must be kept in a form which permits the identification of data subjects for no longer than is needed for which the data were collected or for which they are further processed.

This article obligates that all processing of the IP data itself (when it is considered as personal data) and of other personal data which could be related to an IP address, have to be activities that must conform to these basic principles.

2. Regarding the **information to be given to the data subject**, article 10 enumerates different aspects which the data subject must be informed about, by way of the data collector:

- The identity of the controller and of his representative, if any.
- The purposes of the processing of the personal data.
- Recipients or categories of recipients of the data.
- If the reply to the questions is obligatory or voluntary, as well as the possible consequences of failure to reply.
- The existence of the right of access to the data and the right to rectify.

The moment when the collector obtains the information of the IP address itself and the information that potentially could be associated with this IP address, the collector will have to inform the data subject about these aspects.

The main problem is that this article is applied when the data subject gives his personal information to the collector personally, but there also exists the possibility, in certain cases, that the data subject gives his IP address while surfing the Net and, therefore, without being fully conscious of sharing this information. In this case, it is questioned who is obliged to inform the parties about the situation and in which appropriate way.

Though the answer to this problem should be analyzed case by case, a general answer would suppose that every natural or legal person while surfing the Net, sending emails or receiving communications, for example, becomes familiar with his IP address, processes it, stores it and is able to associate this IP to its owner, thus being held to the legislation as well as by the rest of the requirements of the Directive.

On the other hand, article 11 refers to the suppositions in which it is necessary to observe this legislation though the personal data is not obtained directly from the user. A case in point example is one in which the collection of the IP address, as well as the information associated with it, is given by an Internet Access Provider to a company dedicated to the elaboration of consumers profiles.

As can be seen, these articles establish obligations that could be difficult to observe according to the different agents that process personal data. In this respect, section 5.6 of this Deliverable examines how an IP address may, at first, be associated with its holder by an Internet Access Provider. Nevertheless, there might exist other series of agents (i.e. a provider of services of virtual shop) that by reasonable means (public guides, databases, etc) have the possibility of associating the IP with its holder. In these cases, the problem is deciding who will have to comply with this duty of information: the access provider; the provider of the services of virtual shop or both of them.

3. Finally, regarding the **necessity of obtaining the consent** of the data subject to process his personal data (in this case, his IP address and the data related to that IP address), article 7 of the Directive states that personal data only could be processed when:

- The data subject has unambiguously given his consent (explicit consent, in a few cases and tacit, in others).
- Processing is necessary for the performance of a contract to which the data subject is considered as a party.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary in order to protect the vital interest of the data subject.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed.

In short, the processing of this kind of information will have to be carried out with the data subject's consent or when at least one of the pointed circumstances takes place. In any case, these circumstances could be increased by the different national regulations adopted by the Member States.

Also, article 8 of this Directive determines special requirements for the processing of some categories of data. These categories are racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sexual orientation. For example, these types of special data could be contained in the information that could potentially be related to a concrete IP address.

In that sense, this Directive bans the processing of these categories of data unless it is based on one of the exceptions described in this article. Some of these exceptions are: Obtaining the explicit consent of the data subject, the processing being necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law, the processing being necessary to protect vital interests of the data subject or another person, etc.

These considerations are relevant from the point of view of certain suppositions in which, for example, a service provider could have access to this type of information. An example could be a provider of erotic contents who has a web page which the users can access. If a user is accessing with an IP based on a Unique Identifier, this provider could have information about the sexual contents that this user is accessing and, moreover, he could have the possibility of associating this IP with the machine and, potentially, with the user. In this case, the processing of sexual orientation information associated with an IP and with a user would take place and, therefore, would be bound to the obligations within this article.

4.1.2 IP data processing

Once the personal data are obtained (the IP address itself and, in some cases, another personal information that could be associated with this IP address), the Directive foresees another series of articles intending to regularize these same situations of data processing.

These articles establish the obligation for the agents to adopt some legal, technical and organizational measures to assure the confidentiality, integrity and safety of the personal information. However, the Directive does not establish the type of technical measures to implement, so the domestic legislation of the Member States should determine them. Furthermore, this Directive establishes how the processing of personal data should be executed by third parties.

4.1.3 Cancellation or conservation of the information of IP address

The Directive does not clearly declare which are the requirements that must be highlighted to proceed to the cancellation or to the conservation of personal data. Therefore, it is not possible to know how much time the information regarding IP addresses must remain in the different agents' files and systems or in what cases they would have to be cancelled.

Therefore, it would be necessary to analyze the considerations made by each of the different domestic legislations in order to be able to determine, with certain accuracy, the mentioned time period of conservation of data in light of the remaining parts to the legislation that will be applicable to every supposition of conservation of information.

4.1.4 Must Directive 95/46 be modified because of the implementation of IPv6?

It is indisputable that one of the principal debates generated as a consequence of the future utilization of IPv6 remains the probable necessity of modifying this Directive to adapt it to new problems that could be caused by implementing this Protocol or, on the contrary, the probability that this regulation is suitable for IPv6 and its implications.

As stated previously, the articles of the Directive might be considered applicable to the processing of information derived from the use of IPv6 and, therefore, since the consequences of its use do not differ nor contradict the Directive's principles, obligations, and rights, it would be necessary to determine that there would be no need to modify the Directive.

In this sense, Preliminary Consideration Number 68 of the Directive states that: "*Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular, as far as certain sectors are concerned, by specific rules based on those principles*".

Likewise, the duty of adequacy of these principles to more specific sectors will have to be carried out, for example, by specific legislation or codes of conduct which help, in a dynamical and flexible way, to adapt these principles to every sector involved in the processing of personal data.

Article 27 of the Directive distinguishes between national Codes of Conduct, which will have to be promoted by the Member States and checked by the national authorities on data protection and community Codes of Conduct, which will be submitted to the review of the Article 29 Working Party.

4.2 Directive 2002/58/EC

This Directive is more closely connected with the supposition that is the object of analysis of this Deliverable (implementation of IPv6), since it regulates the specific requirements for processing personal data in relation to the new services of electronic communications. Some of the aspects regulated might be the services of location of terminals, the supply of information, traffic data processing and, in general, any service that could be provided through public electronic communications networks.

In any case, it is important to highlight that what is not regulated by this Directive, will nevertheless be covered by Directive 95/46/EC. For this reason, this section only will consider the specific matters covered by this Directive 2002/58/EC.

4.2.1 Consideration of IP addresses as Traffic Data

One of the most important concepts in this Directive is "Traffic Data" which is defined in paragraph b) of its article 2.

"Traffic Data" must be understood to mean *"any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof"*.

And "communication" must be understood to mean *"any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service"*.

In this regard, the Preliminary Consideration Number 15 clarifies that *"traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection "*.

As a result, it is possible to consider an IP address as traffic data because it helps to conduct the communications along the network.

In this respect, the Directive introduces some parameters which must be considered in the processing of this kind of personal data.

4.2.1.1 General considerations about Traffic Data

Article 5 of the Directive establishes the need to assure the confidentiality, not only of the information which is transmitted, but also of the traffic data related to this information.

This kind of information should only be intercepted, recorded, stored, listened to or monitored when:

- The user has consented.
- Those who carry out these actions are legally authorized to do so.

Nevertheless, the Directive allows for the technical storage of traffic data when it is necessary for the conveyance of a communication. Therefore, if the storage of this kind of data by the Internet access providers, telecommunications companies, etc, is only for this purpose, it would be allowed by the Directive.

Extrapolating these considerations to IPv6, IP addresses, as traffic data, must be confidential. The fulfillment of this obligation is more important in relation to an IP generated with a Unique Identifier since it would be simpler for a non authorized third party, to associate the communication, with the IP, with the machine and with the user that generates it.

For this reason, it is possible to process this kind of traffic data for the following purposes: The conveyance of the communications, subscriber billing and the interconnection of payments. For processing of this type of information for any other reason (i.e. commercial promotion or provision of value added services), as a general rule, the consent of the data subject will be needed (tacit or explicit).

Finally, it is important that every provider or agent that processes this personal information, in any case, will have to comply with their duties in relation to the information and obtain the required consent, as has been outlined in the previous paragraph.

4.2.1.2 What is the conservation period for Traffic Data?

The Directive allows for the storage of traffic data by certain providers, but it must be done in conformity with a series of criteria that guarantee that the data is stored only for the period of time necessary. In addition, this kind of data must be erased when it has stopped being necessary for the purposes that motivated the processing (the conveyance of the communication). Also, its processing is allowed for some purposes such as subscriber billing and for the interconnection of payments, so it can be concluded that traffic data would have to be erased when its continued storage is not necessary for the fulfillment of these purposes.

Preliminary Consideration Number 27 clarifies that "*the exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service provided. For instance, for a voice telephony call, the transmission will be completed as soon as either of the users terminates the connection. For electronic mail, the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider*".

Also, it is significant that one of the alternatives offered by the Directive instead of the erasure of traffic data is to make it anonymous. This possibility raises certain practical difficulties for the providers, in case of the IP addresses generated by a Unique Identifier. These providers would need to adopt some type of measures which make it impossible for them to associate the IP with the user.

Although, these are the main points of the Directive, it is important to highlight a new legislative trend that was being forged within the EU during the preparation of this Deliverable. This trend is based, among other reasons, on the need to fight and prosecute the crimes of terrorism, which could result in series of modifications or amendments regarding the processing and conservation of traffic data.

Specifically, through the press release 7555/04 (Presse 94) of the Extraordinary Session of the Council of Justice and Matters of Interior, held in Brussels on March 19, 2004 as consequence of the terrorist attempts perpetrated in Madrid and presided over by D. Michael McDowell, the European Commission has demonstrated its intention to present in June 2004, a proposal to force Internet providers and the telecommunication companies to store, (for a minimal period of between 2 and 3 years), the traffic data of the users, with the principal aim to attack, using the Internet as a method to assist the commission of terrorist acts.

This future regulation would not be contradictory with what is established in the present Directive since its article 15 allows the adoption of measures to restrict the scope of the rights and obligations of the users and subscribers, when these restrictions are necessary to protect safety, the investigation and prosecution for the commission of criminal acts.

4.2.2 When does the Directive require the obtaining of the users/subscribers´ consent for the processing of their personal data?

Generally speaking, the scope of the Directive states that any activity related to he provision of services of electronic communications which goes beyond the mere conveyance of a communication or billing the service (i.e. the provision of value added services), will have to be based on anonymous information and, in case this is not possible, it will be necessary to obtain the data subject's consent.

4.2.3 Presentation and restriction of the calling and connected line identification

Another main article that could be applied to IPv6 is article 8, which deals with the presentation and restriction of calling and connected line identification. In this respect, although this article might seem to be more focused on the regulation of the services of telephony (mobile or landline), it may be understood that it could be applied to the different cases of electronic communications carried out by using IPv6.

This article demonstrates the intention of the legislator to preserve the privacy of the user who carries out the call, obliging the service provider to offer him technical possibilities that avoid the identification of the calling line, when there exist the possibility that this could be visualized.

In the same way, the legislator wishes to protect the interests of the user allowing him, when receiving calls, to reject the incoming calls when the identification of the incoming caller has been prevented by the calling user.

Following the criteria established in this article, it could be said that, regarding the IP addresses based on a Unique Identifier, users must be able to demand of their providers the adoption of certain preventative mechanisms:

- The identification of the IP address of the user, in the cases in which this identification is not necessary.
- The possibility for the recipient to reject communications transmitted with a certain IP address, when the sender uses the option which allows the restriction of the identification of his IP.

Nevertheless, the Preliminary Consideration Number 19 states that, in those particular cases in which the adoption of these measures is technically impossible for the providers or in which it requires a disproportionate economic effort, the implementation of these measures will not be mandatory. In any case, the interested parties will have to be informed of this impossibility and the Member States will have to notify them to the Commission.

In certain ways, at present, some technical measures are being adopted that encourage these types of activities which are applicable to the IP addresses, some of them based, actually, on the proposed standard RFC 3041.

However, the Directive sets out several cases in which the provider might override the restriction of the identification of the incoming caller. These cases are:

- When it is necessary to trace malicious or nuisance calls.
- When it is necessary to deal with emergency calls, by organizations recognized by the Member States such as enforcement agencies, ambulance services, fire brigades, etc.

4.2.4 Consideration of IP addresses as Location Data

"Location Data" must be understood to mean, as it is stated in article 2 c) of the Directive "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*".

In conformity with the Preliminary Considering Number 14, the location data will be that referring 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 or to the time the location information was recorded*".

In mobile digital networks, it is possible to process location data (which are considered to be traffic data) which can provide the geographic position of the terminal equipment of the mobile user to enable the transmission of the communications.

This fact takes on significant relevancy in the cases in which a device with mobility (PDA's, laptops, mobile telephones, etc.) accesses the Net using an IP, since apart from the existence of the possibility of tracing its movements and surfing, it would be possible to know its physical location, both of the terminal and of the owner of that terminal.

This possibility enables different types of new processing of information that will have to be regularized in conformity with the Directive 95/46 and the national legislation of the Member States, for example, the possibility of acquiring (in most of the cases in an illicit way) this type of information for providers of services of information about the conditions of the vehicles traffic, to offer certain services to a user, on occasions without his specific request (i.e. the state of the traffic in the highway along which he is driving); the control of the teleworkers or the creation of profiles, habits of a certain person, which, from a merely commercial aspect, might bring important economic advantages for those who want to take advantage of these types of technological advances.

In this respect, it is important to highlight that the Directive establishes that this type of information, will only be able to be processed with the consent of the user and, although this have been given for a specific moment, there must be established mechanisms that enable the withdrawal of this consent at any moment.

Likewise, the Directive allows for the processing of this kind of information, by those agents who act in the name and under the instructions of the electronic communications services provider, acquired by the user, not allowing to non authorized third parties to process them.

4.2.5 Regulation for the guides of subscribers

As will be considered in later sections of the Deliverable, one of the means that would allow the association of a certain IP with a certain user and, therefore, that would promote the consideration of the information of IP as personal data, is the adoption of public guides which contain the description of the user and his IP address.

Taking this into consideration, it might be useful to have in mind the criteria established by the Directive regarding this type of public guides.

The user can decide if he wants to disclose his personal information to a third party or not, but, in any case, the incorporation of this data in the abovementioned guides will require that the entities in charge of their provision or the service providers regarding these guides, inform the owners of the information kept of the purposes of these guides, as well as of the rest of the parameters of the duty of information (transfers of information, possibility of exercising the rights of access, rectification, etc.), and obtain their consent.

In this respect, any use of these guides by an agent based on different purposes as those for which the consent was obtained initially from the data subject, will require the obtaining of a new consent by this agent.

In short, article 12 establishes a series of parameters that will have to be born in mind by the Member States at the time that these public guides are created:

- Obligation to inform the owners of the information (subscribers) of its incorporation in the guide.
- Possibility that the guides are printed or electronic.
- Subscribers' power to decide, which data are going to appear in the guides.
- Respect for the main principles and obligations of this legislation, in terms of the quality of information: incorporation of suitable, pertinent and not excessive information.
- The fact of not being included in this kind of directories or any other activity related to these must be free of charge.

The analysis of the consequences that the creation of this type of IP guides might bring is set out in section 5.3.1 of this Deliverable.

4.2.6 Must the Directive 2002/58/EC be modified because of IPv6?

At the moment, this Directive is the regulatory framework for privacy and data protection which comes closest to the regulation that should be offered because of the use of the new Internet Protocol version 6.

Most of the articles gathered in the Directive regulate some cases that, directly or indirectly, could be related to IPv6. In certain cases, like the possibility of restricting the identification of the line of origin or the regulation of the public guides of subscribers, although it seems to be clear that the above mentioned articles try to regulate different cases, they might be applied analogically to the use of the Protocol in its new version 6.

In this respect, it could said that this Directive offers the general criteria to be taken into consideration by the Member States at the time of regulating the use of IPv6 by each of their domestic legislations and the way of complying with the obligations imposed by this Directive and the Directive 95/46.

4.3 Normative Developments on Data Protection Adopted by the Member States

As a consequence of Preliminary Consideration number 22 and of article 32 of the Directive 95/46, the Member States will have to adapt their national legislation in accordance with the regulations contained in this Directive. For this reason, the different Member States have passed their own laws in order to regulate these matters.

For information purposes, some of these States that already have regulation, more or less restrictive, on data protection are Germany, Austria, Belgium, Denmark, Spain, Finland, France, Great Britain, Greece, Holland, Ireland, Italy, Luxembourg, Portugal and Sweden.

As will be seen below, country by country, there are not many innovations contained in these regulations, which are usually a mere reflection of the dispositions of the abovementioned Directive 95/46.

Since it has been introduced, the main laws approved by the Member States on data protection replicate faithfully the obligations, rights and principles stated in the Directive 95/46, so it is not common to find "new" applicable articles intended to regulate specific cases like IPv6. In this respect, it would be necessary to analyze the legislation adopted by these States which intend to legislate some specific sectors of activity as, for example, the telecommunication or Internet sectors.

4.3.1 Germany

Germany was a pioneering country in the adoption of data protection regulation, since the first law was that known as Law of Hesse, of October 7, 1970.

Later, it was passed as the German Federal Law on Data Protection January 27, 1977, which was subsequently amended by the law called Bundesdatenschutzgesetz (BDSG), which came into force on June 1, 1991.

The regulation that is currently in force is the named “The Federal Data Protection Act” (Bundesdatenschutzgesetz) of May 18, 2001.

Likewise, it is important to emphasize that several laws have been approved by different German cities (Berlin, Brandenburgo, Essen, Saarland, etc.) on this matter.

4.3.1.1 Main aspects

The objective of the Act is to protect the individual against his right to privacy being violated through the processing of his personal data (article 1). For this purpose, the norm is a true reflection of the personal data protection model created by the Directive 95/46 and regulates principles and obligations, such as the quality requirements in the collection of data; need of obtaining the consent for the processing; safety and audit principle, etc.

Likewise, in Chapter III, functioning of the German Authority of Control (Federal Data Protection Commissioner) is regulated.

4.3.2 Austria

The first Austrian law on data protection (Datenschutzgesetz) is dated October 18, 1978 and this was amended later by the Decision 609/1989 of the Constitutional Court.

The current Act in force is the Federal Act Concerning the Protection of Personal Data (Dasenschutzgesetz 2000), which came into force on January 1, 2000.

Likewise, different regions (Länders) have adopted their own regulation, such as Kärnten, Salzburg or Vienna, among others.

4.3.2.1 Main aspects

Some of the most important aspects contained in this Act are the following:

- The right to data protection is considered to be a fundamental right (article 1).
- The restrictions on the right to secrecy are only permitted to safeguard the overriding legitimate interests of another (article 1).
- The controllers of a joint information system (joint data processing system by several responsible persons with reciprocal access to the data) shall, unless already regulated by law, appoint a suitable operator for the system, whose name and address shall be included in the notification for registration in the Data Protection Register (article 50).

In short, apart from adapting the Directive 95/46, the Austrian law regulates, in the framework of this Directive, some issues that do not appear in other legal systems, like that mentioned article 50.

4.3.3 Belgium

The first Law on data protection adopted in Belgium is dated December 8, 1992. The current regulation came into force on September 1, 2001.

4.3.3.1 Main aspects

The law states that every individual has the right to the protection of his liberties and fundamental rights, particularly to the protection of his private life in relation to the personal data processing (article 2).

The law applies to automatic processing as well as to non-automatic (article 3). Following this initial policy, the law determines the requirements established by Directive 95/46 and, therefore, sets out some of the main principles and obligations such as the obligation to register files; to respect the rights of the data subject; the special processing of the sensitive data, etc.

4.3.4 Denmark

In Denmark, the first legislation on data protection was two-fold: One applicable to files in public ownership, the Law 294 of June 8, 1978 on public records (later modified on several occasions) and another for files in private ownership, the Law 293 of June 8, 1978 on private records, also modified on several occasions.

The current legislation in this matter is “The Act on Processing of Personal Data” (Act No 429) of May 31, 2000.

4.3.4.1 Main aspects

The Act applies to data processing, automatic or not, where the data subjects are individuals. Nevertheless, certain parts apply, as well, to data processing relating to companies (article 1), so a significant change is introduced in comparison to the application and scope contained in Directive 95/46.

The Act states that Official authorities and private companies may not carry out any automatic registration of the telephone numbers from which calls are made, except with the prior authorization from the supervisory authority in cases where important private or public interests permit. This prohibition shall not apply when it is carried out by operators of telecommunications or in the rendering of services for the identification of the lines.

4.3.5 Spain

In Spain, the first law that came into force was known as LORTAD, Organic Law 5/1992, of October 29, containing the regulation of the automated personal data processing.

Later, this law was repealed by the Organic Law 15/1999 of December 13, of Protection of Information of Personal Character (also known as LOPD), currently in force.

Similarly, it is important to understand that article 9 of the LOPD was developed by the Royal Decree 994/1999, 11th June, the Regulation of Security Measures to be adopted in personal data processing. This Regulation determines the appropriate technical and organizational security measures to be adopted in order to maintain security and to prevent any unauthorized processing of personal data.

In this sense, this Regulation determines three different personal data categories or security levels (basic, medium or high security levels). Each level includes different security measures which must be implemented depending on the type of personal data to be processed.

4.3.5.1 Main aspects

The objective of the law is to guarantee and protect, regarding the personal data processing, the public freedoms and the fundamental rights of the individuals and, especially, of their honor as well as personal and family privacy. In general terms, the Spanish Law is a true reflection of the common community regime established by the Directive 95/46. In this respect, it regulates the principle of quality of data; duty of information; need to obtain the consent for the processing (in general); special processing of sensitive data; conditions for data processing carried out by third parties, etc.

Some of the articles that might be related to some of the topics to be studied in this Deliverable are the ones concerning the phone directories that are considered to be a source accessible to the public, in the terms contained in their specific regulation.

4.3.6 Finland

The Finnish regulation on personal data has been based on three fundamental laws:

- Law of April 30, 1987 on files of personal information.
- Law of April 30, 1987 on the Commission and the Ombudsman for the protection of information.
- Decree of April 30, 1987 on files of personal information.

Now, the legislation in force is “The Finnish Personal Data Protection Act” (523/1999) of April 22. Nevertheless, this law has suffered certain modifications made by “Act on the amendment of the Personal Data Act” (986/2000) that came into force on December 1, 2000.

4.3.6.1 Main aspects

Article 1 establishes that its aim is to implement, in the processing of personal data, the protection of private life and the other basic rights that safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice.

Some of the general rules for the processing of personal data, which are set out in Chapter 2 of the rule, are: the determination of the purpose of the processing; the obligation to process personal data exclusively in conformity with the above mentioned purpose; the quality of the information; the duty of information; the processing of sensitive information, which is prohibited if there do not happen some of the circumstances pointed out in the article, such as the obtaining of the express consent of the data subject; international transfers; the regulation of the rights of access and rectification, etc.

One of the innovations set out on Section 13 relates to the processing of the identity personal number. This processing needs to be based in the obtaining of the unequivocal consent of the data subject.

In the same way, Section 17 regulates the creation of public registers. Personal data can only be included in these public registers if the data subject does not prohibit the collection and introduction of that data in those registers.

Another innovation found in this rule is in Section 21, which establishes different periods of keeping of the information by the controllers of the files containing personal data.

Finally, under Section 38 the Authority of Control on data protection in Finland, called The Data Protection Ombudsman, is created.

4.3.7 France

The first French law on this matter was the Law 78-17 of January 6, 1978. Nowadays, the French Parliament is debating the adoption of a series of modifications to this law.

4.3.7.1 Main aspects

Article 1 state that the processing of personal data will not infringe human identity, neither the rights of the individual, nor privacy, nor individual or public freedoms.

The concept of automatic processing of personal data refers to any series of operations effected by automatic means, including the collection, recording, preparation, modification, storage and destruction of personal data, as well as any operations relating to the use of files or data bases, including interconnections, the consultation or the communication of personal data.

Since the French law predates Directive 95/46, it is necessary to guarantee its evolution in conformity with the criteria indicated by the Directive and, therefore, these criteria will have to be born in mind for the new regulation that will be adopted in France.

4.3.8 Great Britain

The British legislation on data protection begins with the Law of July 12, 1984 (Data Protection Act). Likewise, Great Britain has a Regulation, October 13, 1985 dedicated to the Data Protection Court.

Later, this legislation has been repealed, being in effect "The Data Protection Act of 1998".

4.3.8.1 Main aspects

Through this regulation, different obligations required by Directive 95/46 are regulated. In Part I, some of them are set out such as the right of information, obligation to rectify, block, erase or destroy personal data, prohibition of processing personal data if, previously, the file has not been notified to the British Authority of Control called "Data Protection Commissioner ".

Likewise, it is stated that any processing of information that is carried out for the purposes of prevention or detection of crimes, arrest or prosecution of the persons in charge, will not be linked to the duty of information. In this sense, the processing of IP address data according to these purposes will not require the compliance by the controller, with the information duty.

The principle of obtaining the consent as a main requirement to effect a processing or transfer of personal data is set out in Section 55.

Part II of the statute, sets out the interpretation of the principles contained in the statute as well as the determination of the conditions to be born in mind for the processing of all kinds of information and, specially, of sensitive information, as well as determine the cases in which each of these principles would not be applied.

4.3.9 Greece

The Greek Law 2472/1997, on protection of individuals with regard to the processing of personal data was approved on April 10 of 1997.

4.3.9.1 Main aspects

The scope of this law is to determine the conditions regarding the processing of personal data and the protection of the human rights, fundamental freedoms and private life, as it is established in article 1.

Following the guidelines of Directive 95/46, this law is outlined with respect to certain principles such as the quality of the information, the duty of information, the need to obtain the consent for the processing of personal data, except in those cases considered as exceptions in article 2. In any case, it will be necessary to obtain written consent for the processing of sensitive data.

Other principles and obligations relate to the interconnection of files, which will have to be reported to the Greek Data Protection Authority and, in case they should be based on sensitive information, the controller would have to obtain prior authorization, the regulation of international data transfers; the exercise of the rights of access and opposition or sanctions and penal and administrative infringements, among others.

4.3.10 Holland

The first Dutch law on data protection was the Law of December 28, 1988, called "Wet Personenregistraties" and better known as WPR.

Nowadays, the regulation in force is the "Personal Data Protection Act of July 6, 2000".

4.3.10.1 Main aspects

This law applies to the automatic processing of personal data, as well as to non automatic processing.

Articles 7 to 11 set out some of the requirements that must exist in any processing of information: the obtaining of information for legitimate, specific and explicit purposes; data must be necessary for the fulfillment of a legal obligation or for the fulfillment of a contract (among other reasons); conservation of the information during the time necessary for the fulfillment of the purpose of processing, etc.

On the other hand, articles 16 to 24 regulate the processing of the sensitive information (religion, philosophy of life, politics, race, health, sexual life, trade union membership and criminal behavior).

In some cases, for example, for the processing of information regarding race or ethical origin, amongst the reasons that allow its processing, it is the fact that the data subject had not refused this processing in writing, which differs from the regulations of other Member States on this matter.

Article 25 sets out the possibility of the adoption Codes of Conduct by different entities, for which the approval of the Data Protection Commission (Dutch Control Authority) would be needed.

The duty of information is set out in articles 33 and 34 of this law. Likewise, this law also regulates the rights of data subjects, the international transfers and the breaches and sanctions, among other obligations already imposed by Directive 95/46.

4.3.11 Ireland

The first Irish Law on data protection was dated July 13, 1988. Now, a Bill of law is being debated before the Parliament.

4.3.11.1 Main aspects

The Data Protection Act of 1988 is a quite old law. Article 1 defines "personal data" as all information relating to a living individual who can be identified either from the data or from the data in conjunction with other information in possession of the data controller.

Articles 4 to 6 regulate the conditions for the exercise of the right of access and rectification by the data subjects.

The Irish Control Authority (called the Commission) is created by articles 9 and 10.

Other common matters regulated by this law are the international transfers of personal data; the specific requirements for the notification of files or breaches and sanctions.

4.3.12 Italy

The Italian Law on data protection is the Law 675/96 of December 31 (Tutella delle persone e di altri soggetti rispetto al trattamento dei dati personali). In addition, a set of laws has been approved on the basis of this statute, especially, royal decrees such as: nº 123 dated May, 1997; nº255 dated July, 1997; nº135 dated May, 1998 or the most recent, nº 282 dated July, 1999.

4.3.12.1 Main aspects

As established in its article 1, this law tries to assure that the processing of personal data is carried out respecting the fundamental rights and freedoms and the dignity of natural persons, with special regard to their right to privacy.

Similarly, as an innovation, it guarantees the rights of legal bodies, in this respect.

Following the criteria of Directive 95/46, some of the main principles are: data quality; the duty of information to be given while collecting personal data; the obtaining of the consent and exceptions; data processing security, principles that will be implemented by a royal decree; data disclosure to third parties; the processing of sensitive information or international transfers, among others.

Specifically, this law sets out what must be done by the controller of the file, as soon as he finishes the processing of personal data: to destroy them, to transmit them to another person in charge or to be stored separately.

4.3.13 Luxembourg

The first existing regulation on data protection in Luxembourg were the Law of March 31, 1979 (Act Regulating the Use of National Data in Data Processing), which has undergone several modifications and the Grand Ducal Regulation of August 2, 1979, on the Council of State created by article 30 of the law of March 31.

At the moment, the present law in force came into effect in 2002.

4.3.13.1 Main aspects

The law protects the fundamental rights and freedoms of individuals, especially in their private lives, in relation to their personal data processing.

In conformity with the definition of “Processing of personal data” set out article 2, the law applies to the automatic and non automatic processing of personal data.

As we can see, a clear trend can be observed regarding the faithful transposition of regulation on data protection established by Directive 95/46.

4.3.14 Portugal

The first Portuguese law on data protection is dated April 9th, 1991 (Law 10/91). Currently, the Law in force is Law 67/98 of October 26 (Lei da Proteccao de Dados Pessoais).

4.3.14.1 Main aspects

The general principle of this law is set out in its article 2: personal data processing must be carried out in an open way and have respect for private life, rights, freedoms and fundamental guarantees.

This law does not introduce innovations regarding the principles and obligations imposed by the Directive 95/46, which are: data quality; the need to obtain, generally, the consent of the data subject to be able to process his personal data; special conditions for the processing sensitive data; the regulation of the interconnection of data; the rights of the data subjects; duty of information; security measures; the processing of personal data by third entities; international data transfers; codes of conduct; etc.

The controlling authority in Portugal is called the Proteccao's Comissao Nacional de Dados, also known as CNPD.

4.3.15 Sweden

The first Swedish law on data protection was the Law 1973/289 that was later modified in 1989.

At present, the law in force is the Personal Data Act (1998/204).

4.3.15.1 Main aspects

The scope of this law is to protect individuals against the violation of their personal integrity by the processing of personal data.

As with the rest of the national regulations which have been considered, this protection is ensured by a series of principles and obligations which should be adopted by those who process personal data.

This Law establishes a few essential requirements to bear in mind regarding any personal data processing: The legitimacy of the processing; clear determination of the purposes of the processing; the need for adequate, necessary, pertinent and accurate information; general obligation to obtain the consent of the data subject (except in some cases considered as exceptions); special measures to be adopted in the processing of sensitive information; duty of information; regulation of processing carried out by a third party, etc.

5. PRACTICAL PROBLEMS

Having analyzed the current data protection legislation adopted by the Member States, there follows in this section, an explanation of some of the practical problems with implications for data protection regarding the implementation of IPv6.

5.1 New Processing of Personal Data as Consequence of the Use of IPv6

The IP address may be considered as personal data if the possibility exists of relating that IP address (based on the Unique Identifier which may be part of it) to the interface of the terminal accessing to the Net and, in consequence, if there may also exist the possibility of relating that data to the user or owner of that IP.

This fact has two consequences that, necessarily, would have to be regulated:

- The consequences derived from the obtaining and processing of the IP address based on a Unique Identifier, as personal data itself.
- The new processing of information that could be generated as consequence of the possibility of associating certain information (which until now it was in general perceived as anonymous), different from the IP address itself, with a certain individual. For example, with IP addresses assigned dynamically by an Internet access provider and used with the current Protocol, version 4 a user whenever he was accessing the Net was doing it with a different IP each time he was accessing. In each session, he might access a specific web page where a series of personal data could be requested to him, with the purpose of knowing what type of users access the above mentioned web page, for example, his age and sex.

  In this case, if the user was not providing his name and surname and if the web page did not have mechanisms of tracing, cookies, sniffing software, etc., normally, the above mentioned information would be anonymous. At most, the owner of the web page would be able to associate this information to a specific IP address, which could change every time the user changes his connection to the Net.

  On the other hand, is important to say that still many access providers provide static addresses to the users, and in general because the need of lawful interception and logging of transactions, there is not a real situation of anonymous connection.

On the other hand, with IPv6 this information would be associated with a certain IP based on a Unique Identifier, which would identify automatically the interface of the terminal and, potentially, the concrete user of that IP.

For this reason, the implementation of IPv6 means that both cases imply a processing of new personal data and, therefore, there are new obligations to be complied with by the involved agents that process those personal data.

Is important to remind the importance on this regards of RFC 3041, as explained in section 6, which provides, when used, a further degree of privacy, not available with IPv4.

5.2 Obtaining Information about IP Addresses by the Processing Agents

One of the examples in which the IP address is considered to be personal data, is when its processing is done by the Internet access providers or by the telecommunications companies.

In this way, these agents enter into a contract with the users of their services. In general, as a consequence of these contracts, these agents could include in their files the IP addresses of their users, other types of information that could be requested in these contracts, such as their names, addresses or bank accounts.

Similarly, these agents could be able to register the date of access to the Net, the time and the duration of the connection.

For this reason, it is important to confirm that, in this case, the contract becomes the link across which the provider associates the IP address with its holder, which brings in a series of obligations on data protection for these providers such as: his consideration as the controller of the files created with this information as consequence of its processing and storage, the obligation to notify and register those files to his national authority on data protection, as well as the fulfillment of the rest of obligations that have been outlined previously in this Deliverable.

5.3 Means to Consider an IP Address as Personal Data

5.3.1 The use of public guides or directories

There are some assumptions for which, potentially, an agent could provide the requested service without needing to know the identity of the user who is behind a certain IP address.

In these cases, although the agent, provider of the above mentioned service, holds the information about this IP address, if he does not have the possibility, by any means, of connecting this information with any other concerning its holder, there would not be a personal data processing and, therefore, this processing would not be governed by this regulation, since the mere information of an IP address would not identify the concrete natural person, holder of the IP address.

Though these arguments are valid enough from a theoretical perspective, let's imagine that, as they exist nowadays for landline telephony, for IPv6, public guides or lists have been created in the style of the Whois Database (accessible to everybody) in which there were set out the names and surnames of the users together with the part of the Unique Identifier that would compose their IP addresses and to which there could have access any agent, for example, holders of web pages or of commercial establishments on the Internet.

The mere fact that there exists the possibility of a third party comparing an IP address with a list and getting to know who the holder is would, automatically, turn this Unique Identifier of an IP address into personal data.

In this case, it is important to highlight that this possibility is related to the creation of public directories containing the Unique Identifier of the different IP Addresses, linked to their holder and not the whole IP address, because there are cases regarding mobile terminals or nodes in which their IP addresses will never be totally the same because some parts of them would change depending on the point at which the connection to the Net is made. On the other hand, those terminals or nodes without mobility that access the Net always using the same point of connection will have the same IP address.

Next, we will be set out a series of considerations regarding the creation of public guides, bearing in mind, among other facts, the considerations established in the Directive 2002/58. In this respect, it is important to state that the provisions of this Directive relating to subscriber guides are directly focused on the directories generated for telephony, by which it is possible to associate a certain person to his phone number.

In this respect, apart from the differences that this type of public phone directory could have in comparison with those that could be created for IP addresses based on a Unique Identifier, in this section a brief analysis will be made of the regulations offered by the abovementioned Directive regarding this type of public guide.

5.3.1.1 Nature of public directories

One of the first differences that might arise in relation to the type of guides regulated by this Directive is based on the specific nature of the guides or IP address directories that may be produced.

Specifically, the extraterritorial character of the Internet would strongly associate these directories with this extraterritorial nature. Therefore, it could be asked whether there would be a single directory used world wide or, on the other hand, these guides will have a European or national nature. In this respect, it would become important to ascertain the current system of assignment of IP addresses and, initially, it seems likely it will not suffer substantial changes caused because of the use of IPv6, then perhaps this kind of directory could have a world wide nature.

For this reason, the IP guides which are created might have similarities to certain types of currently used guides, which allow us to carry out enquiries using the Internet and to know, for example, from the domain name of an authority, entity or natural person, who has registered it or its DNS server, amongst other information.

In other ways, these guides allow a reverse association, that is, through an IP address, it is possible to recognize what person or entity has registered that identified domain name.

Finally, among the problems derived from the nature of these public directories, another matter that should be born in mind, is the fact that if the production of these directories would be carried out under a system of free and open competition or, on the contrary, it may be decided that their creation should be performed by only one body that would be in charge of its management, its updating and processing, in compliance with what it is required under the data protection regulation.

5.3.1.2 Incorporation of information in the public directories

Firstly, Directive 2002/58/EC is the data protection regulation that sets out the regulation of public guides which, though it does not try to regulate the IP directories who might be generated in the future, it ought to be taken into consideration in this present analysis.

After analyzing the method of incorporation of information into these guides which is established in the Directive, it could be deduced that this simply enables the data subject to decide if he wishes or not to be included in these directories. For this, there could exist two different ways to proceed to incorporate his information in the directories:

- Automatic incorporation of the information in the guide, complying with the duty of information and obtaining of proper consent, so that if the user does not want to appear in the same one, he must request to be taken out of the directory or,
- Specific request of incorporation in the directory received from the user.

5.3.1.3 Some assumptions to be regulated

The creation of this type of directory would suppose the generation of a series of cases that have to be regulated according to the data protection legislation. These cases, likewise, would be influenced by the system of allotment of IP addresses and, therefore, by the entities empowered to create lists with the users and their respective IP addresses (the Unique Identifier part of the IP´s).

Another important matter would be the way of adding to and updating these guides that, in occasions, would be based on the transmission of the information to be included in them, from the agents with the capacity to allocate IP addresses to the users, to the entity or entities in charge of their production.

Likewise, there should be regulation of the position of this entity or entities and the ownership of the files generated from the creation of these guides.

Specifically, who would be considered the controller of the data contained in these guides: The entity or entities that generate them or the operators or providers who obtain such information and supply it to that entity/entities?. This will be one of the questions for debate in the event that these guides are adopted. This question is not a trivial one because depending on what entity or entities would be considered as the controller of such files, it would be possible to know which of them will have to comply with the duties of information, obtaining of the consent for the incorporation of the information in the guides, etc.

Similarly, if it were decided that these managing entities should not be created but the agents who process this information and allocate IP addresses are enabled to produce their own directories, it would be them who, in any event, should inform the data subjects about the incorporation of their personal data in the abovementioned directories, the purposes of the processing of their data, as well as complying with the remaining matters such as the obtaining of consent, etc.

On the other hand, there should also be data protection obligations in existence for other agents who use and process the information contained in these directories. That is, for example, those agents that, though they would not take part in the production and/or updating of the information contained in the guides, may use them to associate IP addresses based on a Unique Identifier with a certain user, or holder of the concrete IP.

5.3.1.4 The use of Reverse Directories

The revolution in new technologies and the digitalization of information has enabled the development of new possibilities for accessing the information contained in public directories, which make it easier to associate personal information with other types of information.

In this regard, there are some types of directories which make it possible to search for information in a reverse way. In this way, there are reverse directories or multi-criteria directories that enable us, by means of a phone number, to obtain personal information about its holder (name and surnames, address, etc.). Another example are the guides, generally consulted in the Internet, which enable us to obtain certain information about the entity or natural person who has registered a domain name, by the simple provision of that domain name.

Because of the similarity of this type of guide with the ones that should be created in the near future regarding IP addresses (through the IP one might obtain information about its holder), it would be important to bear in mind the following considerations.

These practices of reverse searching have originated and given rise to important concerns, at least, regarding the use of reverse phone directories, based on the possibility of invading the right to privacy and data protection which belongs to the data subjects. This concern has produced that some domestic legislation, especially telecommunications regulations, which have resulted in the prohibition of their use or have set down a series of requirements for their creation, on the basis of the recommendations carried out by the Opinion 5/2000 on the Use of public directories for reverse or Multi-Criteria Searching Services, adopted on July 13, 2000 by the Article 29 Data Protection Working Party.

This Opinion admits that, in many cases, this type of directory can be contrary to the privacy of the users, because it is understood that use of these public guides based on the purpose of verifying personal information concerning the holder of the phone number, constitutes a totally different use from the one which motivated the data subject to give his consent to provide his personal data for use in a public directory.

Nevertheless, it states that, in other situations, they could be useful and, therefore, they should not always be prohibited, but it is necessary to adopt all the measures set down in the Directive 95/46 to enable the regulation of: Duty of information and obtaining of consent from the data subject, among other obligations.

Therefore, it is important to take these points into account and bear in mind the differences outlined above between reverse phone directories and those which might be created in relation to IP addresses. Therefore, it is possible to conclude that, although the general rule is the option of not producing and using these directories, in the cases in which they could be considered to be really useful, it would be necessary to comply with all the existing principles and obligations on data protection, specially, the duty of information and obtaining of the consent of the data subjects for the inclusion in the guide of their personal data and their subsequent processing in conformity with the established purposes.

5.3.2 Contracting of services

Although the creation of public guides with lists of IP addresses is one of the methods used to relate an IP to his holder, there are other ways that could be used to associate this type of information with its holder and, therefore, that could turn this type of data into personal data.

For certain agents, when the user is contracting a service, it is a fundamental requirement to obtain the IP address based on the Unique Identifier to be able to provide the service correctly. For example, let us think about an Internet access provider. In this case, this agent would associate an IP address with its holder through the contract.

Another example, regards the possibility that household appliances could incorporate IP addresses based on a Unique Identifier. This raises the possibility that, for example, supermarkets could begin to provide some services based on sending the products which were demanded by a fridge, as soon as it had detected the lack of the product.

In such cases, it could be the case that the provider of this service could need to associate the IP address with, at least, the address to which it must send the ordered product and, therefore, with its holder who will have to pay for the service.

In these cases, the normal method of obtaining this information would be from signing the contract with the user.

For this reason, in relation to the providers of these services, it could be understood that the information of the IP address would be considered as personal data since the association of the IP address with its holder, would be achieved by these providers through the contract entered into by them.

In this case, the contract is the most suitable means to be used by this kind of service providers or agents to comply their information duties as well as the obtaining of the data subject's consent to process their personal data.

5.4 Possibility of Maintaining IP Addresses based on an Unique Identifier

Another legal problem that might arise is based on who or what entity will be in charge of allocating these types of IP addresses and, likewise, in case they are granted by the Internet access providers or by the telecommunications companies, if those IP addresses are intended to be the same for every user or they would be changed, instead, when a user changes his access provider or telecommunications company.

The fact that these addresses would not be considered "permanent" for each of the users could bring about the need to carry out certain relevant activities, which should be regulated.

For example, the obligation to update the public directories that might be generated and the requirement that access providers, telecommunications companies and any other agent that processes this kind of data, communicates any modifications undertaken regarding these IP addresses.

In these cases, it would be useful to develop some regulations that help to determine the criteria to be born in mind relating to the processing of this information, in conformity with the data protection legislation then in force.

5.5 Possibility of Tracing the User's Activities

One of the main problems that have been detected with regard to the implementation of the IP addresses based on a Unique Identifier, is the fact that it is possible to trace the activities being carried out by the user connected to the Net (which already was possible in the version 4 of the Protocol by using cookies or spy programs), but the innovation is based on the fact that the results of the tracing can be associated to a given interface in a terminal and, potentially, to its holder.

Normally, the users are unaware that while they are surfing the Net, typing an URL or downloading something, their browser will systematically transmit their IP address based in a Unique Identifier. In these cases, their personal data could be collected and further processed for purposes that are unknown to them.

Since one of the principal features of the regulations we have analyzed is that the processing of personal data must be carried out with some guarantees for the data subject, this possibility allowed by IPv6 favors new types of personal data processing that, till now, did not need to be regulated.

For example, an eavesdropper would be able to link this information with its holder, being able to find out, for example, the places or web pages visited by the user, his connection and disconnection hours, the products or services acquired, the purchases carried out, for example, through the requests effected to the supermarket by his fridge, and even, the location of the terminal from which the corresponding communications are being carried out.

Nevertheless, analyzing these cases from another perspective, may be less alarmist, it is possible to realize that at the moment in which a user obtains a certain IP address based on a Unique Identifier, he should begin to be conscious of the possibility that this type of processing can be carried out with his personal data and, also, he might be informed of this by the different agents that are going to process his data. As a result, these agents must be obliged to provide the users with some technical measures that guarantee the preservation of their privacy while accessing and surfing the Net (i.e. RFC 3041).

In this respect, the Common Position regarding Online profiles on the Internet adopted at the 27th meeting of the Working Group on 4/5 May, 2000 in Rethymnon, Crete, establishes for Internet service providers the obligation to notify users, in any case, the type, scope, place, duration of storage and purposes of collection, processing and use of their data for profiling purposes.

Also, this obligation to inform must be complied with even in the case of data being collected using pseudonymous.

5.6 What Means can exist to Comply with the Duty of Information by the Personal Data Processing Agencies?

In some senses, it could be stated that IPv6 does not introduce different problems for the compliance with the duty of information by the agents, which process personal data that did not exist with previous versions of the Protocol.

In the cases in which a contract is entered into by the user and the agent or provider which tries to keep his IP address for certain processing purposes, an informative clause should be included in the aforementioned contract.

On the other hand, if the above mentioned obtaining and processing of personal data is affected through the use of any service provided in the Internet, by using any terminal or device connected to the Net, the agent or provider who processes this data must include the informative clause in each of the accesses web pages.

In this respect, it is important to highlight that if a certain agent had informed the holder of the IP address about each one of the aspects determined by the Directive regarding the information duties, included the purposes of the processing of his personal data, in case that at a later date, he decides to process them for different or new purposes, he would have to inform the data subjects, once again, of this intention as well as to obtain their due consent (tacit in a few occasions and express in others) for the processing of the data according to these new purposes.

In short, as regards the fulfillment of this obligation, as well as some of the others contained in the current legislation on data protection, there are no specifics concerning the way to comply this obligation. Maybe, the main change derived from the implementation of IPv6 relates to the fact that there will be more agents who must comply their information duties because, with IPv6, more information might be considered as personal data.

5.7 Mobility in IPv6

The term “mobility in IPv6” refers to all those mobile devices that have the possibility of being connected to the Net by different points, so it seems that they are “moving along the Net” (i.e. laptops, mobile phones, PDA's, etc).

It is a question of asking whether any device can be connected to one point or another of the Net without losing its IP address. Therefore, mobileIPv6 allows a mobile node to move from one link to another without changing the mobile node's IP address.

Let's think about an executive’s laptop, which can be connected to the Net from his office, house, from the hotel where he stays, etc.

For this type of device, it could be questioned whether their IP addresses, based in IPv6, contain the part of the Unique Identifier and, therefore, if the possibility exists of identifying these devices and, potentially, their holders.

In this case, if it is possible that this type of IP´s is given to mobile devices, how is it then possible to identify them if these devices can be connected to the Net from different physical places, bearing in mind that when these devices move along the Net, they generate new IP addresses as consequence of their new point of connection.

Nevertheless, it is important to highlight that although a part of their IP address is being modified depending on the connection point, the Unique Identifier contained in the IP address, does not suffer any modifications. Thus, it is possible to identify these devices.

However, this possibility raises problems beyond the mere identification of the user, as, for example, the possibility of knowing, with enough wisdom, its geographical location.

In this respect, it will be necessary to be aware of what it is considered in section 4.2.4 of this Deliverable. Nevertheless, IPv6 doesn’t introduce, in this aspect, new threats, compared with IPv4.

5.8 IPv6 in Household Appliances

One of the areas where the advances achieved during recent years by Home Automation, is in household appliances. In this respect, Home Automation has come to be defined as *"the simultaneous use of the electricity, electronics and computer science, applied to the technical management of the home"*.

In particular, some of the aims pursued by these advances are:

- Energetic Saving: Temperature control, lighting, consumption, etc.
- Security: Custody and intrusion alertness, floods, fire, gas leaks, personal safety, etc.
- Communications: Access to Internet, internal communications, computer resources sharing in a home.
- Comfort: Heating programming, automatic watering, etc.

Home Automation uses a multitude of devices that can be distributed around the entire home depending on the needs of the owners. Basically these devices can be sensors with sufficient capacity to implement a "home area network".

With regard to the present study, it is interesting to be aware of the possible implications concerning the use of the protocol IPv6, in household appliances.

For example, in the event that each one of the different devices in a house has their own IP address with a Unique Identifier, used to access the Net, the agents who have the possibility of gaining access to the results of the surfing or access undertaken with those IP´s, might obtain valuable information such as the profiles of consumption of the house holders, their routines, their preferences, etc.

Similarly, this possibility could be increased if there was the possibility that all the devices in a house had the same prefix in their IP address, serving as a constant identifier.

Nevertheless, from the point of view of the data protection, it is important to highlight that:

- The creation of profiles, without the obtaining of the data subject's consent, is a problem that has existed with previous versions of the Internet Protocol and, therefore, it is not a problem caused by the use of IPv6.
- It is not easy for one agent or provider to access these IP's or to group all those in a house, to obtain profiles.
- The creation of profiles is lawful if it is carried out with the fulfillment of the measures contained in the Directive and in the domestic legislation adopted by the Member States regarding data protection.
- One IP address that is considered as personal data by a particular agent or service provider may not always be considered personal data by a different one.

5.9 Security Measures to be Adopted in the Processing of IP Addresses

The various Directives in force on Data Protection oblige the controllers (persons in charge of the personal data processing) to adopt technical and organizational measures that, besides guaranteeing the confidentiality of the information and its correct processing, bring about security.

In this respect, none of those Directives set out an approximate set of safety measures to be adopted by the Member States, which means that, sometimes, these States have their own legal regulations but with different contents.

With regard to the implementation of safety measures, it is important to highlight that the new Protocol IPv6 includes a security protocol called IPSec through which it guarantees, among other matters, the following:

- Authentication of the origin of the information and, therefore, the possibility of not receiving communications sent by users which are identified by a certain IP.
- Integrity of the information transmitted.
- Confidentiality of the information.

In conclusion, it is important to say that the matters raised by this security protocol IPSec will be analyzed in the Euro6IX Deliverable 4.8, because of the implications that its adoption could have in the struggle against piracy and in the defense of intellectual property rights, copyrights, etc.

6. THE USE OF RFC 3041

6.1 Brief Explanation of How it Operates

RFC 3041 "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" is a technical proposed standard that is considered to be, at present, a technical solution to the possible risks that, with regard to the privacy and data protection, might exist as consequence of the use of the new Protocol IPv6.

As it was explained in the previous Deliverable 4.2, this RFC establishes a system of two addresses used by the terminal equipment: An address which is used for entering communications, so the terminal is always reachable using its permanent address; and another one, generated on a pseudo random basis, used by the terminal for outgoing communications. Hereby, through RFC 3041, in general terms, when the communications are generated by the user who is responsible for the connection, his IP address would not be traceable by a non authorized third party (eavesdropper).

6.2 Implications of its Adoption from the Data Protection Point of View

If the adoption of this standard could prevent certain agents from discovering the Unique Identifier of a certain IP address, at first, it could be stated that this address could not be associated with a certain device by the agent, and, therefore, with a concrete user. Likewise, it would not be possible for him to trace its movements along the Net.

As a consequence, for this agent, this IP address could not have the consideration of personal data and, therefore, they would not have to comply with the obligations imposed by data protection regulation since, in these circumstances, the above mentioned information would be considered as anonymous information.

These assertions will be valid, in case the above mentioned agent does not have alternative means to be able to identify the device to which the above mentioned IP address is linked.

On the other hand, in spite of the use of this measure, by necessity, other agents will have to still know the real IP address that contains the Unique Identifier, for example, to provide their services. Therefore, they will continue to be obliged by the obligations imposed by the data protection regulation.

Though this technical measure would be applicable to the majority of the situations, it has been determined that RFC 3041 is not applicable to mobile IP's. In these cases, the different agents would continue to be obliged because of this type of IP's.

6.3 The Use of RFC 3041 by the Manufacturers of Hardware and Software

Following the recommendations made by Article of 29 Working Party, the manufacturers will have to adopt the necessary technical measures, required at all times, which guarantee the privacy of the users.

Likewise, Directive 2002/58/CE, in its Preliminary Consideration Number 46 establishes that *"it may therefore be necessary to adopt measures requiring manufacturers of certain types of equipments used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected"*.

In this respect, it is recommended that manufacturers (software and hardware manufacturers), enable users to use this type of device or, on the other hand, of accessing the Net avoiding them. In this way, they should inform the users, by way of standardized informative clauses, about the possibilities afforded by these mechanisms and the consequences of their use.

In this sense, in spite of the possible technical difficulties that could exist for their implementation, there would be several different possibilities for these manufacturers in adopting them:

- OPT OUT: According to this system all manufacturers must incorporate in the elements which form part of the hardware or software elements that they produce, devices of this nature based on the RFC 3041 or on any other standard of this nature. If the user does not want to use this type of tool, he should request its "deactivation" by his manufacturer or corresponding provider.
- OPT IN: On the other hand, this new method would suppose that manufacturers would not include, in a general way, this type of tool in hardware or software elements that they generate but, on the other hand, they would remain obliged to give the option to the users to acquire them, informing them about the way to use them and about the consequences of their use.
- Intermediate System: Through this system, the manufacturers will be able to give the possibility to the users of their products to activate or deactivate this technical solution, depending on whether they wish to access anonymously or not.

  This third option appears, at first, as the most suitable one since, in certain situations, it will be necessary for the user to access with a recognizable IP.

6.4 Other Relevant Considerations

The implementation of IP addresses based on Unique Identifiers has given rise to certain opinions regarding the fact that, in addition to the implications of its implementation on the users´ right to privacy, the use of this kind of IP´s could be contradictory in relation to one of the principal characteristics of Internet: i.e. its anonymous character.

For this reason, the development of technical measures based on the RFC 3041 probably will have a good reception in certain sectors. Nevertheless, some doubts have appeared regarding its utilization, for example, the fact that these measures may cause the obstruction of judicial or police investigations relating to the commission of criminal or unlawful activities.

Therefore, it would be appropriate to determine which agents or bodies on the Internet, for example, access providers, would continue to have the possibility of identifying a certain IP address from its Unique Identifier, in spite of the use that could be made by a user of the technical measures mentioned above, in protection of his anonymity. This point is specially relevant because this possibility would turn this type of agent or body into the main means of collaborating with the relevant authorities in the pursuit of criminal and unlawful activities committed while using Internet.

7. THE PROBLEM OF THE EXTRATERRITORIALITY

7.1 Some Problematic Cases

In many cases, it may be difficult to determine what legislation, in this case, on data protection, would be applicable to certain data processing, principally, when these are carried out in the Internet.

One example of this problem could be the following: a web page located in a certain Member State (for example, France) through which, information is obtained by its Internet users from any country of the world and whose holder and, therefore, person in charge or controller of such files, is an entity whose nationality belongs to one of the Members States, for example, Spain.

The mere storage of information is considered as personal data processing. Therefore, in the described situation, there would be two agents who are processing personal data, so two different sets of regulations exist which might be applied to this processing.

Whilst this situation would give rise to problems regarding the determination of the applicable regulation, in any case, the physical and legal safety of the obtained information would not be in danger, because both States (France and Spain) have their own data protection legislation based on the Directive 95/46.

Now let's think about a new situation that could give rise to major complications. The web page is located or hosted in France but the holder of the web page and person in charge of such information belongs to a State that has not adopted any regulation on data protection. How could this information be protected?

7.2 General Aspects to be Considered

It could be noted that this problem happens not only because of the implementation of IPv6. On the contrary, it is an intrinsic problem for the Internet.

Although it is clearly tremendously difficult to adopt, around the world, a single set of legislation which tries to solve this problem, at least from the perspective of the European Union, it would be necessary to continue with the current plan of action, characterized by the desire to create and form a common, clear, strict but at the same time flexible set of regulations, that enables the resolution the major problems that arise from the processing of personal data, as well as to increase the agreements with different foreign States not included in the EU concerning these matters, focused on the previous education and awareness on data protection.

Thus, Member States and those with recognized levels on data protection, will have to, gradually, adapt their regulations to the legal initiatives adopted, as an answer to the new problems which have arisen in relation to personal data processing.

7.3 The Power of Self-Regulation

Nowadays one of the principal methods being adopted on the Internet (among other sectors of activity) trying to lessen the effect of the lack of specific regulation on certain topics, is the self-regulation or the adhesion to codes of conduct produced by different sectors, through which have been generated a series of procedures or "good practices" that govern the activities of the members of this sector adhering to the code until a specific regulation is provided.

According to this idea, the Preliminary Consideration Number 61 of the Directive 95/46 establishes that*: "Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concern to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation".*

As it could be expected, although this option appears useful, there is a problem and it is that the abovementioned codes do not bind those agents who do not adhere voluntarily to them.

Some of the matters that should be contemplated in the Codes alluded to and whose adoption by the different agents would be suitable, would be, among others, the following:

- Prohibition of processing personal data (including IP addresses) for different purposes from those which are necessary to provide the services contracted by the users (i.e. provision of access to the Net; providing of some concrete services, etc.).
- Obtaining the users consent by using some standard clauses set out in the above mentioned Codes. This consent must be obtained by the agents, which are going to process personal data with different purposes from those which the user was previously informed of at the moment of the introduction to the services to be contracted (i.e. profiling of the user by tracing his movement on the Net).
- Obtaining the users consent to enable the agents to forward their personal information to third entities (i.e. to obtain their consent to be able to transmit their IP address to an entity in charge of the management of public guides or directories or to send the above mentioned information to companies dedicated to the production of advanced users profiles, etc).
- The setting out of a series of security measures that should be applied by virtue of the different types of information that these agents could process in their daily activity, giving a guarantee in relation to the confidentiality and integrity of this information.

  In this respect, the Directive 95/46 already establishes this need in its Preliminary Consideration Number 46 when sets out: "*Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected".*

Finally, it is necessary to emphasize that it would be suitable that these types of codes are adopted by the providers of technical solutions for hardware and software elements, in order to assure the confidentiality of the personal data and the privacy of the users. Thus, the abovementioned providers would remain informed about certain practices that they should develop with the purpose of protecting the user's rights to privacy and data protection.

For example, one of the main points to include in such codes, would be the obligation to inform the users of the existence of these technical measures and of the consequences of their adoption or of the lack of their adoption in relation to the protection of the above mentioned rights.

8. SUMMARY AND CONCLUSIONS

This section sets out the principal conclusions of this study regarding the implications on data protection of the implementation and use of the new Protocol IPv6:

1. The standardization of the implications on data protection resulting from the implementation and use of IPv6 must be a top priority, so that the different entities, authorities and citizens, increasingly conscious of their rights and obligations on this matter, can have total confidence in the safety of this Protocol in connection the processing of personal data.

2. Data protection refers to the legal protection of individuals concerning the automatic processing of their own personal data. In this respect, personal data is considered as any information relating to an identified or identifiable natural person. Therefore, an IP address would be personal data if it is possible to associate it to a certain natural person, direct or indirectly.

3. Using IPv6, the IP addresses based on a Unique Identifier allow the association of these IP´s with the nodes or devices that are using them. Then, if it is possible that an agent associates it with its holder, by any means, for example, through the contract that a provider has entered into with this holder or by other means like the use of public guides, these IP´s will be deemed to be personal data and their processing will remain governed by this regulation.

   On the contrary, if the agent does not have the possibility of association open to him, this IP address would not be considered as personal data.

4. Directive 95/46 is the fundamental regulatory framework on data protection, through which the basic principles and obligations applicable to all personal data processing have been established. Its provisions may be considered to be directly applicable to the processing derived from the use of the Protocol IPv6 and, therefore, since the consequences of the processing of this type of data do not differ or contradict the principles, obligations and rights stipulated in this Directive, it should be concluded that, at first, it would not be necessary to modify the Directive.

5. Directive 2002/58/CE is the community regulation that tries to standardize the specific requirements on data protection regarding the new services of electronic communications. Some of its main considerations are the following:
   - Consideration of the information related to the IP addresses as traffic data. Any processing based on different purposes other than the ones which are necessary for the conducting of communications, the billing of the service or as a proof of the performance of a commercial transaction, as a general rule, the consent of the holder (data subject) will be needed to enable this processing.
   - The Directive allows the users who originate a communication, to request the restriction of the identification of the line of origin as well as to the user who receives them, to reject those which come from non identified lines. Analogically, this practice might be applicable to IPv6, which is being done by using technical solutions based on the RFC 3041.

- The IP address can be considered as location data which enables the finding out of the geographical location of a concrete terminal or node. In this case, the possibility similarly exists of identifying the location of the user of this terminal.
- Public guides or directories are one of the means that would allow the association of a certain IP with a certain user and, therefore, that would promote the consideration of IP addresses as personal data. Nevertheless, it is important to highlight that the regulation offered by the Directive is not totally adjusted to the nature of the IP guides which might be created, since its regulation is orientated to telephone directories.

6. The implementation of IPv6 means that some processing of information that, previously, was not bound by the data protection regulation because the processing was carried out over anonymous information, now, begins to be covered by this regulation. Specifically, this processing is carried out in relation to the information of IP address itself and the one produced by the information associated with those IP addresses.

7. One of the principal problems detected with regard to the implementation of IPv6 is the possibility of tracing the activities undertaken by the user connected to the Net, for example, while he is surfing, and associating the results of the above mentioned tracing with a concrete node or device and, potentially, with its holder or person who has carried them out.

   These activities, at first, would not always be considered as unlawful. On the other hand, these kinds of processing could be lawful if they are carried out in compliance of what it is established on the current regulation.

   In this sense, the Common Position regarding online profiles on the Internet, adopted at the 27th meeting of the Working Group on 4/5 May, 2000 in Crete, establishes for the Internet service providers the obligation to inform the users about this type of processing and the obligation of obtaining their consent.

8. The activities of generation of profiles, without the previous collection of the data subject consent, are a problem that has existed with the previous versions of the IP protocol and, therefore, it could be stated that it is not a problem initiated by the use of IPv6. With regard to this, the obtaining of a profile is lawful if it is carried out in compliance to the provisions contained in Directive 95/46 and in the legislation adopted by every Member State.

9. With regard to the implementation of security measures, the new Protocol IPv6 has an option specifically dedicated to security matters named IPSec, through which it guarantees the authentication of the user in the origin of the information; the integrity of the information transmitted from this Protocol and the confidentiality of the same.

10. If the adoption of the RFC 3041 prevents certain agents from knowing the Unique Identifier of a certain IP address and preventing him from linking to the device and its holder, the information of IP address, to the above mentioned agent would not be considered as personal data and, therefore, this agent would not remain obliged to fulfill of the obligations imposed by the data protection regulation.

    It is recommended that an obligation is established for software and hardware manufacturers to give users the possibility of using devices based on this standard or, on the other hand, of accessing the Net being able to avoid them. In any case, these

manufactures should inform the users, by means of a standardized informative clause, of the possibilities afforded by these mechanisms and the consequences of their utilization.

11. The extraterritorial character of Internet raises, in many situations, problems relating to the determination as to what legislation should govern certain processing of personal information.

12. One of the principal means that are being adopted to relieve the lack of specific regulation on the Internet is self-regulation or the adhesion to codes of conduct produced by different sectors of activities. In this respect, the Directive 95/46 promotes the creation of these types of codes by the Members State, regarding the protection of personal data.

In general, could be stated that IPv6, in regards of this document, is not worst than. IPv4, more on the contrary, provides means for increasing the privacy of the users, which can't be done using IPv4.

Nevertheless, is also important to track and consider existing and future new works regarding the IPv6 implementation (i.e., draft-dupont-ipv6-rfc3041harmful-04.txt), that could imply future legislation amendments.