European Union Data Protection Law and
The Friend Finder Service in Social Networks

A thesis submitted to the Bucerius/WHU Master of Law and Business Program in partial fulfillment of the requirements for the award of the Master of Law and Business (“MLB”) Degree.

Alon Saposhnik

July 22, 2011

14,314 words (excluding footnotes)

Supervisor 1: Professor Dr. Jörn Axel Kämmerer
Supervisor 2: Dr. Felix Wittern
Table of Contents

A. INTRODUCTION .................................................................................................................................................3

1. Objectives of this Thesis .....................................................................................................................................3

2. What is a "Social Networking Site"?..................................................................................................................4

3. What are the risks associated with privacy for SNS users?............................................................................5

4. What are the main features of the "Friend Finder" service in SNS?............................................................6

5. What are the legal questions that are addressed within the Thesis that could arise with regards to the provision of the "Friend Finder" service in Social Networks?..............................................................7

6. Methodology .........................................................................................................................................................8

B. PART I – THE LEGAL FRAMEWORK OF DATA PROTECTION LAW IN THE EUROPEAN UNION...........................................................................................................................................................................8

I. The European Union and its general approach to data protection law .......................................................8

   1. EU data Protection law and the internal market ........................................................................................8

   2. Basic principles of data protection law in the EU ....................................................................................12

II. The application of EU data protection law to non-EU based entities .....................................................14

C. PART II – THE LEGAL INSTRUMENTS OF DATA PROTECTION AND THE IMPLEMENTATION OF DATA PROTECTION IN MEMBER STATES ................................................17

III. Legal instruments.............................................................................................................................................17

   1. The EU data protection directive 95/46/EC ("General Directive") ...................................................17

   2. The European directive 2002/58/EC on privacy and electronic communications and direct marketing ("e-Privacy Directive")....................................................................................................................24

   3. Overview on the implementation of the General Directive and the e-Privacy Directive in the German legal system..........................................................................................................................................28

D. PART III – THE APPLICATION OF THE GENERAL DIRECTIVE AND THE E-PRIVACY DIRECTIVE TO THE "FRIEND FINDER" SERVICE .................................................................33

IV. Application of the General Directive ...........................................................................................................33

   1. Whether an Entity is allowed to collect email addresses by using the "Friend Finder" service........33

   2. The question of the application of the EU data protection law to non-EU based entities which are processing personal data of individuals in the EU outside of the EU territory..............................................37

V. Application of the E-Privacy Directive...........................................................................................................40

E. CONCLUSION .....................................................................................................................................................44

BIBLIOGRAPHY ......................................................................................................................................................48

Appendix

• The European Data Protection Directive 95/46/EC

• European Directive 2002/58/EC on Privacy and Electronic Communications and Direct Marketing
A. INTRODUCTION

1. Objectives of this Thesis

This paper addresses the legal implications of the "Friend Finder", an online service, which is provided by Social Networking Site ("SNS"). In particular, this paper aims to examine what issues an entity engaged in operating an internet website that provides the registered users from the European Union ("EU") territory the "Friend Finder" service must adhere to in light of the provisions of the EU data protection law. An Investigation procedure opened by the local data protection authority in Hamburg, Germany, against "Facebook" (one of the largest Social Networking Sites in the world), claimed, inter alia, that the "Friend Finder" feature, allowing the site to contact individual person which are not subscribed yet to the SNS violating Germany's data protection law, raises three important legal issues concerning data protection law: Firstly, whether the SNS provider is allowed to collect personal data such as electronic mail addresses from individuals using the SNS services, and from unregistered individuals ("Friend"), and what are the limitations under EU data protection law for using such data for commercial purposes. Second, whether national data protection authorities of EU Member States have jurisdiction over global Internet entities located outside of the EU that are processing personal data of individuals inside the EU. Third, whether it should be considered as illegal marketing practice for the SNS provider to use the “Friend Finder” service to send email messages to the Friend, inviting him or her to join the SNS.

Part I provides the legal framework of data protection law in the European Union and introduces the main legal principles for processing the personal data of individuals inside the EU. In addition, part I provides a legal analysis for questions of jurisdiction and conflict of law. Part II provides a brief overview on the General Directive, and on the provisions of the e-privacy Directive. In addition, part II provides an overview on the implementation of the


General Directive and the e-Privacy Directive in the German legal system. Part III analyses the EU data protection law provisions, which are applicable to the use of the "Friend Finder" service. The last part of this Master's Thesis concludes that SNS providers using the "Friend Finder" service in a social networking sites for commercial purposes, are held fully reliable for compliance with the EU data protection law provisions.

2. What is a "Social Networking Site"?

Social networking sites have been defined by Boyd and Elisson as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system". The main feature in SNS is an individual's ability to create a profile containing data such as age, location, interests, education and a profile photo and the ability to share the profile with a list of "Friends" who are a part of the same network. Other features like comments, private messaging, photo and video sharing services are also provided in SNS. Social networking sites popularity among Internet users is increasing at a dramatic rate and they are used worldwide. Some recent studies on the usage of social networking sites indicate that millions of individuals around the globe visit SNS each month, and that social networking sites are still experiencing extreme growth. However it is important to point out that, recent market research showed a slowing growth rate trend in the usage of social networking sites in the U.S, due to the rising sophistication of the social networking audience, the battle between email and social networks, and the increase in

---

mobile social usage. Scholars that are studying the SNS phenomena stated that the reason for the usage of SNS is the motivation for communication and maintaining relationships with "Friends" on the social network.

3. What are the risks associated with privacy for SNS users?

In a recent published report, the OECD noted that "there is a general perception that certain risks associated with privacy have increased as a result of the shift in scale and volume of personal data flows and the ability to store data indefinitely". OECD explains that one of the main risks for privacy arises because of using personal data of individuals in ways that the individual did not anticipate when the data was collected. An example of unanticipated use of personal data could be using data mining practice to analyze "the digital trails left by individuals, by mining information about preferences, interests, behaviors, or buying patterns expressed on social networking sites". Another risk for unanticipated use of personal data was described in a position paper published by the "European Network and Information Security Agency" (ENISA). The paper lists the important risks to SNS users and SNS providers, such as the download of profiles on SNS by third parties for the use of creating a digital dossier of personal data, as well as secondary data collection on the users, e.g., messages sent, other users visited, photographs, videos and more. Some research showed that SNS providers are capturing "Personally identifiable information" (e.g., Full name, telephone numbers, email address, home address, place of birth, mother's maiden name, asset information etc.), which is linkable to a specific SNS user.

---

and make it available to third parties which track and aggregate user habits, a practice which can lead to identity theft.\textsuperscript{12} Considering the high economic value of data generated by users on the Internet, it can be used for advertising, discrimination or for a transfer of data to third parties through resale for considerable financial gain.\textsuperscript{13} A report on the economic value of data generated online showed online advertising accounted for $22 Billion in spending in 2009, and is expected to increase due to the data that can be collected on consumers online, which allows companies to measure the response of a specific individual to an ad, and to learn better on consumers habits and to target ads to consumers that are likely to buy the company’s products.\textsuperscript{14} In light of the above, it is clear that many risks for privacy are associated with the use of SNS.

\textbf{4. What are the main features of the "Friend Finder" service in SNS?}

The "Friend Finder" service (also known as "Tell a Friend" service), is a method of marketing that uses a visitor of a website (e.g., a Social Networking website) to send information about a website, a product, or a service to people they know by using email or text message. An example of using this method can be found in the SNS "Facebook". "Facebook" allows the user to upload his or her email address book data to "Facebook's" server. "Facebook" processes this data and compares it with email addresses of existing "Facebook" users that are registered on its database. Registered users whose details match with "Facebook" data are displayed to the user, who is then asked to use the "Friend Finder" service to invite the registered user to become a "Friend" on the user's network. As regards to unregistered users, whose email address was supplied by providing access to the initial user's address book, the user has been asked to use the "Friend Finder" service to send email messages that were formulated by "Facebook", inviting the "Friend" to join "Facebook". If the "Friend" does not

\textsuperscript{14} Catherine Tucker, on "The Economics Value of Online Customer Data", OECD, 1 December 2010, available at, \url{http://www.oecd.org/document/22/0,3746,en_2649_34255_46565782_1_1_1_1,00.html}, last visited in 7 July 2011, p. 12.
respond to the invitation, "Facebook" continues to send emails on behalf of the registered user, reminding the "Friend" to join "Facebook" until he or she decides to join. The "Friend Finder" service covers three kinds of marketing methods: One method is where a website asks a user to provide the email address of a friend or a person he or she knows and the website sends an email offering that person a product or a service. This method uses the initial user to attract new potential SNS users as follows: "The friend receives an email that on arrival looks like it was sent by the person making the recommendation in order that it appears to come from a trusted person". The second method allows a user to enter the email of a friend, on the website, and to send an email message, by him/herself. A third method is where the website asks a user to send an email message which recommends a service or a product to third parties. It is important to note that the "Friend Finder" service is used by SNS providers that are based outside the EU territory, to process the email address book data of individuals that located inside the EU territory.

5. What are the legal questions that are addressed within the Thesis that could arise with regards to the provision of the "Friend Finder" service in Social Networks?

1. Whether the SNS provider is allowed to collect personal data such as email addresses, from individuals using the SNS services, and from unregistered users of the SNS, and what are the limitations under EU data protection law for using such data for commercial purposes.

2. Whether national data protection authorities in the EU have jurisdiction over global internet entities situated outside of the EU territory which involved in processing personal data of individuals in the EU outside of the EU territory.

3. Whether it should be considered as illegal marketing practice for the SNS provider to use the “Friend Finder” service for sending email messages to the Friend, inviting him or her to join the SNS.

---

These legal questions will be discussed in the Thesis and a possible answer for each question will be suggested.

6. Methodology
The method used in the Thesis to answer the legal questions is discussing and making a legal analysis of the specific provisions which may be applicable to the case. Case law, relevant literature, articles, and specifically The Article 29 Working Party ("The Art. 29 WP") guidelines, as well as sources from the internet will be used to describe the application of EU data protection law to online services such as the "Friend Finder" service.

B. PART I – THE LEGAL FRAMEWORK OF DATA PROTECTION LAW IN THE EUROPEAN UNION

I. The European Union and its general approach to data protection law

1. EU data Protection law and the internal market
The basic treaties that have been established the EU are the Treaty On European Union16 ("TEU"), and the Treaty On The Functioning Of The European Union17 ("TFEU"), and they are the primary sources of the community law. Article 47 of the TEU states that the EU "shall have legal personality". Based on this Article, the European Court Of Justice ("ECJ") on one of its earliest cases recognized the EU has an international legal personality.18 The EU international capacity is governed by public international law and it allows the EU, inter alia, to conclude treaties, to submit claims or to act before an international court and to become party of international conventions.19 The division of powers between the EU and the Members States is governed by community law. The ECJ, on decision given in the Costa v. ENEL case, sets out the basis for the supremacy of community law over Member States national law by stating, that the community law created a new independent legal order which

18 See ECJ, Case C-22/70, Commission v. Council (AETR/ERTA), ECR 1971, 263, Par. 14.
became an integral part of the Member States legal systems, which the courts are bound to apply. Given the EU powers and the supremacy of the community law, the EU may act only when there is a legal basis for action provided in the community law treaties. The legal basis of the EU competence to legislate with regards to data protection is based on Article 100a of the Treaty Of Rome (currently Article 114 of the TFEU). Article 114 of the TFEU grants the EU parliament and the Council the power to legislate and take administration measures, which aim to ensure the establishment and functioning of the internal market. The internal market is one of the EU main policies. According to Article 26 of the TFEU, the internal market aims to achieve: "an area without internal frontiers in which the free movement of goods, person, services and capital is ensured". In the Passenger Name Records ("PNR") case, the ECJ ruled that the Council's decision to conclude agreement with the U.S on the processing and transfer of PNR data, and that a decision adopted by the Commission determining that the US customs authorities provided an adequate level of data protection to the PNR under the General Directive falls outside the EU competence. Hence, the ECJ has considered both acts invalid. It is important to note that the competence to legislate the e-Privacy Directive was based also on Article 95 of the Amsterdam Treaty (currently Article 114 of the TFEU). In addition to community law, data protection law is based on human rights such as the right for privacy and the right to the protection of personal data. Thus, the right to the protection of personal data is regarded as a fundamental human right in Article 8 of the Charter of Fundamental Rights of the European Union, which was given binding legal status by Article 6(2) of the TEU.

20 See ECJ, Case C-6/64 Flaminio Costa v. ENEL, CMLR 1964, 585, 593.
states that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. The "Charter" also grants the right of access to data that has been collected concerning the person, and the right to have it rectified, and states that compliance with these rules shall be subject to control by an independent authority.

Through the General Directive, the EU intended to achieve two main objectives: 1. The harmonization of data protection law amongst Member States, which aims to ensure the free flow of personal data between Member States which is necessary to create the internal market. 2. To protect fundamental freedoms and rights of individuals. 27 The way the General Directive seeks to accomplish harmonization of data protection was described as follows: "The Directive's goal is to promote harmonization of member states data privacy legislation and, thereby, the free flow of data. To achieve this goal the EU legislator specified a set of rules which must be implemented by the member states in their legal system "as is", and also granted member states a margin for maneuver in such implementation. According to the principle of harmonization, member states' national legislation should be based upon the compulsory rules". 28

In addition, scholars regard data as "commercial goods", which is covered by the same principles that aim to prevent barriers to the four basic freedoms of movement: "The Data Protection Directive establishes the internal market in the meaning of art. 14 of the EC Treaty with reference to the free flow of personal data among Member States, mirroring the equivalent principles that apply to goods, persons, services and capital". 29

Many EU organs are involved in the development, implementation and enforcement of data protection law. Some of them shall be discussed below:

The European Commission ("Commision") is the executive arm of the EU. In the field of EU data protection the Commision acts as the organ that is responsible to propose legislation, monitor the implementation of EU data protection legislation in the domestic

27 See Article 1 of the General Directive
laws of the Member States, and to take legal actions against Member States, public and private bodies - when legal problem arise on this topic.\textsuperscript{30}

The Council of the European Union ("Council") is the political arm of the EU. In the field of EU data protection law the Council provides a forum where Member States representatives makes decisions and exercise their political influence on matters concerning the development of EU data protection law. The Council is also involved in EU data protection law issues through the Committee that was established by Article 31 of the General Directive ("Art. 31 Committee").

The ECJ involvement in EU data protection law was described as follows: "First, a Member State or the Commission may bring an action before the Court, such as against a Member State for failing to implement an instrument of EU law. And second, a national court of an EU Member State may refer a question of EU law to the Court for interpretation". \textsuperscript{31}A few decisions the ECJ has given on issues relating to EU data protection law will be discussed below.

The Art. 29 WP was established under the General Directive as an independent advisory body comprised of representatives from Member States' data protection authorities. The Art. 29 WP responsible to issue interpretative documents and opinions, which have influence on public and private bodies as well as professionals which are dealing with data protection issues.\textsuperscript{32} It is important to note that the Art. 29 WP opinions are not binding as it is only an advisory body.

The countries which are members of the EU are affected by the EU data protection law legislation because Members States was bound to implement the General Directive and the e-Privacy Directive into their legal systems. Three more countries that are members of the European Free Trade Association ("EFTA") - Iceland, Liechtenstein and Norway – which are not members of the EU, have been ratified the General Directive and implemented the General Directive into there legal system. Therefore those EFTA countries have also been

affected by the EU data protection law legislation. Together with the EU Member State those three EFTA countries comprise the European Economic Area ("EEA").

2. Basic principles of data protection law in the EU

Several basic principles which were implemented in the General Directive exist with regards to the processing of personal data. These principles shall be presented below:

"Fair and Lawful processing" is the primary principle of data protection law. The principle was implemented in Article 6 (1) (a) of the General Directive. Lawful processing means that processing may be undertaken only if it based on legal grounds. "Fair" processing means that "the collection and further processing of personal data must not intrude unreasonably upon the data subject's privacy nor interfere unreasonably with their autonomy and integrity". According to this principle, processing should be transparent for the data subject and personal data should be collected directly from the data subject and not from third parties. This principle raises the legal question of fairness of the "Friend Finder" service, which allows the SNS provider to collect information on unregistered users which was not obtained from them directly, but from SNS users who provided access to their address book data by using the service.

The "purpose specification" principle was implemented on article 6 (1) (b) of the General directive, and means that if personal data has been collected for a certain use and subsequently used for another purpose, and the data subject could not reasonably have expected that data would be used for another purpose, a consent for the new use should be obtained by the data controller. The principle is relevant for the "Friend Finder" service when the data that user provides for the purpose of adding new "Friends" to his or her network is been used to analyze the user's address book data to recruit new SNS users or for sending them marketing massages.

The "Data subject's participation and control" principle, is a principle which enables the data subject to participate and to have influence over the processing of data on them by

---

The participation can be expressed in allowing the data subject to be aware that their personal data has been processed, or in the obligation of collecting consent from the data subject for processing their data. This principle is relevant for the "Friend Finder" service, because of the practice used by the "Friend Finder" service, to analyze the data in the address book without obtaining consent from the persons in the address book.

The "Disclosure limitation" principle is a basic principle that limits data controllers in disclosure of personal data to third parties only in place where a data subject has given consent for the disclosure. As shall be discussed below, in certain cases the "Friend Finder" service user could be regarded as a data controller and held responsible for compliance with the General Directive provisions. In light of the information included in the address book, the disclosure limitation could become relevant for the "Friend Finder" service, when the user decides to provide access to the address book to third parties without obtaining consent.

The "information security" principle is a principle that was implemented in Article 17 of the General Directive and requires a data controller which uses a data processor to process personal data behalf of him to ensure by way of contract that the sufficient security measures will be carried out by the data processor to ensure that personal data is not destroyed accidentally and not subject to unauthorized access, alteration, destruction or disclosure. This principle is relevant to the "Friend Finder" service, when the SNS provider can be considered as a controller, a duty that makes him responsible to carry out security measures.

The "Transparency" principle requires that data subject given information regarding the data processing that relate to him. This principle was implemented in the requirement to

---

36 See Article 18 of the General Directive.
give notification about the data processing methods used by the data controller.\textsuperscript{41} Such requirement is relevant to the context of the "Friend Finder" service in light of the SNS provider analysis and usage of personal data contained in individuals address book data.

It is important to note that the principles underlying the processing of personal data, have been acting as a guiding standards for data protection authorities where balance is necessary between the data subject's rights and the public interests to ensure free flow of data, as will be described below. In addition, these principles have also helped to shape the drafting of new data protection law, as will be described below.

II. The application of EU data protection law to non-EU based entities

The "Friend Finder" service is used by SNS providers such as "Facebook", that are based outside the EU territory, to process personal data of individuals located inside the EU territory. Therefore it is important to clarify some of the main jurisdictional issues and legal framework of global personal data processing.

The issue whether EU data protection law should be applicable to non-EU based entities, especially to entities hosting a website outside the EU territory, arises due to Member States Data Protection Authorities ("DPA") concern, with ensuring that personal data of EU residents are not deprived of the national data protection law once the data have been transferred to a foreign country. Therefore, the DPA may assert that the processing abroad should be conducted under their own data protection law.\textsuperscript{42}

On the other hand, the DPA assertion of jurisdiction over non EU based entities may create a jurisdictional conflict between international law and the Member State who seeks to verify that the processing of personal data outside of their borders is conducted in compliance with the law and any agreements they have concluded. Scholars argue that international law prohibits an act by one state in the territory of another state that only state officials may perform.

\textsuperscript{41} See Article 11 and 12 of the General Directive.

For example, European DPA's have sought the power to perform enforcement audits of data processors in other countries. Audits carried out by a DPA for purposes of regulatory compliance outside its own territory would seem to be a breach of international law unless the State concerned gives its consent.\(^{43}\) Scholars criticized that asserting of jurisdiction over non EU based entities by DPA of Member States in the context of data protection may increase the chance of jurisdictional conflicts, as well as the risk that respect for data protection law will be diminished due to little chance of enforcement, and therefore not necessary, especially where other ways such as "soft" penalties which could result in potential reputational damage could be used for enforcement purposes.\(^{44}\) It is worth noting that the Art. 29 WP expressed its opinion on this issue, stating that in its view the application of EU data protection law to non-EU based entities is a general question of international law.\(^{45}\) Therefore, it is necessary to see what jurisdictional and conflict of law rules the EU legislator chose to implement in regards to data protection law.

According to Article 4(1)(a) of the General Directive, the location of "establishment" triggers the applicability of a Member State data protection law. The Art. 29 WP defines "establishment" as an, "effective and real exercise of activity through stable arrangements and has to be determined in a conformity with the case law of the court of justice of the European Communities".\(^{46}\) For example, an attorney's office, a one-person office and a simple agent can be considered as an "establishment".\(^{47}\) In addition, the EU data protection law is applicable only where the processing


is carried out "in the context of activities of a data controller". The Art. 29 WP noted that the concept "in the context of the activities" means that the applicable law shall be the law of the Member State where an establishment of an entity is involved in activities relating to data processing. For example, when "establishment" of an entity processes personal data "in the context of the activities" of another "establishment", the applicable law will be the law of the Member State in which the other "establishment" is located.

The most important rule for the case of application of EU data protection law to non-EU based entities is Article 4(1)(c) of the General Directive, which according to the Art. 29 WP applies where Article 4(1)(a) does not apply. The first condition for the application of this article is that an entity has no "establishment" inside the EU territory. This article can be relevant to online services such as search engines, social networks and cloud computing. The second condition for Article 4(1)(c) to be applicable is that "equipment" is located inside a territory of a Member State. The Art. 29 WP considered the wording "equipment" as "means" used for processing of information, which can be automated or otherwise.

Article 4(1)(c) provides exception to non-EU based entities from EU Data Protection law "when the equipment used by the controller and located within the Member State is used only in order to ensure transit through Union territory". For example, the Art. 29 WP pointed out that "point to point" cable transmission used on telecommunication networks, comply with the conditions of the article 4(1)(c) exception. However, the Commission is in a position that the exception should be interpreted narrowly and that EU Data Protection law should have a broad scope, even if it

---


16
extends beyond the EU and the EEA territory, because the Commission's role to ensure that individuals inside the EU are not deprived from the protection to which they are entitled under the General Directive, and at the same time, to prevent circumvention of the law.\textsuperscript{54} In light of the Commission's opinion and the General Directive provision presented here, non-EU based entities which are involved in the processing of personal data of EU residents outside the territory could be exposed to the application of EU data protection law, as shall be analyzed in more details below.

C. PART II – THE LEGAL INSTRUMENTS OF DATA PROTECTION AND THE IMPLEMENTATION OF DATA PROTECTION IN MEMBER STATES

III. Legal instruments

1. The EU data protection directive 95/46/EC ("General Directive")

The General Directive governs the processing of personal data regardless of the processing context. The General Directive applies only when "personal data" is processed.\textsuperscript{55} The General Directive defines "personal data" as "...any information relating to an identified or identifiable natural person".\textsuperscript{56} When considering if the concept of "personal data" should apply to specific data, the objectives of the General Directive to protect the fundamental rights and freedoms of the natural person, and in particular the rights to privacy with respect to the processing of personal data have to be taken in account.\textsuperscript{57} The concept of "personal data" was criticized as very broad as it is possible to classify almost any data that could be linked to a specific individual as "personal data". The concept of personal was described in the Art. 29 WP opinion No. 4/2007,\textsuperscript{58} which noted that data should be classified as personal data when the data either contains information about a specific person ("content" element), or when the


\textsuperscript{55} See Article 3 of the General Directive.

\textsuperscript{56} See Article 2 (a) of the General Directive.

\textsuperscript{57} See Article 1 (1) of the General Directive.

data is used or likely to be used to determine the treatment of a specific person ("purpose" element), or when the data is likely to have an impact on a specific person ("result" element). To classify data as "personal data" one of the elements of content, purpose and result must exist. Even after the Art. 29 WP expressed its interpretation to the concept of "personal data", it still can be argued that the three criteria are very broad, and allow almost any type of data that can directly or indirectly linked to a person (e.g., images, telephone number, home address), to be brought under the umbrella of "personal data". For example, in the context of communication, the issue of whether an IP address can be considered as "personal data" is a subject for dispute because sometimes the IP address reveals the identity of a specific person.

Another important element relating to the classification of data as personal data, is that the person can be "identified or identifiable" by the data directly or indirectly. An example of direct identifier data is the name of a specific person, address, place of birth, DNA, etc. An indirect identifier could be data such as a telephone number, working conditions, or hobbies of a person, as has been stated by the ECJ in Lindqvist case: "referring on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number to information regarding their working conditions and hobbies, constitutes the processing of personal data...within the meaning of...Directive 95/46".

It is important to note that, where data cannot be classified as "personal data", the General Directive should not be applicable. Some more examples of data that has been considered by the U.K. DPA as "personal data" are bank account number, debit or credit details, shoe size, medical history, geographical location, passport number, and even favorite

61 See Article 2(1) of the General Directive.
63 See ECJ, Case C-101/01 Bodil Lindqvist v. Kammarklagenrenh, ECR 2003, I-12971, paragraph 27.
The concept of "personal data" is relevant to the determine whether email address data which the "Friend Finder" service collects from users, should be classified as personal data, especially where users are not obliged to use their actual name for their email address.

The actors who process personal data are called "data controllers" and "data processors". The concept of "data controller" has been defined in Article 2 (d) of the General Directive. For example, in the Bodil Lindquist case, a private person working on a voluntary basis who had published data about her colleagues on the internet has been considered as a data controller. The controller is the one who is responsible for compliance with the General Directive that imposes obligations that intend to protect the rights of data subjects. Article 6(2) of the General Directive explicitly states that the controller must ensure that personal data will be: 1. Processed fairly and lawfully; 2. Collected for specified, explicit and legitimate purposes; 3. Adequate, relevant and not excessive in relation to the purposes for which they are collected; 4. Accurate and kept up to date; 5. Kept in form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data was collected. Furthermore, the General Directive imposed obligations on data controllers as stated in Articles 10 and 11 of the General Directive that the controller must provide the data subject information about the identity of the controller, the purposes of the data processing and information on the right to access and rectify data concerning him or her. In addition, the controller is obliged to provide the data subject, an access to data, and to allow him or her the to rectify the data, erase and block the data which does not comply with the General Directive, and to object to the processing of the data. Some scholars argue


67 See article 12 of the General Directive.
that the right to block the data is problematic and disproportionate because in most cases, in order to block data the controller has to block the whole processing activity, a consequence that can cause a disproportionate damage to the controller especially where the database is used by others. Furthermore, the controller also has an obligation to notify the national data protection authority about any operation of data processing that he or she intends to carry out. Finally, the controller is liable for any damages that a person suffered as a result of an unlawful processing operation.

Article 2 (e) of the General Directive defines the concept of "processor". The distinction between the controller and the processor is that the controller is the one who controls the processing of the data and is held responsible for the compliance of the data protection laws, and the processor is the one who only responsible for processing personal data and is acting on behalf of the controller. To clarify the distinction between control to processor, it is necessary to refer to article 16 of the General Directive which states that the processor himself and any person acting under his/her authority access to personal data must not process the data except on instructions from the controller. For example, where company A outsources its mail marketing activity to company B, to carry out mail marketing campaigns on behalf of company A, and gives clear instructions such as what marketing material to send out and to whom and also provides access to the company’s mailing list in which company B is allowed to process, company A shall be considered as the data controller and company B shall be considered as data processor. It is important to note that the carrying out of the processing by way of a processor must be governed by a contract or a legal act binding the processor to the controller to act only on instructions from the controller and to implement appropriate technical and organizational measures to protect personal data against accidental

---

68 See article 14 of the General Directive.
70 See Article 18 of the General Directive.
71 See Article 23 of the General Directive.
or unlawful destruction or accidental loss, or unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network.\textsuperscript{73}

In an analysis made by the Art. 29 WP, for the concept of the "controller" and "processor", it was suggested that an essential element to distinguish the controller from the processor is the factual circumstances of the parties involved in the processing. According to the Art. 29 WP, it is necessary to understand the factual elements concerning who has the competence to determine the specific processing operations.\textsuperscript{74} The competence to determine may come from a legal provision that appoints the controller to process data or it may come from contractual relations between the parties involved in the processing.\textsuperscript{75} To qualify as a controller one also has to be able to determine the purposes of the processing of data or the means of processing, which refer to both the technical and organizational matters, such as which data shall be processed.\textsuperscript{76} An example for the relevance of the assessing the factual elements to distinguish between processor and controller can be seen in the "Society for Worldwide Interbank Financial Telecommunication" ("SWIFT") case, where the Commission had to assess SWIFT's functions in order to decide whether it should be classified as a data controller or a data processor. The Commission Opinion was as follows: "While SWIFT presents itself as a data processor, and some elements might suggest that SWIFT has acted in the past as a processor in certain cases on behalf of the financial institutions, the Working Party, having considered the effective margin of maneuver it possesses in the situations described above, is of the opinion that SWIFT is a controller."\textsuperscript{77} The opinion of the Art. 29 WP, that was presented here, could be relevant to decide if the SNS provider who offers the "Friend Finder" service shall be regarded as data

\textsuperscript{73} See Article 17 (3) of the General Directive.
controller or data processor. If the SNS provider falls into the scope of a controller, it should require from the controller to comply with all the obligations of controller set under data protection law.

As stated above, the General Directive applies to the processing of personal data, irrespective of the means used. Article 2(b) of the General Directive defines "processing" very broadly. Thus, activities such as collection, recording, organization, storage, and other uses performed on personal data could be considered processing. For example, in the Bodil Lindquist case, the ECJ considered placing information about individuals on a website as processing of personal data. Article 6 (1) of the General Directive states that personal data must be processed fairly, for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes. In Article 7 of the General Directive, it stated what could be considered as fair and legitimate processing. Thus, Member States may provide processing of data only when the data subject has unambiguously given his consent, or processing is necessary for the performance of a contract to which the data subject is a party, or processing is necessary for compliance of a legal obligation of the controller, or the processing is necessary in order to protect the vital interest of the data subject.

For the purpose of using the "Friend Finder" service, it is important to examine whether the processing of user data shall be done on legitimate grounds in compliance with the rules set by the General Directive provision. Violation of the rules may deem the "Friend Finder" service illegal, and may result in the risk of attached criminal liability, administrative fines, stop orders, civil law claims and other sanctions.

To enhance compliance with the General Directive by the controllers, Article 28(3) of the General Directive provides the local DPA, of each Member State, with investigative powers, effective powers of intervention in processing of personal data by controller and the power to

---

78 See Article 3(1) of the General Directive.
79 See ECJ, Case C-101/01 Bodil Lindqvist v. Kammaraklagarenh, ECR 2003, I-12971, paragraph 27.
80 See Article 6(1)(b) of the General Directive.
81 See Article 7(a) of the General Directive.
82 See Article 7(b) of the General Directive.
83 See Article 7(c) of the General Directive.
84 See Article 7(d) of the General Directive.
engage in legal proceedings where provisions of the General Directive have been violated and to bring these violation to court.\textsuperscript{85} The Art. 29 WP noted that the role of the DPA in enforcement of the General Directive on controllers should be narrowed to "investigations or inspections, with a view to checking compliance. This may involve the use of formal powers and may result in the imposition of sanctions, depending on the applicable national laws."\textsuperscript{86} Examples of enforcement actions carried out by local DPA's of Member States were imposing of sanctions by the local Czech Republic DPA for insufficiently obtaining consent from customers and other persons in relation with an offer for services and business,\textsuperscript{87} undertaking investigation of the Ireland DPA in relation to breaches of the SPAM regulations implementing the e-Privacy Directive,\textsuperscript{88} and enforcement actions carried out by the U.K. DPA for direct marketing and the unfair processing of personal data by private utility companies and companies sending unsolicited mail.\textsuperscript{89} In addition to the administrative enforcement action of the DPA, the General Directive provides every person the right for a judicial remedy,\textsuperscript{90} as well as the right to receive compensation from data controllers for damaging the person suffered as a result of an unlawful processing operation or violation of national legislation.\textsuperscript{91} Finally the General Directive requires that Member States shall adopt suitable measures to insure compliance with the General Directive provision including the use of sanctions.\textsuperscript{92} It is important to notice that scholars criticized that the national Member States courts and the ECJ are not involved

\textsuperscript{85} See Article 28(3) of the General Directive.
\textsuperscript{90} See Article 22 of the General Directive.
\textsuperscript{91} See Article 23 of the General Directive.
\textsuperscript{92} See Article 24 of the General Directive.
enough in interpreting and applying data protection laws, and that the absence of courts from the field is problematic for the development of data protection law.\textsuperscript{93}

2. The European directive 2002/58/EC on privacy and electronic communications and direct marketing ("e-Privacy Directive")

The e-Privacy Directive addresses the protection of privacy with respect to the processing of personal data in the electronic communication sector. Unlike the General Directive which applies to processing of personal data regardless of the processing context, the e-Privacy Directive is more specific and applies to the processing of personal data of users that are using publicly available electronic communication services such as e-mail, SMS, fax, and telephone that are provided in public communication networks in the EU.\textsuperscript{94} Another example where the e-Privacy Directive applies is Internet services. According to the Art. 29 WP opinion, the internet is a network of computers that is open to the public and belong to the telecommunication sector, therefore the protection under e-Privacy Directive applies to the processing of personal data on the internet.\textsuperscript{95} The e-Privacy Directive functions as a complement to the General Directive,\textsuperscript{96} in the sense that it applies in the electronic communication sector to all matters concerning protection of fundamental rights and freedoms that are not specifically covered by the General Directive.\textsuperscript{97} According to the e-Privacy Directive objectives, taking into consideration that the "Friend Finder" service belongs to the context of electronic communication sector, it should be covered by the e-Privacy Directive.

In addition, the e-Privacy Directive aims to harmonize the legal framework governing the use of electronic communications for the purposes of direct marketing. Article 13 of the e-Privacy Directive relates to the sending of unsolicited communications. One of the most well-
known practices for direct marketing purposes is "spamming", which has been described as follows: "Spamming is the practice of sending unsolicited e-mails, usually of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact." It is important to point out that spamming is easy and cheap for the "spammer", however, that sending Spam creates an economic impact both on the recipient of the email message and Internet Service Provider ("ISP"), due to the cost of the recipient expressed in time spent downloading and sorting unwanted messages, and the cost to the ISP, which is expressed in storing those messages in its servers until it is download by the recipient. According to the OECD report on Spam, "in addition to the cost faced by ISP, businesses would also be faced with cost to filter spam, cost associated with hiring administrators to deal with spam, and productivity and other costs associated with spam reaching end user e-mail boxes". It is important to note that, Spam could be carried out by the sender only when the sender has been collected enough email addresses. One of the ways to collect email address may be by obtaining access to a person address book data, a practice that has been carried out by the "Friend Finder" service.

Article 2(h) of the e-Privacy Directive used a broad definition to describe what can be considered as "electronic mails". Thus, any text, voice, sound or image message sent over a public communications network, such as SMTP, SMS, MMS, and newsletters sent by emails should be classified as email. Article 13(1) of the e-Privacy Directive states that the use of emails for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. The requirement to give consent to receive emails is known as the "opt-in" regime.

---


The meaning of the word "consent" is similar to the meaning that is stated in article 2(h) of the General Directive and that was discussed above.\textsuperscript{102} Consent to use email for direct marketing purposes, may be given in various ways enabling to indicate a freely given specific and informed user's willingness to receive marketing messages.\textsuperscript{103} For example, lawful consent in the context of internet website may be given by ticking a box when visiting a website. In contrast, because of the requirement that the consent shall be legitimate, explicit and specific, it can be argued that pre-ticked boxes should not be considered compatible with the definition of consent.\textsuperscript{104} The application of the obligation to receive consent before sending email messages should be relevant to the "Friend Finder" service in light of the practice used by the SNS provider to send invitations to email addresses of unregistered users that were collected from processing the user's address book data, either on behalf of the user or by the user him/herself.

Furthermore, Article 13(4) of the e-Privacy Directive imposes obligation on the sender of the email to provide his or her identity and a valid address to which the recipient may send a request that sending of e-mails cease.\textsuperscript{105} Two important notes worth mentioning: Firstly, the meaning of direct marketing cannot be found in the e-Privacy Directive, however, in the Art. 29 WP opinion, sales promotion, as well as direct marketing made by charities and political organizations may constitute direct marketing.\textsuperscript{106} Second, scholars suggest that Article 13 of the e-Privacy Directive applies to data controllers who are established outside the EU territory, as soon as they are sending unsolicited communications to persons established on the EU.\textsuperscript{107} As will


\textsuperscript{103} See Recital 17 of the e-Privacy Directive.


be discussed below, these two notes, is important to the question whether the e-Privacy Directive applies to the "Friend Finder" service or not.

Although, it may not be considered relevant to the "Friend Finder" service, it is worth noting that article 13(2) of the e-Privacy Directive provides an exception to the "opt-in" regime, in three conditions: Firstly, the email contact details must have been obtained by the sender from its customer. Second, the email data have to be obtained in the context of the sale of a product or a service. Third, the email data have to be obtained in accordance with the provision of the General Directive, requiring, inter alia, to inform the customer on the purpose of the use of the email data, as well as on the right to object such use and for fair use. Furthermore, the customer must have been given the opportunity to object free of charge to the use of e-mail data when it was collected. This exception is known as the "opt-out" regime, because unlike the "opt-in" regime, the recipient whose email data is used is not required to provide prior consent but rather shall be entitled to oppose such use in each marketing message. In addition, Article 13(5) of the e-Privacy Directive states that the protection against unsolicited communications applies to natural persons, but EU Member States shall ensure also the protection of legitimate interest of legal persons within Member States national legislation. For example, if a recipient of unsolicited communications is a company, a Member State may choose to apply the protection given under the "opt-in" or "opt-out" regime to the sender of the unsolicited communications. Scholars criticize that in practice it could be hard to implement the protection against sending unsolicited communications because it would be hard for the sender to verify whether the recipient is a natural person or a company. Finally, it is worth mentioning that the e-Privacy Directive applies the provisions of the General Directive concerning remedies, liability and sanctions to

---


110 See Article 22-24 of the General Directives.
cases of remedies demanded for an infringement of a data subject's rights derived from the e-
Privacy Directive.\textsuperscript{111}

The legal framework of sending unsolicited communication could provide many
difficulties for the practice used by the "Friend Finder" service, in fact, one of the reasons why
the DPA in Hamburg chose to open an investigation against "Facebook", was because the DPA
was in the opinion that sending emails to unregistered users, reminding them to respond to the
user's invitation to join "Facebook", was violating the obligation to ask for prior consent before
sending the email to a "Friend". An analysis for the legal question of whether Article 13 should
be applicable to this practice will be given below.

3. Overview on the implementation of the General Directive and the
e-Privacy Directive in the German legal system

This part of the Thesis shall give an overview on the implementation of the General Directive
and the e-Privacy Directive in the German legal system with an emphasis on the provisions that
could be applicable to a private entity who provides the "Friend Finder" services on the Internet.

The German data protection law is the Federal Data Protection Act,
(Bundesdatenschutzgesetz) ("BDSG").\textsuperscript{112} The BDSG applies to the collection, processing and use
of personal data by public federal bodies and private bodies.\textsuperscript{113} In the German legal system each
one of Germany's states has its own state data protection law, which applies to the public sector
only. Personal data is defined in the BDSG as "any information concerning the personal or material
circumstances of an identified or identifiable natural person".\textsuperscript{114} Processing of personal data according to
the BDSG, means collecting data for use in data processing systems, or using such systems to
process or use data, or collect data in or from non-automated filing systems, or use such systems
to process or use data, unless the data is collected, processed or used solely for personal or

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{111} See Article 15(2) of the e-Privacy Directive.
\item \textsuperscript{112} See The Federal Data Protection Act (BDSG) In the version promulgated on 14 January 2003 (Federal Law
Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force
from 1 September 2009, available at,
\url{http://www.bfdi.bund.de/klc_136/EN/DataProtectionActs/DataProtectionActs_node.html}, last visited on 20,
June 2011.
\item \textsuperscript{113} See Section 1 (2) of the BDSG; See Sections 3(3), 3(4) and 3(5) of the BDSG.
\item \textsuperscript{114} See Section 3 (1) of the BDSG.
\end{itemize}
\end{footnotesize}
domestic activities. In addition, the protection under BDSG has been given only to a natural person.

The BDSG defines the concept of "controller" as any person or body which collects processes or uses personal data on his, her or its own behalf, or commissions others to do the same. According to the BDSG, the processor may process or use the data only as instructed by the controller, however, the processor is reliable to ensure that the implementation of the provisions of the BDSG are in place, and to appoint an internal data protection officer. The distinction between "controller" and "processor", under the BDSG was described by scholars as follows: "If a data processor (the term used in the BDSG to refer to an entity that processes data on behalf of a data controller) is used by the data controller, the BDSG does not treat the data processor as a data controller, nor the data transfer to the data processor as a disclosure of the data, provided that the data processor processes the data within the EU or the EEA. Rather, responsibility for compliance with the BDSG and other data protection provisions rests with the data controller". Therefore, most of the obligations under the BDSG must be met by the controller.

The BDSG states that the controller has the obligation to notify the competent supervisory authority before carrying out any automated processing operations. BDSG exempts the notification requirement in cases where the controller has appointed an internal data protection officer ("DPO"). In addition, the exemption applies where the controller collects, processes or uses personal data for its own persons and no more than nine employees are employed in collecting, processing or using personal data, and either the data subject has given his or her consent or the collection, processing or use is needed to create, carry out or terminate a legal obligation or a quasi-legal obligation with the data subject.

---

115 See Section 1 (2) No.3 of the BDSG.
116 See Section 3(7) of the BDSG.
117 See Section 9 of the BDSG.
118 See Section 4f and 4g of the BDSG.
119 See Christopher Milford, Mark Ford, Marcus Turle: "Data Protection Laws of the World", Sweet & Maxwell Thomson Reuters, London 2010, p. Germany/6 ; see also Section 11 of the BDSG.
120 See Section 4d(1) of the BDSG.
121 See Section 4d(3) of the BDSG.
A Controller is obliged to appoint a DPO where personal data are collected, processed or used by other means and, as a rule, at least 20 persons are employed for this purpose unless more than nine persons are permanently employed in the automated processing of personal data.\textsuperscript{122} The DPO is responsible for the compliance of the data controller with the data protection laws and may be an internal employee or external third party.\textsuperscript{123} The BDSG states that the collection, processing and use of personal data shall be lawful only if permitted or ordered by the BDSG provision or other law, or if the data subject has provided consent.\textsuperscript{124} In addition, consent shall be effective only when based on the data subject’s free decision. The BDSG requires that data subjects shall be informed of the purpose of collection, processing or use and, as necessary in the individual case or on request, of the consequences of withholding consent, and that consent shall be given in writing.\textsuperscript{125}

The specific provisions of the e-Privacy Directive concerning the telecommunication sectors and the sending of unsolicited communications for direct marketing purposes were implemented in Germany’s Telecommunications Act\textsuperscript{126} (TKG) and the Act Against Unfair Competition (AAUC).\textsuperscript{127} Article 13 of the e-Privacy Directive was implemented in section 7 of the AAUC. According to this provision, using e-mails for advertising without the recipient’s prior consent shall be considered unconscionable pestering, and therefore illegal.\textsuperscript{128} The BDSG requires that explicit consent shall be given by the recipient of the email. However, scholars in Germany argue that consent may result from the actual circumstances, but have pointed out that

\begin{footnotesize}
\begin{enumerate}
\item See Section 4f (1) of the BDSG.
\item See Section 4f(2) of the BDSG; For other provisions facilitating the position of the data protection officer see Section 4f(3) of the BDSG.
\item See Section 4 (1) of the BDSG.
\item See Section 4a(1) of the BDSG.
\item See Section 4a(1) of the BDSG.
\end{enumerate}
\end{footnotesize}
the publication of an email address or just visiting a website for example does not constitute consent to receive an email advertisement.  

The AAUC states that using emails for direct marketing purposes shall not be considered illegal practice, where the following conditions have been fulfilled: Firstly, the email sender has obtained from the customer the email address in connection with the sale of goods or services; Second, the email sender uses the email address for direct advertising of his own similar goods or services; Third, the customer has not objected to this use; Fourth, the customer has been clearly and unequivocally advised, when the address is recorded, and each time it is used, that he/she can object to such use at any time without costs arising by virtue thereof other than transmission costs pursuant to the basic rates. Some scholars argue that the exception for sending emails for marketing purposes without prior consent of the recipient, does not apply to businesses because the wording of section 7(3) of the AAUC refers only to "customers", but on the other hand, some scholars suggest arguments which support the application of the exemption to businesses, based on the reason that data protection law also allows Member States to protect the legitimate interest of enterprises to have functioning networks. To sum, in Germany, without the recipient providing explicit prior consent for sending email messages for direct marketing, the act of sending of a message should be considered unlawful unless it falls under the exemption stated on section 7(3) of the AAUC.

The BDSG entitles the data subject to the right to be informed by the data controller if personal data relating to him or her have been processed for the first time without the data subject’s knowledge, for personal purposes or for purposes of transfer for third parties. The right to be informed may be exempted on cases applying to the right to access, with the

---

130 See Section 7(3) of the AAUC.
132 See Section 33 of the BDSG.
133 See Section 33 of the BDSG.
supplement of exemptions which are resulted from the fact that the data subject already received knowledge of holding records or transferring data to third parties. In addition, under the BDSG the data subject has the right to make corrections to data, when data relating to him or her is inaccurate, and the right to deletion and the right to blocking of such data.

Section 7 of the BDSG stated that controller is obliged to compensate the data subject for damages that he or she suffered as a result of unlawful or improper collection, processing and use of personal data which is relating to the data subject unless the controller exercised reasonable due care. In addition, in Germany, a violation of obligations imposed by the BDSG shall be deemed an administrative offence that may lead to fines or criminal offence that may lead to imprisonment.

An overall assessment of the implementation of the General Directive and the e-Privacy Directive in the German legal system can bring to the conclusion that the German legislators have chosen to give high level of protection to the processing of the personal data of individuals. The strict approach for data protection in Germany can be seen for example, in the provision imposing on the data controller obligation to appoint internal DPO, and the provision restricting effective consent only to cases where consent has been given in writing and the provision which limits the cases where the obligation to inform data subject when his or her personal data is processed, could be applicable. The German approach for protection processing of personal data may raise a legal question whether the strict approach for data protection may be considered as disproportionate and in conflict with EU data protection law, as it may lead to restriction for the free movement of data which is necessary to achieve the internal market.

---

134 See Section 33(2) of the BDSG.
135 See Section 35 of the BDSG.
136 See Section 43-44 of the BDSG.
IV. Application of the General Directive

1. Whether an Entity is allowed to collect email addresses by using the "Friend Finder" service

An email address can be classified as personal data because it contains information which allows one to identify a specific person. Email addresses (e.g., john.smith@example.com) can include the name of the person on the left part, and on the right part, the name of the host server where the person has registered his or her email account. It is worth pointing out that even if the user does not use his or her actual name, it is possible to identify information about the person through the host server. Therefore, email addresses are "personal data".

As discussed above, the "Friend Finder" service is a marketing method, inviting the SNS user to provide access to his or her email address book data (from outlook, webmail, iPod), including an access to email addresses of unregistered users. The SNS provider collects the email addresses, including those of unregistered users, to its database, compares it with email addresses of existing users, and uses the "Friend Finder" service to invite the unregistered users to join the SNS. Therefore, the analysis of the address book could be considered as processing of personal data.

Furthermore, the SNS provider could be classified as a data controller. Firstly, the SNS provider can be classified as a data controller, because it provides the means for processing the user's address book data. Thus, the SNS provider provides the "Friend Finder" service, including the server and the database where the email address book data are saved and have been analyzed.

---

137 See Article 2(a) of the General Directive.
139 See Article 2(b) of the General Directive.
Secondly, the SNS provider determines the use that may be made with the email address book. Thus, as has been described above, the email address is used for the purpose of sending emails messages to Friends, asking them to subscribe to the SNS. Therefore the SNS provider shall be considered a data controller, and held responsible for compliance with the General Directive and the e-Privacy Directive provisions. A question might arise whether the SNS user who chooses to use the "Friend Finder" service, can be classified as a data controller. This can be the case where the user uses the "Friend Finder" service for activities that extend beyond "purely personal or household activities"("Household Exemption"). When the Household Exemption does not cover the user activity, the General Directive applies and the user could be classify as "data controller", and held responsible to comply with the obligation of the General Directive and the e-Privacy Directive like any other data controller, including the obligation to obtain a consent from a "Friend", before the user decides to use the "Friend Finder" service, to invite friends to join his or her network on the SNS. Some scholars support the argument, that within Social Networking Sites, it may be possible that the individual user can be brought within the scope of the definition "data controller".

It can be argued that the practice of collecting and analyzing of addresses of unregistered users should be considered an illegal practice according to the General Directive provisions for three main reasons:

Firstly, the processing of email addresses of the unregistered users which was obtained from the user's address book data, may be considered as "unfair" processing of data, unless the Friend, has been provided with information on the identity of the controller and his representative, the purpose of the processing and any further information such as the recipient,

---

141 See Article 3(2) of the General Directive.
144 See Article 6(a) of the General Directive.
and the existence of the right to rectify the data.\footnote{See Article 11 (1) of the General Directive.} In addition, it is the data controller's obligation to notify the unregistered user about this information at the time of the processing of the data or, if the data is likely to be disclosed to a third party other then the controller, no later than the time when the data is first disclosed.\footnote{See Article 11 (1) of the General Directive.} To clarify the notion of "fairness", it may be worth referring to the U.K. Data Protection Tribunal judgment of Midlands Electricity Plc v Data Protection Register: "We consider an underlying purpose of the data protection principles is to protect privacy with respect to processing of personal data. We do not overlook the fact that the ability to process personal data, including that for purposes of trade and commerce, has substantial benefits for the general public. In approaching the question of fairness undefined in the Act, we consider it requires that we should weigh up the interests both of data subjects and data users". \footnote{See Data Protection Tribunal, England, Midlands Electricity Plc. v Data protection Registrar, [1999] Info TLR 217, available at \url{http://www.informationtribunal.gov.uk/DBFiles/Decision/i236/Midlands_Electricity.pdf}, last visited in 3 July 2011, p. 8; See Data Protection Tribunal, Case No. DA98 3/49/2, British Gas Trading Limited v Data Protection Registrar, (Unreported), 24 March 1998, \url{http://www.informationtribunal.gov.uk/DBFiles/Decision/i162/british_gas.pdf}, last visited in 3 July 2011, p. 11, paragraph 4.} In light of the above rule and case law, processing of unregistered user's by the "Friend Finder" service, may be considered as unfair and therefore illegal processing of personal data, unless relevant information has been given to the "Friend". It is worth pointing out that the Art. 29 WP expressed its opinion that collecting of email address in a "public space on the internet" without the informed knowledge of the individual for the purposes of electronic mailing could be seen as "unfair processing".\footnote{See the Article 29 Working Party “Opinion 1/2000 on certain data protection aspects of electronic commerce”, (WP 28), 3 February 2000, available at, \url{http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2000_en.htm}, last visited in 15 July 2011 p. 4; See the Article 29 Working Party “Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union”, (WP 43) 17 May 2001, available at, \url{http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/}, last visited on 23 June 2011, p.8, and the reference in footnote No.13.} Applying this opinion to the case of the "Friend Finder" service, may bring to a result that the use of the "Friend Finder" service for collecting email address of unregistered users shall be considered as an "unfair" practice. On the other hand, it could be argued that collecting of email addresses in the "Friend Finder" Service can not be regarded as "public space" because Social Networking Sites usually are not opened to the public, therefore, the Art. 29 WP opinion on these issues could be argued as irrelevant. An exception to the obligation which bounds the controller to provide information to the unregistered user,
whose email address was supplied by the SNS user, applies where the provision of that information would involve a "disproportionate effort".149 Scholars have suggested that in considering whether to apply the "disproportionate effort" exemption, the following factors should be taken in account: The time and the effort or the cost to the controller in providing the relevant information to the data subject and the "prejudicial effect on the data subject caused by the lack of availability of such information".150 A potential argument for the application of the "disproportionate effort" exemption to the practice used by the "Friend Finder" service for processing address book data, is that in view of the high quantity of email address which are collected from the user's email address book, the effort and the cost involved in making the information readily available to each data subject shall be quite a considerable effort, considering the prejudicial effect on the data subject, whose email is been processed. Therefore, the obligation to make the information available to the "Friend" has to be removed.

Second, the collection of email addresses of a "Friend" that was provided by the user of the SNS for a specific purpose (e.g., to be able to contact with others), shall be considered illegal processing if it will be used by the controller for other purposes such as sending marketing messages.151

Third, legitimate grounds for collection of personal data without the data subject’s consent is where collecting of data is necessary for the purpose of a legitimate interest pursued by the controller, except where such interest are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under article 1(1) of the General Directive.152 An argument for considering the "Friend Finder" service as non-legitimate processing can be that allowing the processing of unregistered users in the absence of consent to allow the SNS provider to engage in direct marketing, may not be considered as a legitimate

149 See Article 11(2) of the General Directive.
151 See Article 6 (b) sentence No.1 of the General Directive.
interest of a controller, unless the recipient of the marketing communication is an existing user\textsuperscript{153}. It is worth pointing out that the Art. 29 WP is in the opinion that, "The cost imbalance and the nuisance to the recipient, such mailing could not be regarded as passing the balance of interest test in Article 7(6)"\textsuperscript{154}. Therefore, unless legitimate interests exist for processing unregistered users email data, the "Friend Finder" service shall be considered illegitimate and should be restricted to those cases where consent has been already given by the "Friend",\textsuperscript{155} or where there is a contract or a legal obligation allowing the controller to collect the email address data and to use it for marketing purposes.\textsuperscript{156} It is worth to note that, the user's interests also have to be taken into account when collecting email addresses from his or her address book in the sense that the controller is obliged to inform about the collection of the address book data for the purpose of sending marketing messages.\textsuperscript{157} In addition, the user has the right to be informed before the email address data is collected from his/her address book, and the right to object to the collecting and further use of the data.\textsuperscript{158} Finally, it should be mentioned that the user is also entitled to rectify, erase or block any data which is unlawfully collected by the controller or on behalf of the controller.\textsuperscript{159}

2. The question of the application of the EU data protection law to non-EU based entities which are processing personal data of individuals in the EU outside of the EU territory

It can be argued that Article 4(1)(c) of the General Directive should be applicable to non-EU based entities which are involved in providing services for individuals in the EU territory. To support this argument, it is worth to note that on Recital 20 of the General Directive, the EU legislator wished to ensure that even in the event the controller has no establishment in the EU at


\textsuperscript{155}See Article 7(a) of the General Directive.

\textsuperscript{156}See Article 7(b) and 7(c) of the General Directive.

\textsuperscript{157}See Article 10 of the General Directive.

\textsuperscript{158}See Article 14 of the General Directive.

\textsuperscript{159}See Article 12(b) of the General Directive.
all, EU data protection law will apply if the actual data processing takes place in a Member State by means of use of the equipment.\textsuperscript{160}

Furthermore, as stated above, article 4(1)(c) of the General Directive applies when an entity engaged in the processing of personal data, does not hold an "establishment" in the EU territory. The Art. 29 WP pointed out that, this provision is relevant in particular in light of developing internet technologies which enable the collection and processing of personal data without maintaining a presence in the EU territory.\textsuperscript{161} The most important requirement for applying EU data protection law on an entity located outside of the EU territory is that this entity is "making use" of "equipment" located on the EU territory - such as a server or a computer - for processing information.\textsuperscript{162} The Art. 29 WP clarifies that the concept of "making use of equipment" consists of some kind of activity of the entity and the existence of the clear intention of the controller to process personal data.\textsuperscript{163} However, the Art. 29 WP points out that whether an activity of an entity should be considered as an "equipment" and thereby, triggers the application of the EU Member State national data protection law, is subject to a case to case assessment. The Art. 29 WP, had been suggested that a computer collects personal data from users situated in the EU territory could be considered as "equipment".\textsuperscript{164} An argument against the application of article 4(1)(c) of the General Directive, is when the non-EU based entity's "equipment" which is located in the EU is used only to ensure transit of data through the union territory, with no element of processing of personal data or providing "any added value" services manipulating the


data (such as spam filtering) at the time of transmission. Another argument against the application of article 4(1)(c) of the General Directive regarding non-EU based entities is that it may be very difficult to enforce a non-EU based entity to comply with EU data protection rules. Scholars argue that "strict application of article 4(1)(c) of the General Directive, may create a situation in which large numbers of data controllers outside the EU/EEA are supposed to comply with at least two sets of data protection rules that may not be harmonized". To avoid such a consequence, it may be justified to exempt entities which carry out the processing of personal data outside the EU territory, and which do not hold an "establishment" in the EU territory when it is already subject to its own national data protection law. It is worth noting that scholars have already suggested to limit the application of article 4(1)(c) of the General Directive only to the cases where the non-EU based entity either attempts to circumvent the law of an EU Member State by relocation his/her/its establishment to a third country (but still uses means situated in the EU), or where the controller (who is located in a third country) transmits data to a third country for further processing. Based on the opinion represented above, it may be possible that non-EU based entities that are involved in processing personal data of individuals from the EU, may have to respect the rights and obligations provided in EU data protection law.

Another legal question is whether EU data protection law applies when the non-EU based entity holds a sales office inside the EU territory, which is not involved in activities relating to data processing of personal data of visitors of the website from the EU. On this case, it could be argued that Article 4(1)(a) of the General Directive may be applicable only if, the sales office could be considered as "establishment", and if the sales office processes data of visitors of a website from the EU. If the processing by the non-EU based entity, can be considered "to be carried out in the context of the activities of the establishment", the foreign entity should be

---


subject to EU data protection law. However, if the sales office has no involvement with the relevant website users, by maintaining relations with the users or by sending advertisement to users article 4(1)(a) will not apply.\textsuperscript{168}

V. Application of the E-Privacy Directive

1. Whether the SNS provider is allowed to use the "Friend Finder" service for sending email messages inviting unregistered users to join the SNS

After the user's email address book has been processed by the SNS provider, the user is asked to invite "Friends", by sending an email message in which the content was formulated by the SNS provider, and that the sender can not freely determine, asking the "Friends" to join the SNS (The formulated message shall be referred as "The Invitation"). If the "Friend" does not respond to The Invitation, the SNS provider keeps and sends The Invitations on behalf of the registered user, reminding the "Friend" to join the SNS. This method, is similar to the first marketing method used by the Friend Finder service that was presented above. For the purpose of the legal analysis it is worth mentioning the second method as well, which allows the user to enter an email of a "Friend" on the website, and send an email message to the "Friend", by him/herself. In addition, the third method, when the SNS provider asks the user to send email message inviting potential "Friend" to join the SNS, should be taken in account in the legal analysis.

As mentioned above, a controller is responsible for the compliance with the provisions of EU data protection law. In particular, according to the e-Privacy Directive, the controller has to ensure that an unregistered user has given prior consent for using his/her email address for direct marketing purposes.\textsuperscript{169} Hence, the practice of using the "Friend Finder" service for sending the invitations to the unregistered user, on behalf of the registered user, asking him/her to join to the SNS, without consent, may be considered unlawful, except in certain circumstances that fall


\textsuperscript{169} See Article 13(1) of the e-Privacy Directive.
under the "opt-out" regime mentioned above. In addition to the obligation to obtain prior consent, the practice of sending reminder emails to join the SNS on behalf of the user, may be prohibited according to article 13(4) of the e-Privacy Directive. The Art. 29 WP expressed its opinion that sending invitations asking unregistered users, whose details were obtained from a user to join an SNS violates the prohibition to disguise or to conceal the identity of the person on whose behalf the communication is made, laid down in Article 13(4) of the ePrivacy Directive.\textsuperscript{170} However, it's unclear whether article 13(4) of the e-Privacy Directive covers a case where the "Friend Finder" service allows the user to send The Invitation to unregistered users by him/herself, as was described in the second method. An argument against the application of article 13 (4) of the e-Privacy Directive regarding the practice of sending the invitation by the sender him/herself could be that this practice falls into the scope of the "personal communications" exemption, which requires the following conditions to be fulfilled: "- no incentive is given to either sender or recipient; - the provider does not select the recipients of the message; the identity of the sending user must be clearly mentioned; - the sending user must know the full content of the message that will be sent on his behalf".\textsuperscript{171} Under this condition, the practice of allowing the user to send the invitation to a "Friend", may not fall under the prohibition laid down under article 13(4) of the e-Privacy Directive. An objection to this argument could be that by formulating the content of the invitation on behalf of the user, and by restricting the possibility to personalize the content of the invitation before sending the invitation to a "Friend", may be considered giving "incentive" to send the invitation, thereby failing to trigger the application of the "personal communication" exception. Based on the "personal communication" exception represented here, it can be argued that article 13(4) of the e-Privacy Directive does not cover the practice allowing the user to send the invitation to join the SNS, unless the user has given some kind of incentive to send the invitation.


A question may arise whether article 13 (1) of the e-Privacy Directive covers the sending of emails to an unregistered user for the purposes of direct marketing without his/her prior consent. Thus, an argument against the application of Article 13(1) of the e-Privacy Directive could be that when a user sends an email to a "Friend" offering him/her a chance to join, the SNS should not be considered as "Direct Marketing". To be able to answer this question it might be useful to look at the meaning of "Direct Marketing". The meaning of Direct marketing was not defined either in the General Directive nor in the e-Privacy Directive. However, "Direct Marketing" was defined by the "Federation of European Direct and Interactive Marketing" ("FEDMA"), in the European code of practice for the use of personal data in direct marketing ("The European code") as follows: "The communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc...) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals".172

It is important to point out that the Art. 29 WP considers the definition of the European code for "Direct Marketing" to be in accordance with the General Directive and the e-Privacy provisions.173 Therefore, in view of The European code definition, it can be argued that when the SNS provider sends The Invitation, it may be considered as "Direct Marketing" and prior consent must then be obtained. On the other hand, when the sender of The Invitation is the user him/herself, and not the SNS provider (the "Direct Marketer"), it may not considered as "Direct Marketing", presuming the user does not send The Invitation on behalf of the Direct Marketer. Therefore, if the above argument could be accepted, the result should be that Article 13(1) of the e-Privacy Directive may not be applicable to the case of sending messages by the user him/herself to a "Friend" and that the requirement to obtain prior consent shall be removed.

Where consent must be obtained for sending email messages to the "Friend", such consent should be by way of clicking on a box online,174 or by asking the "Friend" to register to the SNS service and later asking the new user to confirm that he/she was the person who has

---

174 See Recital 17 of the e-Privacy Directive.
been registered in order to confirm that consent has been really given.175 It is worth pointing out that the exception of "opt-out" described in Article 13(2) of the e-Privacy Directive may not be applicable to the "Friend Finder" service due to the requirement that the SNS provider has obtained the email contact details directly from a "customer". Due to the reason that a "Friend" may not be considered as a "customer" of an SNS service the "opt-out" exception should not apply.

In light of the above legal analysis one may conclude as follow:

With regards to the first method: the practice where the SNS provider sends an invitation to unregistered users asking him/her to join the SNS (or a reminder email asking to join the SNS), without obtaining consent, may be considered unlawful. In addition, the practice of sending reminding emails to join the SNS on behalf of the user could be covered by the prohibition laid down in Article 13(4) of the e-Privacy Directive.

With regards, to the second and the third method: where the SNS provider allows the user to send the "Friend" The Invitation by him/herself, this practice could be lawful if the "personal communication" exception is applicable, unless the user has given some kind of incentive to send The Invitation to the unregistered "Friend". If the practice of allowing the user to send The Invitation to an unregistered user by him/herself is not considered as "Direct Marketing", Article 13(1) of the e-Privacy Directive should not cover the case and the requirement to obtain prior consent, shall be removed.

---

E. CONCLUSION

1. Applicable law – Generally

- The "Friend Finder" service is a method of marketing that uses the SNS user's email address book data to send an email message to invite unregistered users, to join the SNS. The "Friend Finder" service utilizes three kinds of marketing methods: One method, is when the SNS provider asks a user to provide an email address of a "Friend" or a person they know, and the website sends an email offering that person a product or a service on behalf of the user. The second method allows the user to enter an email address of a friend on the website and to send an email message by him/herself. The third method is where the website asks a user to send an email message recommending a service or a product to a "Friend".

- The General Directive and the e-Privacy Directive may cover the use of the "Friend Finder" service and they may provide the answer for the three legal questions that have been discussed in the Thesis.

2. The application of the General Directive

- An email address shall be classified as "personal data". The SNS provider activity is considered as processing of personal data. The SNS provider could be classified as a controller. However, in some cases, the user can be classified as a data controller as well. A question might arise, if the relationship between the SNS provider and the SNS user could be classified as a relationship of a controller and a processor.

- The practice of collecting and processing email addresses of unregistered users by using the "Friend Finder" service may be considered to be illegal according to the General Directive provisions for three main reasons: Firstly, the use of the "Friend Finder" service for collecting email addresses of unregistered users can be considered as an "unfair" practice, unless relevant information has been given to the "Friend". The obligation to make the information available to the "Friend" could be removed if
the "disproportionate effort" exemption is applicable to the practice used by the "Friend Finder" service.

- Second, the practice of collecting email addresses could be considered to be illegal, if it will be used by the controller for other purposes, such as marketing purposes.

- Third, unless legitimate interests exist for processing unregistered users’ email data, the "Friend Finder" service shall be considered as illegitimate and should be restricted to those cases where consent has already been given by the "Friend", or where there is a contract or a legal obligation allowing the controller to collect the email address data and use it for marketing purposes.

3. The application of the e-Privacy Directive

- In regard to the application of the e-Privacy Directive, one can conclude as follows: The first method, the practice where the SNS provider sends an invitation to unregistered users asking him/her to join the SNS (or reminder email asking him/her to join the SNS), without obtaining consent, may be considered unlawful. The practice of sending messages inviting an individual to join the SNS on behalf of the user could be covered by the prohibition laid down in Article 13(4) of the e-Privacy Directive to disguise the identity of the sender.

- The second and the third method, where the SNS provider allows the user to send the "Friend" the invitation by him/herself, could be lawful if the "personal communication" exception is applicable, unless the sender of The invitation has given some kind of incentive to send The invitation to the "Friend". If the practice of allowing the user to send The Invitation to unregistered users by him/herself should not considered as "Direct Marketing", Article 13(1) of the e-Privacy Directive should not cover the case and the requirement to obtain prior consent shall be removed.
4. Jurisdiction

- Article 4(1)(c) of the General Directive could be applicable to non-EU based entities which does not hold an "establishment" in the EU territory but is involved in providing online services for individuals in the EU territory by using "equipment" (e.g., computer or a server) located in the EU territory.

- An argument against the application of Article 4(1)(c) of the General Directive could be when the non-EU based entity's "equipment" is used only to ensure transit of data through the union territory. When considering whether the EU data protection should be applicable, one may take in account if it is possible to enforce a non-EU based entity to comply with EU data protection law, especially when the non EU-based entity is already subject to its own national data protection law.

- In a case when the non-EU based entity holds a sales office in the EU, which is not involved in activities relating to data processing of personal data of visitors of the website from the EU, it could be argued that Article 4(1)(a) of the General Directive should not apply on the non-EU based entity, unless the sales office involved with maintaining relations with the users or by sending advertisement to users.

5. Rights and obligations

- The controller is obliged to inform both the user and the non-member of the SNS about the collection of the email contact details, about the purposes of the collecting, the recipient of the data, and on the existence of the right to rectify the data.

- The user has the right to be informed before the email address data is collected from his/her address book and holds the right to object to the collecting and further use of the data. The user is also entitled to rectify, erase, or block any data that is unlawfully collected by the controller or on behalf of the controller.

- The SNS provider must ensure compliance of the provisions of the e-Privacy Directive. Among other provisions, the controller needs to ensure that the "Friend" is
a "subscriber" or a user of the SNS service and that he/she has given prior consent for using his/her email address for marketing purposes.

- Giving consent may be for example the action of clicking on a box online or asking a user to register to the SNS service and later asking the new user to confirm that he/she was the person who has been registered and confirm his/her consent.

- Based on the legal framework provided in the General Directive and the e-Privacy Directive, it is clear that the current data protection legislation does not give a complete answer to the legal questions that arise in the context of "Friend Finder" service. For instance, the General Directive is still very ambiguous with regards to what constitutes legitimate consent for the purpose of processing personal data in social networks. It may be argued that in the context of private Social Networking Sites, which are considered to be closed to the public, no consent is needed for the processing of address book data of friends. It is needless to say, that once a person offered his or her contact details, this act itself can be considered as giving a "consent". Furthermore, in view of the personal relationships that characterize a Social Networking Site, the obligation to obtain a prior consent from a friend before sending an email could be deemed unnecessary. In addition, the current requirement to inform a friend each time his or her email address has been analyzed or processed by the "Friend Finder" service may be practically impossible and could result in additional costs for the SNS provider, as well as the SNS user, due to the measures that would subsequently need to be implemented. Finally, EU data protection law does not provide adequate provisions to deal with the problem of processing of personal data by entities which are located outside the EU territory and are already subject to there own national law. This situation may bring uncertainty to global internet companies with regards to the laws they need to comply with, and can result in an additional costs, which again, probably will and should fall on the person who chooses to use the Social Networking Sites.
BIBLIOGRAPHY

BOOKS


CASE LAW

ECJ, Case C-22/70, Commission v. Council (AETR/ERTA), ECR 1971, 263.

ECJ, Case C-6/64 Flaminio Costa v. ENEL, CMLR 1964, 585.


ECJ, Case C-101/01 Bodil Lindqvist v. Kammaraklagarenh, ECR 2003, I-12971


ARTICLES


**OTHER REFERENCES**


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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF
THE EUROPEAN UNION.

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on
European Union, include creating an ever closer union among the peoples of Europe, fostering
closer relations between the States belonging to the Community, ensuring economic and social progress
by common action to eliminate the barriers which divide Europe, encouraging the constant
improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and
promoting democracy on the basis of the fundamental rights recognized in the constitution
and laws of the Member States and in the
European Convention for the Protection of Human
Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to
serve many whereas they must, whatever the
nationality or residence of natural persons, respect
their fundamental rights and freedoms, notably the
right to privacy, and contribute to economic and
social progress, trade expansion and the well-being
of individuals;

(3) Whereas the establishment and functioning of an
internal market in which, in accordance with

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11.
No C 94, 13. 4. 1992, p. 198), confirmed on 2 December
position of 20 February 1995 (OJ No C 93, 13. 4. 1995,
p. 1) and Decision of the European Parliament of 15 June

Article 7a of the Treaty, the free movement of
goods, persons, services and capital is ensured require not only that personal data should be able to
flow freely from one Member State to another, but also that the fundamental rights of individuals
should be safeguarded;

(4) Whereas increasingly frequent recourse is being
had in the Community to the processing of
personal data in the various spheres of economic
and social activity; whereas the progress made in
information technology is making the processing
and exchange of such data considerably easier;

(5) Whereas the economic and social integration
resulting from the establishment and functioning of
the internal market within the meaning of Article
7a of the Treaty will necessarily lead to a
substantial increase in cross-border flows of
personal data between all those involved in a
private or public capacity in economic and social
activity in the Member States; whereas the
exchange of personal data between undertakings in
different Member States is set to increase; whereas
the national authorities in the various Member
States are being called upon by virtue of
Community law to collaborate and exchange
personal data so as to be able to perform their
duties or carry out tasks on behalf of an authority
in another Member State within the context of the
area without internal frontiers as constituted by
the internal market;

(6) Whereas, furthermore, the increase in scientific and
technical cooperation and the coordinated
introduction of new telecommunications networks in
the Community necessitate and facilitate
cross-border flows of personal data;

(7) Whereas the difference in levels of protection of
the rights and freedoms of individuals, notably the
right to privacy, with regard to the processing of
personal data afforded in the Member States may
prevent the transmission of such data from the
territory of one Member State to that of another
Member State; whereas this difference may
therefore constitute an obstacle to the pursuit of a
number of economic activities at Community level,
distort competition and impede authorities in the
discharge of their responsibilities under
Community law; whereas this difference in levels
of protection is due to the existence of a wide
variety of national laws, regulations and
administrative provisions;

(8) Whereas, in order to remove the obstacles to flows
of personal data, the level of protection of the
rights and freedoms of individuals with regard to
the processing of such data must be equivalent in
all Member States; whereas this objective is vital to the
internal market but cannot be achieved by the
Member States alone, especially in view of the
scale of the divergences which currently exist
between the relevant laws in the Member States
and the need to coordinate the laws of the Member States so as to ensure that the
cross-border flow of personal data is regulated in a
consistent manner that is in keeping with the
objective of the internal market as provided for in
Article 7a of the Treaty; whereas Community
action to approximate those laws is therefore
needed;

(9) Whereas, given the equivalent protection resulting
from the approximation of national laws, the
Member States will no longer be able to inhibit the
free movement between them of personal data on
grounds relating to protection of the rights and
freedoms of individuals, and in particular the right
to privacy; whereas Member States will be left a
margin for manoeuvre, which may, in the context of
implementation of the Directive, also be
exercised by the business and social partners;
whereas Member States will therefore be able to
specify in their national law the general conditions
governing the lawfulness of data processing;
whereas in doing so the Member States shall strive
to improve the protection currently provided by
their legislation; whereas, within the limits of this
margin for manoeuvre and in accordance with
Community law, disparities could arise in the
implementation of the Directive, and this could
have an effect on the movement of data within a
Member State as well as within the Community;

(10) Whereas the object of the national laws on the
processing of personal data is to protect
fundamental rights and freedoms, notably the right
to privacy, which is recognized both in Article 8 of
the European Convention for the Protection of
Human Rights and Fundamental Freedoms and in
the general principles of Community law; whereas,
for that reason, the approximation of those laws
must not result in any lessening of the protection
they afford but must, on the contrary, seek to
ensure a high level of protection in the
Community;

(11) Whereas the principles of the protection of the
rights and freedoms of individuals, notably the
right to privacy, which are contained in this
Directive, give substance to and amplify those
contained in the Council of Europe Convention of
28 January 1981 for the Protection of Individuals
with regard to Automatic Processing of Personal
Data;

(12) Whereas the protection principles must apply to all
processing of personal data by any person whose
activities are governed by Community law; whereas
there should be excluded the processing of data
carried out by a natural person in the exercise of
activities which are exclusively personal or
domestic, such as correspondence and the holding
of records of addresses;

(13) Whereas the activities referred to in Titles V and
VI of the Treaty on European Union regarding
public safety, defence, State security or the
activities of the State in the area of criminal laws
fall outside the scope of Community law, without
prejudice to the obligations incumbent upon
Member States under Article 56 (2), Article 57 or
Article 101a of the Treaty establishing the
European Community; whereas the processing of
personal data that is necessary to safeguard the
economic well-being of the State does not fall
within the scope of this Directive where such
processing relates to State security matters;

(14) Whereas, given the importance of the
developments under way, in the framework of the
information society, of the techniques used to
capture, transmit, manipulate, record, store or
communicate sound and image data relating to
natural persons, this Directive should be applicable
to processing involving such data;

(15) Whereas the processing of such data is covered by
this Directive only if it is automated or if the data
processed are contained or are intended to be
contained in a filing system structured according to
specific criteria relating to individuals, so as to
permit easy access to the personal data in
question;

(16) Whereas the processing of sound and image data,
such as in cases of video surveillance, does not
come within the scope of this Directive if it is
carried out for the purposes of public security,
defence, national security or in the course of State
activities relating to the area of criminal law or of
other activities which do not come within the
scope of Community law;

(17) Whereas, as far as the processing of sound and
image data carried out for purposes of journalism
or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectoral laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas 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 are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set,
may be laid down by each Member State; whereas
files or sets of files as well as their cover pages,
which are not structured according to specific
criteria, shall under no circumstances fall within
the scope of this Directive;

(28) Whereas any processing of personal data must be
lawful and fair to the individuals concerned;
whereas, in particular, the data must be adequate,
reliable and not excessive in relation to the
purposes for which they are processed; whereas
such purposes must be explicit and legitimate and
must be determined at the time of collection of
the data; whereas the purposes of processing further to
collection shall not be incompatible with the
purposes as they were originally specified;

(29) Whereas the further processing of personal data
for historical, statistical or scientific purposes is
not generally to be considered incompatible with
the purposes for which the data have previously
been collected provided that Member States furnish
suitable safeguards; whereas these safeguards must
in particular rule out the use of the data in support
of measures or decisions regarding any particular
individual;

(30) Whereas, in order to be lawful, the processing of
personal data must in addition be carried out with
the consent of the data subject or be necessary for
the conclusion or performance of a contract
binding on the data subject, or as a legal
requirement, or for the performance of a task
carried out in the public interest or in the exercise
of official authority, or in the legitimate interests of
a natural or legal person, provided that the
interests or the rights and freedoms of the data
subject are not overriding; whereas, in particular,
in order to maintain a balance between the
interests involved while guaranteeing effective
competition, Member States may determine the
circumstances in which personal data may be used
or disclosed to a third party in the context of the
legitimate ordinary business activities of companies
and other bodies; whereas Member States may
similarly specify the conditions under which
personal data may be disclosed to a third party for
the purposes of marketing whether carried out
commercially or by a charitable organization or by
any other association or foundation, of a political
nature; for example, subject to the provisions
allowing a data subject to object to the processing
of data regarding him, at no cost and without
having to state his reasons;

(31) Whereas the processing of personal data must
equally be regarded as lawful where it is carried
out in order to protect an interest which is
essential for the data subject’s life;

(32) Whereas it is for national legislation to determine
whether the controller performing a task carried
out in the public interest or in the exercise of
official authority should be a public administration
or another natural or legal person governed by
public law, or by private law such as a professional
association;

(33) Whereas data which are capable by their nature of
infringing fundamental freedoms or privacy should
not be processed unless the data subject gives his
explicit consent; whereas, however, derogations
from this prohibition must be explicitly provided
for in respect of specific needs, in particular where
the processing of these data is carried out for
certain health-related purposes by persons subject
to a legal obligation of professional secrecy or in
the course of legitimate activities by certain
associations or foundations the purpose of which is
to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized,
when justified by grounds of important public
interest, to derogate from the prohibition on
processing sensitive categories of data where
important reasons of public interest so justify in
areas such as public health and social protection -
especially in order to ensure the quality and
cost-effectiveness of the procedures used for
settling claims for benefits and services in the
health insurance system - scientific research and
government statistics; whereas it is incumbent on
them, however, to provide specific and suitable
safeguards so as to protect the fundamental rights
and the privacy of individuals;

(35) Whereas, moreover, the processing of personal
data by official authorities for achieving aims, laid
down in constitutional law or international public
law, of officially recognized religious associations is
carried out on important grounds of public
interest;

(36) Whereas where, in the course of electoral activities,
the operation of the democratic system requires in
certain Member States that political parties
compile data on people’s political opinion, the
processing of such data may be permitted for
reasons of important public interest, provided that
appropriate safeguards are established;

(37) Whereas the processing of personal data for
purposes of journalism or for purposes of literary
of artistic expression, in particular in the
audiovisual field, should qualify for exemption
from the requirements of certain provisions of this
Directive in so far as this is necessary to reconcile
the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) 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;

(47) Whereas a message containing personal data
is transmitted by means of a telecommunications
or electronic mail service, the sole purpose of
which is the transmission of such messages, the
controller in respect of the personal data contained
in the message will normally be considered to be
the person from whom the message originates,
rather than the person offering the transmission
services; whereas, nevertheless, those offering such
services will normally be considered controllers in
respect of the processing of the additional personal
data necessary for the operation of the service;

(48) Whereas the procedures for notifying the
supervisory authority are designed to ensure
disclosure of the purposes and main features of
any processing operation for the purpose of
verification that the operation is in accordance
with the national measures taken under this
Directive;

(49) Whereas, in order to avoid unsuitable
administrative formalities, exemptions from the
obligation to notify and simplification of the
notification required may be provided for by
Member States in cases where processing is
unlikely adversely to affect the rights and freedoms
data subjects, provided that it is in accordance
with a measure taken by a Member State
specifying its limits; whereas exemption or
simplification may similarly be provided for by
Member States where a person appointed by the
controller ensures that the processing carried out is
not likely adversely to affect the rights and
freedoms of data subjects; whereas such a data
protection official, whether or not an employee of
the controller, must be in a position to exercise his
functions in complete independence;

(50) Whereas exemption or simplification could be
provided for in cases of processing operations
whose sole purpose is the keeping of a register
intended, according to national law, to provide
information to the public and open to consultation
by the public or by any person demonstrating a
legitimate interest;

(51) Whereas, nevertheless, simplification or exemption
from the obligation to notify shall not release the
controller from any of the other obligations
resulting from this Directive;

(52) Whereas, in this context, ex post facto verification
by the competent authorities must in general be
considered a sufficient measure;

(53) Whereas, however, certain processing operation are
likely to pose specific risks to the rights and
freedoms of data subjects by virtue of their nature,
their scope or their purposes, such as that of
excluding individuals from a right, benefit or a
contract, or by virtue of the specific use of new
technologies; whereas it is for Member States, if
they so wish, to specify such risks in their
legislation;

(54) Whereas with regard to all the processing
undertaken in society, the amount posing such
specific risks should be very limited; whereas
Member States must provide that the supervisory
authority, or the data protection official in
cooperation with the authority, check such
processing prior to it being carried out; whereas
following this prior check, the supervisory
authority may, according to its national law, give
an opinion or an authorization regarding the
processing; whereas such checking may equally
take place in the course of the preparation either of
a measure of the national parliament or of a
measure based on such a legislative measure, which
defines the nature of the processing and lays down
appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights
data subjects, national legislation must provide
for a judicial remedy; whereas any damage which a
person may suffer as a result of unlawful
processing must be compensated for by the
controller, who may be exempted from liability if
he proves that he is not responsible for the
damage, in particular in cases where he establishes
fault on the part of the data subject or in case of
force majeure; whereas sanctions must be imposed
on any person, whether governed by private of
public law, who fails to comply with the national
measures taken under this Directive;

(56) Whereas cross-border flows of personal data are
necessary to the expansion of international trade;
whereas the protection of individuals guaranteed in
the Community by this Directive does not stand in
the way of transfers of personal data to third
countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned 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;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) 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;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period

(1) OJ No L 197, 18. 7. 1987, p. 33.
expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive’s provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State’s regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER 1
GENERAL PROVISIONS

Article 1
Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2
Definitions

For the purposes of this Directive:

(a) ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) ‘processing of personal data’ (‘processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) ‘personal data filing system’ (‘filing system’) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

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

(e) ‘processor’ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

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

(h) 'the data subject’s consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3
Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

— in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
— by a natural person in the course of a purely personal or household activity.

Article 4
National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.
SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

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

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

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

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:
   (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject’s giving his consent; or
   (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
   (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
   (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular
contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

c) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

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

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

— the recipients or categories of recipients of the data,

— whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

— the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;
(c) any further information such as
   — the categories of data concerned,
   — the recipients or categories of recipients,
   — the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V
THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12
Right of access

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

(a) without constraint at reasonable intervals and without excessive delay or expense:
   — confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
   — communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
   — knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

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

SECTION VI
EXEMPTIONS AND RESTRICTIONS

Article 13
Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

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

SECTION VII
THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14
The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where
otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

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

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

Article 15
Automated individual decisions

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

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII
CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16
Confidentiality of processing

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

Article 17
Security of processing

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

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

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

— the processor shall act only on instructions from the controller,

— the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX
NOTIFICATION

Article 18
Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory
authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

— where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

— where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

— for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

— for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.
The register shall contain at least the information listed in Article 19 (1) (a) to (c). The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (c) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III

JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration
shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission’s decision.

**Article 26**

**Derogations**

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject’s request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects to justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission’s decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission’s decision.
CHAPTER V

CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI

SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

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

— effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

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

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.
4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman’s term of office shall be two years. His appointment shall be renewable.

5. The Working Party’s secretariat shall be provided by the Commission.


7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission’s request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

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

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

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

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party’s opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall
also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII

COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

— the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,

— the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need
not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament
The President
K. HANSCH

For the Council
The President
L. ATIENZA Serna
DIRECTIVES


of 25 November 2009


(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Having regard to the opinion of the European Data Protection Supervisor (3),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (4),

Whereas:


(2) In that regard, the Commission presented its findings in its Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions of 29 June 2006 on the review of the EU regulatory framework for electronic communications networks and services.

(3) The reform of the EU regulatory framework for electronic communications networks and services, including the reinforcement of provisions for end-users with disabilities, represents a key step towards simultaneously achieving a Single European Information Space and an inclusive information society. These objectives are included in the strategic framework for the development of the information society as described in the Commission Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions of 1 June 2005 entitled ‘i2010 – A European Information Society for growth and employment’.

(4) A fundamental requirement of universal service is to provide users on request with a connection to the public communications network at a fixed location and at an affordable price. The requirement is for the provision of local, national and international telephone calls, facsimile communications and data services, the provision of which may be restricted by Member States to the end-user’s

primary location or residence. There should be no constraints on the technical means by which this is provided, allowing for wired or wireless technologies, nor any constraints on which operators provide part or all of universal service obligations.

(5) Data connections to the public communications network at a fixed location should be capable of supporting data communications at rates sufficient for access to online services such as those provided via the public Internet. The speed of Internet access experienced by a given user may depend on a number of factors, including the provider(s) of Internet connectivity as well as the given application for which a connection is being used. The data rate that can be supported by a connection to the public communications network depends on the capabilities of the subscriber’s terminal equipment as well as the connection. For this reason, it is not appropriate to mandate a specific data or bit rate at Community level. Flexibility is required to allow Member States to take measures, where necessary, to ensure that a data connection is capable of supporting satisfactory data rates which are sufficient to permit functional Internet access, as defined by the Member States, taking due account of specific circumstances in national markets, for instance the prevailing bandwidth used by the majority of subscribers in that Member State, and technological feasibility, provided that these measures seek to minimise market distortion. Where such measures result in an unfair burden on a designated undertaking, taking due account of the costs and revenues as well as the intangible benefits resulting from the provision of the services concerned, this may be included in any net cost calculation of universal obligations. Alternative financing of underlying network infrastructure, involving Community funding or national measures in accordance with Community law, may also be implemented.

(6) This is without prejudice to the need for the Commission to conduct a review of the universal service obligations, which may include the financing of such obligations, in accordance with Article 15 of Directive 2002/22/EC (Universal Service Directive), and, if appropriate, to present proposals for reform to meet public interest objectives.

(7) For the sake of clarity and simplicity, this Directive only deals with amendments to Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications).

(8) Without prejudice to Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (1), and in particular the disability requirements laid down in Article 3(3)(b) thereof, certain aspects of terminal equipment, including consumer premises equipment intended for disabled end-users, whether their special needs are due to disability or related to ageing, should be brought within the scope of Directive 2002/22/EC (Universal Service Directive) in order to facilitate access to networks and the use of services. Such equipment currently includes receive-only radio and television terminal equipment as well as special terminal devices for hearing-impaired end-users.

(9) Member States should introduce measures to promote the creation of a market for widely available products and services incorporating facilities for disabled end-users. This can be achieved, inter alia, by referring to European standards, introducing electronic accessibility (Accessibility) requirements for public procurement procedures and calls for tender relating to the provision of services, and by implementing legislation upholding the rights of disabled end-users.

(10) When an undertaking designated to provide universal service, as identified in Article 4 of Directive 2002/22/EC (Universal Service Directive), chooses to dispose of a substantial part, viewed in light of its universal service obligation, or all, of its local access network assets in the national territory to a separate legal entity under different ultimate ownership, the national regulatory authority should assess the effects of the transaction in order to ensure the continuity of universal service obligations in all or parts of the national territory. To this end, the national regulatory authority which imposed the universal service obligations should be informed by the undertaking in advance of the disposal. The assessment of the national regulatory authority should not prejudice the completion of the transaction.

(11) Technological developments have led to substantial reductions in the number of public pay telephones. In order to ensure technological neutrality and continued access by the public to voice telephony, national regulatory authorities should be able to impose obligations on undertakings to ensure not only that public pay telephones are provided to meet the reasonable needs of end-users, but also that alternative public voice telephony access points are provided for that purpose, if appropriate.

(12) Equivalence in disabled end-users’ access to services should be guaranteed to the level available to other end-users. To this end, access should be functionally equivalent, such that disabled end-users benefit from the same usability of services as other end-users, but by different means.

13) Definitions need to be adjusted so as to conform to the principle of technology neutrality and to keep pace with technological development. In particular, conditions for the provision of a service should be separated from the actual definitional elements of a publicly available telephone service, i.e. an electronic communications service made available to the public for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international telephone numbering plan, whether such a service is based on circuit switching or packet switching technology. It is the nature of such a service that it is bidirectional, enabling both the parties to communicate. A service which does not fulfil all these conditions, such as for example a 'click-through' application on a customer service website, is not a publicly available telephone service. Publicly available telephone services also include means of communication specifically intended for disabled end-users using text relay or total conversation services.

14) It is necessary to clarify that the indirect provision of services could include situations where originating is made via carrier selection or pre-selection or where a service provider resells or re-brands publicly available telephone services provided by another undertaking.

15) As a result of technological and market evolution, networks are increasingly moving to 'Internet Protocol' (IP) technology, and consumers are increasingly able to choose between a range of competing voice service providers. Therefore, Member States should be able to separate universal service obligations concerning the provision of a connection to the public communications network at a fixed location from the provision of a publicly available telephone service. Such separation should not affect the scope of universal service obligations defined and reviewed at Community level.

16) In accordance with the principle of subsidiarity, it is for the Member States to decide on the basis of objective criteria which undertakings are designated as universal service providers, where appropriate taking into account the ability and the willingness of undertakings to accept all or part of the universal service obligations. This does not preclude that Member States may include, in the designation process, specific conditions justified on grounds of efficiency, including, inter alia, grouping geographical areas or components or setting minimum periods for the designation.

17) National regulatory authorities should be able to monitor the evolution and level of retail tariffs for services that fall under the scope of universal service obligations, even where a Member State has not yet designated an undertaking to provide universal service. In such a case, the monitoring should be carried out in such a way that it would not represent an excessive administrative burden for either national regulatory authorities or undertakings providing such service.

18) Redundant obligations designed to facilitate the transition from the regulatory framework of 1998 to that of 2002 should be deleted, together with other provisions that overlap with and duplicate those laid down in Directive 2002/21/EC (Framework Directive).

19) The requirement to provide a minimum set of leased lines at retail level, which was necessary to ensure the continued application of provisions of the regulatory framework of 1998 in the field of leased lines, which was not sufficiently competitive at the time the 2002 framework entered into force, is no longer necessary and should be repealed.

20) To continue to impose carrier selection and carrier pre-selection directly in Community legislation could hamper technological progress. These remedies should rather be imposed by national regulatory authorities as a result of market analysis carried out in accordance with the procedures set out in Directive 2002/21/EC (Framework Directive) and through the obligations referred to in Article 12 of Directive 2002/19/EC (Access Directive).

21) Provisions on contracts should apply not only to consumers but also to other end-users, primarily micro enterprises and small and medium-sized enterprises (SMEs), which may prefer a contract adapted to consumer needs. To avoid unnecessary administrative burdens for providers and the complexity related to the definition of SMEs, the provisions on contracts should not apply automatically to those other end-users, but only where they so request. Member States should take appropriate measures to promote awareness amongst SMEs of this possibility.

22) As a consequence of technological developments, other types of identifiers may be used in the future, in addition to ordinary forms of numbering identification.

23) Providers of electronic communications services that allow calls should ensure that their customers are adequately informed as to whether or not access to emergency services is provided and of any limitation on service (such as a limitation on the provision of caller location information or the routing of emergency calls). Such providers should also provide their customers with clear and transparent information in the initial contract and in the event of any change in the access provision, for example in billing.
information. This information should include any limitations on territorial coverage, on the basis of the planned technical operating parameters of the service and the available infrastructure. Where the service is not provided over a switched telephony network, the information should also include the level of reliability of the access and of caller location information compared to a service that is provided over a switched telephony network, taking into account current technology and quality standards, as well as any quality of service parameters specified under Directive 2002/22/EC (Universal Service Directive).

(24) With respect to terminal equipment, the customer contract should specify any restrictions imposed by the provider on the use of the equipment, such as by way of ‘SIM-locking’ mobile devices, if such restrictions are not prohibited under national legislation, and any charges due on termination of the contract, whether before or on the agreed expiry date, including any cost imposed in order to retain the equipment.

(25) Without imposing any obligation on the provider to take action over and above what is required under Community law, the customer contract should also specify the type of action, if any, the provider might take in case of security or integrity incidents, threats or vulnerabilities.

(26) In order to address public interest issues with respect to the use of communications services and to encourage protection of the rights and freedoms of others, the relevant national authorities should be able to produce and have disseminated, with the aid of providers, public interest information related to the use of such services. This could include public interest information regarding copyright infringement, other unlawful uses and the dissemination of harmful content, and advice and means of protection against risks to personal security, which may for example arise from disclosure of personal information in certain circumstances, as well as risks to privacy and personal data, and the availability of easy-to-use and configurable software or software options allowing protection for children or vulnerable persons. The information could be coordinated by way of the cooperation procedure established in Article 33(3) of Directive 2002/22/EC (Universal Service Directive). Such public interest information should be updated whenever necessary and should be presented in easily comprehensible printed and electronic formats, as determined by each Member State, and on national public authority websites. National regulatory authorities should be able to oblige providers to disseminate this standardised information to all their customers in a manner deemed appropriate by the national regulatory authorities. When required by Member States, the information should also be included in contracts. Dissemination of such information should however not impose an excessive burden on undertakings. Member States should require this dissemination by the means used by undertakings in communications with subscribers made in the ordinary course of business.

(27) The right of subscribers to withdraw from their contracts without penalty refers to modifications in contractual conditions which are imposed by the providers of electronic communications networks and/or services.

(28) End-users should be able to decide what content they want to send and receive, and which services, applications, hardware and software they want to use for such purposes, without prejudice to the need to preserve the integrity and security of networks and services. A competitive market will provide users with a wide choice of content, applications and services. National regulatory authorities should promote users’ ability to access and distribute information and to run applications and services of their choice, as provided for in Article 8 of Directive 2002/21/EC (Framework Directive). Given the increasing importance of electronic communications for consumers and businesses, users should in any case be fully informed of any limiting conditions imposed on the use of electronic communications services by the service and/or network provider. Such information should, at the option of the provider, specify the type of content, application or service concerned, individual applications or services, or both. Depending on the technology used and the type of limitation, such limitations may require user consent under Directive 2002/58/EC (Directive on privacy and electronic communications).

(29) Directive 2002/22/EC (Universal Service Directive) neither mandates nor prohibits conditions imposed by providers, in accordance with national law, limiting end-users’ access to and/or use of services and applications, but lays down an obligation to provide information regarding such conditions. Member States wishing to implement measures regarding end-users’ access to and/or use of services and applications must respect the fundamental rights of citizens, including in relation to privacy and due process, and any such measures should take full account of policy goals defined at Community level, such as furthering the development of the Community information society.

(30) Directive 2002/22/EC (Universal Service Directive) does not require providers to monitor information transmitted over their networks or to bring legal proceedings against their customers on grounds of such information, nor does it make providers liable for that information. Responsibility for punitive action or criminal prosecution is a matter for national law, respecting fundamental rights and freedoms, including the right to due process.
(31) In the absence of relevant rules of Community law, content, applications and services are deemed lawful or harmful in accordance with national substantive and procedural law. It is a task for the Member States, not for providers of electronic communications networks or services, to decide, in accordance with due process, whether content, applications or services are lawful or harmful. The Framework Directive and the Specific Directives are without prejudice to Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (1), which, inter alia, contains a ‘mere conduit’ rule for intermediary service providers, as defined therein.

directories, as well as their right, free of charge, not to be included in a public subscriber directory, as provided for in Directive 2002/58/EC (Directive on privacy and electronic communications). Customers should also be informed of systems which allow information to be included in the directory database but which do not disclose such information to users of directory services.

(32) The availability of transparent, up-to-date and comparable information on offers and services is a key element for consumers in competitive markets where several providers offer services. End-users and consumers of electronic communications services should be able to easily compare the prices of various services offered on the market based on information published in an easily accessible form. In order to allow them to make price comparisons easily, national regulatory authorities should be able to require from undertakings providing electronic communications networks and/or services greater transparency as regards information (including tariffs, consumption patterns and other relevant statistics) and to ensure that third parties have the right to use, without charge, publicly available information published by such undertakings. National regulatory authorities should also be able to make price guides available, in particular where the market has not provided them free of charge or at a reasonable price. Undertakings should not be entitled to any remuneration for the use of information where it has already been published and thus belongs in the public domain. In addition, end-users and consumers should be adequately informed of the price and the type of service offered before they purchase a service, in particular if a freephone number is subject to additional charges. National regulatory authorities should be able to require that such information is provided generally, and, for certain categories of services determined by them, immediately prior to connecting the call, unless otherwise provided for by national law. When determining the categories of call requiring pricing information prior to connection, national regulatory authorities should take due account of the nature of the service, the pricing conditions which apply to it and whether it is offered by a provider who is not a provider of electronic communications services. Without prejudice to Directive 2000/31/EC (Directive on electronic commerce), undertakings should also, if required by Member States, provide subscribers with public interest information produced by the relevant public authorities regarding, inter alia, the most common infringements and their legal consequences.

(33) Customers should be informed of their rights with respect to the use of their personal information in subscriber directories and in particular of the purpose or purposes of such directories. A competitive market should ensure that end-users enjoy the quality of service they require, but in particular cases it may be necessary to ensure that public communications networks attain minimum quality levels so as to prevent degradation of service, the blocking of access and the slowing of traffic over networks. In order to meet quality of service requirements, operators may use procedures to measure and shape traffic on a network link so as to avoid filling the link to capacity or overfilling the link, which would result in network congestion and poor performance. Those procedures should be subject to scrutiny by the national regulatory authorities, acting in accordance with the Framework Directive and the Specific Directives and in particular by addressing discriminatory behaviour, in order to ensure that they do not restrict competition. If appropriate, national regulatory authorities may also impose minimum quality of service requirements on undertakings providing public communications networks to ensure that services and applications dependent on the network are delivered at a minimum quality standard, subject to examination by the Commission. National regulatory authorities should be empowered to take action to address degradation of service, including the hindering or slowing down of traffic, to the detriment of consumers. However, since inconsistent remedies can impair the functioning of the internal market, the Commission should assess any requirements intended to be set by national regulatory authorities for possible regulatory intervention across the Community and, if necessary, issue comments or recommendations in order to achieve consistent application.

(34) In future IP networks, where provision of a service may be separated from provision of the network, Member States should determine the most appropriate steps to be taken to ensure the availability of publicly available telephone services provided using public communications networks and uninterrupted access to emergency services in the event of catastrophic network breakdown or in cases of force majeure, taking into account the priorities of different types of subscriber and technical limitations.

In order to ensure that disabled end-users benefit from competition and the choice of service providers enjoyed by the majority of end-users, relevant national authorities should specify, where appropriate and in light of national conditions, consumer protection requirements to be met by undertakings providing publicly available electronic communications services. Such requirements may include, in particular, that undertakings ensure that disabled end-users take advantage of their services on equivalent terms and conditions, including prices and tariffs, as those offered to their other end-users, irrespective of any additional costs incurred by them. Other requirements may relate to wholesale arrangements between undertakings.

Operator assistance services cover a range of different services for end-users. The provision of such services should be left to commercial negotiations between providers of public communications networks and operator assistance services, as is the case for any other customer support service, and it is not necessary to continue to mandate their provision. The corresponding obligation should therefore be repealed.

Directory enquiry services should be, and frequently are, provided under competitive market conditions, pursuant to Article 5 of Commission Directive 2002/77/EC of 16 September 2002 on competition in the markets for electronic communications networks and services (1). Wholesale measures ensuring the inclusion of end-user data (both fixed and mobile) in databases should comply with the safeguards for the protection of personal data, including Article 12 of Directive 2002/58/EC (Directive on privacy and electronic communications). The cost-oriented supply of that data to service providers, with the possibility for Member States to establish a centralised mechanism for providing comprehensive aggregated information to directory providers, and the provision of network access under reasonable and transparent conditions, should be put in place in order to ensure that end-users benefit fully from competition, with the ultimate aim of enabling the removal of retail regulation from these services and the provision of offers of directory services under reasonable and transparent conditions.

End-users should be able to call and access the emergency services using any telephone service capable of originating voice calls through a number or numbers in national telephone numbering plans. Member States that use national emergency numbers besides ‘112’ may impose on undertakings similar obligations for access to such national emergency numbers. Emergency authorities should be able to handle and answer calls to the number ‘112’ at least as expeditiously and effectively as calls to national emergency numbers. It is important to increase awareness of ‘112’ in order to improve the level of protection and security of citizens travelling in the European Union. To this end, citizens should be made fully aware, when travelling in any Member State, in particular through information provided in international bus terminals, train stations, ports or airports and in telephone directories, payphone kiosks, subscriber and billing material, that ‘112’ can be used as a single emergency number throughout the Community. This is primarily the responsibility of the Member States, but the Commission should continue both to support and to supplement initiatives of the Member States to heighten awareness of ‘112’ and periodically to evaluate the public’s awareness of it. The obligation to provide caller location information should be strengthened so as to increase the protection of citizens. In particular, undertakings should make caller location information available to emergency services as soon as the call reaches that service independently of the technology used. In order to respond to technological developments, including those leading to increasingly accurate caller location information, the Commission should be empowered to adopt technical implementing measures to ensure effective access to ‘112’ services in the Community for the benefit of citizens. Such measures should be without prejudice to the organisation of emergency services of Member States.

Member States should ensure that undertakings providing end-users with an electronic communications service designed for originating calls through a number or numbers in a national telephone numbering plan provide reliable and accurate access to emergency services, taking into account national specifications and criteria. Network-independent undertakings may not have control over networks and may not be able to ensure that emergency calls made through their service are routed with the same reliability, as they may not be able to guarantee service availability, given that problems related to infrastructure are not under their control. For network-independent undertakings, caller location information may not always be technically feasible. Once internationally-recognised standards ensuring accurate and reliable routing and connection to the emergency services are in place, network-independent undertakings should also fulfil the obligations related to caller location information at a level comparable to that required of other undertakings.

(42) Development of the international code ‘3883’ (the European Telephony Numbering Space (ETNS)) is currently hindered by insufficient awareness, overly bureaucratic procedural requirements and, in consequence, lack of demand. In order to encourage the development of ETNS, the Member States to which the International Telecommunications Union has assigned the international code ‘3883’ should, following the example of the implementation of the ‘.eu’ top-level domain, delegate responsibility for its management, number assignment and promotion to an existing separate organisation, designated by the Commission on the basis of an open, transparent and non-discriminatory selection procedure. That organisation should also have the task of developing proposals for public service applications using ETNS for common European services, such as a common number for reporting thefts of mobile terminals.

(43) Considering the particular aspects related to reporting missing children and the currently limited availability of such a service, Member States should not only reserve a number, but also make every effort to ensure that a service for reporting missing children is actually available in their territories under the number ‘116000’, without delay. To that end, Member States should, if appropriate, inter alia, organise tendering procedures in order to invite interested parties to provide that service.

(44) Voice calls remain the most robust and reliable form of access to emergency services. Other means of contact, such as text messaging, may be less reliable and may suffer from lack of immediacy. Member States should, however, if they deem it appropriate, be free to promote the development and implementation of other means of access to emergency services which are capable of ensuring access equivalent to voice calls.

(45) Pursuant to its Decision 2007/116/EC of 15 February 2007 on reserving the national numbering range beginning with ‘116’ for harmonised numbers for harmonised services of social value (¹), the Commission has asked Member States to reserve numbers in the ‘116’ numbering range for certain services of social value. The appropriate provisions of that Decision should be reflected in Directive 2002/22/EC (Universal Service Directive) in order to integrate them more firmly into the regulatory framework for electronic communications networks and services and to facilitate access by disabled end-users.

(46) A single market implies that end-users are able to access all numbers included in the national numbering plans of other Member States and to access services using non-geographic numbers within the Community, including, among others, freephone and premium rate numbers. End-users should also be able to access numbers from the European Telephone Numbering Space (ETNS) and Universal International Freephone Numbers (UIFN). Cross-border access to numbering resources and associated services should not be prevented, except in objectively justified cases, for example to combat fraud or abuse (e.g. in connection with certain premium-rate services), when the number is defined as having a national scope only (e.g. a national short code) or when it is technically or economically unfeasible. Users should be fully informed in advance and in a clear manner of any charges applicable to freephone numbers, such as international call charges for numbers accessible through standard international dialling codes.

(47) In order to take full advantage of the competitive environment, consumers should be able to make informed choices and to change providers when it is in their interests. It is essential to ensure that they can do so without being hindered by legal, technical or practical obstacles, including contractual conditions, procedures, charges and so on. This does not preclude the imposition of reasonable minimum contractual periods in consumer contracts. Number portability is a key facilitator of consumer choice and effective competition in competitive markets for electronic communications and should be implemented with the minimum delay, so that the number is functionally activated within one working day and the user does not experience a loss of service lasting longer than one working day. Competent national authorities may prescribe the global process of the porting of numbers, taking into account national provisions on contracts and technological developments. Experience in certain Member States has shown that there is a risk of consumers being switched to another provider without having given their consent. While that is a matter that should primarily be addressed by law enforcement authorities, Member States should be able to impose such minimum proportionate measures regarding the switching process, including appropriate sanctions, as are necessary to minimise such risks, and to ensure that consumers are protected throughout the switching process without making the process less attractive for them.

(48) Legal ‘must-carry’ obligations may be applied to specified radio and television broadcast channels and complementary services supplied by a specified media service provider. Member States should provide a clear justification for the ‘must carry’ obligations in their national law so as to ensure that such obligations are transparent, proportionate and properly defined. In that regard, ‘must carry’ rules should be designed in a way which provides sufficient incentives for efficient investment in infrastructure. ‘Must carry’ rules should be periodically reviewed in order to keep them up-to-date with technological and market evolution and in order to ensure that they continue to be proportionate to the objectives to be achieved. Complementary services include, but are not limited to, services designed to improve accessibility for end-users with disabilities, such as video-text, subtitling, audio description and sign language.

(49) In order to overcome existing shortcomings in terms of consumer consultation and to appropriately address the interests of citizens, Member States should put in place an appropriate consultation mechanism. Such a mechanism could take the form of a body which would, independently of the national regulatory authority and service providers, carry out research into consumer-related issues, such as consumer behaviour and mechanisms for changing suppliers, and which would operate in a transparent manner and contribute to the existing mechanisms for stakeholder consultation. Furthermore, a mechanism could be established for the purpose of enabling appropriate cooperation on issues relating to the promotion of lawful content. Any cooperation procedures agreed pursuant to such a mechanism should, however, not allow for the systematic surveillance of Internet usage.

(50) Universal service obligations imposed on an undertaking designated as having universal service obligations should be notified to the Commission.

(51) Directive 2002/58/EC (Directive on privacy and electronic communications) provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, in particular the right to privacy and the right to confidentiality, with respect to the processing of personal data in the electronic communications sector, and to ensure the free movement of such data and of electronic communications equipment and services in the Community. Where measures aiming to ensure that terminal equipment is constructed so as to safeguard the protection of personal data and privacy are adopted pursuant to Directive 1999/5/EC or Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and telecommunications (\(^{(1)}\)), such measures should respect the principle of technology neutrality.

(52) Developments concerning the use of IP addresses should be followed closely, taking into consideration the work already done by, among others, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of 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 (\(^{(2)}\)), and in the light of such proposals as may be appropriate.

(53) The processing of traffic data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious acts that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by providers of security technologies and services when acting as data controllers is subject to Article 7(6) of Directive 95/46/EC. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communications systems.

(54) The liberalisation of electronic communications networks and services markets and rapid technological development have combined to boost competition and economic growth and resulted in a rich diversity of end-user services accessible via public electronic communications networks. It is necessary to ensure that consumers and users are afforded the same level of protection of privacy and personal data, regardless of the technology used to deliver a particular service.

(55) In line with the objectives of the regulatory framework for electronic communications networks and services and with the principles of proportionality and subsidiarity, and for the purposes of legal certainty and efficiency for European businesses and national regulatory authorities alike, Directive 2002/58/EC (Directive on privacy and electronic communications) focuses on public electronic communications networks and services, and does not apply to closed user groups and corporate networks.

(56) Technological progress allows the development of new applications based on devices for data collection and identification, which could be contactless devices using radio frequencies. For example, Radio Frequency Identification Devices (RFIDs) use radio frequencies to capture data from uniquely identified tags which can then be transferred over existing communications networks. The wide use of such technologies can bring considerable economic and social benefit and thus make a powerful contribution to the internal market, if their use is acceptable to citizens. To achieve this aim, it is necessary to ensure that all fundamental rights of individuals, including the right to privacy and data protection, are safeguarded. When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply.

(57) The provider of a publicly available electronic communications service should take appropriate technical and organisational measures to ensure the security of its services. Without prejudice to Directive 95/46/EC, such measures should ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, and that the personal data stored or transmitted, as

\(^{(1)}\) OJ L 36, 7.2.1987, p. 31.
\(^{(2)}\) OJ L 281, 23.11.1995, p. 31.
well as the network and services, are protected. Moreover, a security policy with respect to the processing of personal data should be established in order to identify vulnerabilities in the system, and monitoring and preventive, corrective and mitigating action should be regularly carried out.

(58) The competent national authorities should promote the interests of citizens by, inter alia, contributing to ensuring a high level of protection of personal data and privacy. To this end, competent national authorities should have the necessary means to perform their duties, including comprehensive and reliable data about security incidents that have led to the personal data of individuals being compromised. They should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services. Providers should therefore maintain an inventory of personal data breaches to enable further analysis and evaluation by the competent national authorities.

(59) Community law imposes duties on data controllers regarding the processing of personal data, including an obligation to implement appropriate technical and organisational protection measures against, for example, loss of data. The data breach notification requirements contained in Directive 2002/58/EC (Directive on privacy and electronic communications) provide a structure for notifying the competent authorities and individuals concerned when personal data has nevertheless been compromised. Those notification requirements are limited to security breaches which occur in the electronic communications sector. However, the notification of security breaches reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised, as well as of available or advisable precautions that they could take in order to minimise the possible economic loss or social harm that could result from such failures. The interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority. Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), regardless of the sector, or the type, of data concerned.

(60) Competent national authorities should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services.

(61) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the subscriber or individual concerned. Therefore, as soon as the provider of publicly available electronic communications services becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The subscribers or individuals whose data and privacy could be adversely affected by the breach should be notified without delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community. The notification should include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned.

(62) When implementing measures transposing Directive 2002/58/EC (Directive on privacy and electronic communications), the authorities and courts of the Member States should not only interpret their national law in a manner consistent with that Directive, but should also ensure that they do not rely on an interpretation of it which would conflict with fundamental rights or general principles of Community law, such as the principle of proportionality.

(63) Provision should be made for the adoption of technical implementing measures concerning the circumstances, format and procedures applicable to information and notification requirements in order to achieve an adequate level of privacy protection and security of personal data transmitted or processed in connection with the use of electronic communications networks in the internal market.

(64) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(65) Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party (spyware) poses a serious threat to the privacy of users, as do viruses. A high and equal level of protection of the private sphere of users needs to be ensured, regardless of whether unwanted
spying programmes or viruses are inadvertently downloaded via electronic communications networks or are delivered and installed in software distributed on other external data storage media, such as CDs, CD-ROMS or USB keys. Member States should encourage the provision of information to end-users about available precautions, and should encourage them to take the necessary steps to protect their terminal equipment against viruses and spyware.

(66) Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.

(67) Safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications.

(68) Electronic communications service providers make substantial investments in order to combat unsolicited commercial communications (spam). They are also in a better position than end-users in that they possess the knowledge and resources necessary to detect and identify spammers. E-mail service providers and other service providers should therefore be able to initiate legal action against spammers, and thus defend the interests of their customers, as part of their own legitimate business interests.

(69) The need to ensure an adequate level of protection of privacy and personal data transmitted and processed in connection with the use of electronic communications networks in the Community calls for effective implementation and enforcement powers in order to provide adequate incentives for compliance. Competent national authorities and, where appropriate, other relevant national bodies should have sufficient powers and resources to investigate cases of non-compliance effectively, including powers to obtain any relevant information they might need, to decide on complaints and to impose sanctions in cases of non-compliance.

(70) The implementation and enforcement of the provisions of this Directive often require cooperation between the national regulatory authorities of two or more Member States, for example in combating cross-border spam and spyware. In order to ensure smooth and rapid cooperation in such cases, procedures relating for example to the quantity and format of information exchanged between authorities, or deadlines to be complied with, should be defined by the relevant national authorities, subject to examination by the Commission. Such procedures will also allow the resulting obligations of market actors to be harmonised, contributing to the creation of a level playing field in the Community.

(71) Cross-border cooperation and enforcement should be reinforced in line with existing Community cross-border enforcement mechanisms, such as that laid down in Regulation (EC) No 2006/2004 (the Regulation on consumer protection cooperation) (1), by way of an amendment to that Regulation.


(73) In particular, the Commission should be empowered to adopt implementing measures on effective access to ‘112’ services, as well as to adapt the Annexes to technical progress or changes in market demand. It should also be empowered to adopt implementing measures concerning information and notification requirements and security of processing. Since those measures are of general scope and are designed to amend non-essential elements of Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) by supplementing them with new non-essential elements, they must be adopted in accordance with the regulatory procedure with scrutiny provided for in Article 5a of Decision 1999/468/EC. Given that the conduct of the regulatory procedure with scrutiny within the normal time limits could, in certain exceptional situations, impede the timely adoption of implementing measures, the European Parliament, the Council and the Commission should act speedily in order to ensure the timely adoption of those measures.

When adopting implementing measures on security of processing, the Commission should consult all relevant European authorities and organisations (the European Network and Information Security Agency (ENISA), the European Data Protection Supervisor and the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC), as well as all other relevant stakeholders, particularly in order to be informed of the best available technical and economic means of improving the implementation of Directive 2002/58/EC (Directive on privacy and electronic communications).

Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) should therefore be amended accordingly.

In accordance with point 34 of the Interinstitutional Agreement on better law-making (1), Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications) and the transposition measures, and to make them public.

H ave A dopted t his D irective:

Article 1

Amendments to Directive 2002/22/EC (Universal Service Directive)

Directive 2002/22/EC (Universal Service Directive) is hereby amended as follows:

1) Article 1 shall be replaced by the following:

‘Article 1

Subject-matter and scope

1. Within the framework of Directive 2002/21/EC (Framework Directive), this Directive concerns the provision of electronic communications networks and services to end-users. The aim is to ensure the availability throughout the Community of good-quality publicly available services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market. The Directive also includes provisions concerning certain aspects of terminal equipment, including provisions intended to facilitate access for disabled end-users.

2. This Directive establishes the rights of end-users and the corresponding obligations of undertakings providing publicly available electronic communications networks and services. With regard to ensuring provision of universal service within an environment of open and competitive markets, this Directive defines the minimum set of services of specified quality to which all end-users have access, at an affordable price in the light of specific national conditions, without distorting competition. This Directive also sets out obligations with regard to the provision of certain mandatory services.

3. This Directive neither mandates nor prohibits conditions, imposed by providers of publicly available electronic communications and services, limiting end-users’ access to, and/or use of, services and applications, where allowed under national law and in conformity with Community law, but lays down an obligation to provide information regarding such conditions. National measures regarding end-users’ access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, including in relation to privacy and due process, as defined in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

4. The provisions of this Directive concerning end-users’ rights shall apply without prejudice to Community rules on consumer protection, in particular Directives 93/13/EEC and 97/7/EC, and national rules in conformity with Community law:·

2) Article 2 shall be amended as follows:

(a) point (b) shall be deleted;

(b) points (c) and (d) shall be replaced by the following:

‘(c) “publicly available telephone service” means a service made available to the public for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international telephone numbering plan;

(d) “geographic number” means a number from the national telephone numbering plan where part of its digit structure contains geographic significance used for routing calls to the physical location of the network termination point (NTP);’;

(c) point (e) shall be deleted;

(d) point (f) shall be replaced by the following:

‘(f) “non-geographic number” means a number from the national telephone numbering plan that is not a geographic number. It includes, inter alia, mobile, freephone and premium rate numbers:’;

3) Article 4 shall be replaced by the following:

'Article 4

Provision of access at a fixed location and provision of telephone services

1. Member States shall ensure that all reasonable requests for connection at a fixed location to a public communications network are met by at least one undertaking.

2. The connection provided shall be capable of supporting voice, facsimile and data communications at data rates that are sufficient to permit functional Internet access, taking into account prevailing technologies used by the majority of subscribers and technological feasibility.

3. Member States shall ensure that all reasonable requests for the provision of a publicly available telephone service over the network connection referred to in paragraph 1 that allows for originating and receiving national and international calls are met by at least one undertaking.';

4) Article 5(2) shall be replaced by the following:

'2. The directories referred to in paragraph 1 shall comprise, subject to the provisions of Article 12 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (\(^\text{1}\)), all subscribers of publicly available telephone services.

\(^\text{1}\) OJ L 201, 31.7.2002, p. 37.‘;

5) the title of Article 6 and Article 6(1) shall be replaced by the following:

'Public pay telephones and other public voice telephony access points

1. Member States shall ensure that national regulatory authorities may impose obligations on undertakings in order to ensure that public pay telephones or other public voice telephony access points are provided to meet the reasonable needs of end-users in terms of the geographical coverage, the number of telephones or other access points, accessibility to disabled end-users and the quality of services.';

6) Article 7 shall be replaced by the following:

'Article 7

Measures for disabled end-users

1. Unless requirements have been specified under Chapter IV which achieve the equivalent effect, Member States shall take specific measures to ensure that access to, and affordability of, the services identified in Article 4(3) and Article 5 for disabled end-users is equivalent to the level enjoyed by other end-users. Member States may oblige national regulatory authorities to assess the general need and the specific requirements, including the extent and concrete form of such specific measures for disabled end-users.

2. Member States may take specific measures, in the light of national conditions, to ensure that disabled end-users can also take advantage of the choice of undertakings and service providers available to the majority of end-users.

3. In taking the measures referred to in paragraphs 1 and 2, Member States shall encourage compliance with the relevant standards or specifications published in accordance with Articles 17 and 18 of Directive 2002/21/EC (Framework Directive).

7) in Article 8, the following paragraph shall be added:

'3. When an undertaking designated in accordance with paragraph 1 intends to dispose of a substantial part or all of its local access network assets to a separate legal entity under different ownership, it shall inform in advance the national regulatory authority in a timely manner, in order to allow that authority to assess the effect of the intended transaction on the provision of access at a fixed location and of telephone services pursuant to Article 4. The national regulatory authority may impose, amend or withdrew specific obligations in accordance with Article 6(2) of Directive 2002/20/EC (Authorisation Directive).‘;

8) Article 9(1) and (2) shall be replaced by the following:

'1. National regulatory authorities shall monitor the evolution and level of retail tariffs of the services identified in Articles 4 to 7 as falling under the universal service obligations and either provided by designated undertakings or available on the market, if no undertakings are designated in relation to those services, in particular in relation to national consumer prices and income.

2. Member States may, in the light of national conditions, require that designated undertakings provide to consumers tariff options or packages which depart from those provided under normal commercial conditions, in particular to ensure that those on low incomes or with special social needs are not prevented from accessing the network referred to in Article 4(1) or from using the services identified in Article 4(3) and Articles 5, 6 and 7 as falling under the universal service obligations and provided by designated undertakings.’;
9) Article 11(4) shall be replaced by the following:

‘4. National regulatory authorities shall be able to set performance targets for undertakings with universal service obligations. In so doing, national regulatory authorities shall take account of views of interested parties, in particular as referred to in Article 33;’

10) the title of Chapter III shall be replaced by the following:

‘REGULATORY CONTROLS ON UNDERTAKINGS WITH SIGNIFICANT MARKET POWER IN SPECIFIC RETAIL MARKETS’;

11) Article 16 shall be deleted;

12) Article 17 shall be amended as follows:

(a) paragraph 1 shall be replaced by the following:

‘1. Member States shall ensure that national regulatory authorities impose appropriate regulatory obligations on undertakings identified as having significant market power on a given retail market in accordance with Article 14 of Directive 2002/21/EC (Framework Directive) where:

(a) as a result of a market analysis carried out in accordance with Article 16 of Directive 2002/21/EC (Framework Directive), a national regulatory authority determines that a given retail market identified in accordance with Article 15 of that Directive is not effectively competitive; and

(b) the national regulatory authority concludes that obligations imposed under Articles 9 to 13 of Directive 2002/19/EC (Access Directive) would not result in the achievement of the objectives set out in Article 8 of Directive 2002/21/EC (Framework Directive);’;

(b) paragraph 3 shall be deleted;

13) Articles 18 and 19 shall be deleted;

14) Articles 20 to 23 shall be replaced by the following:

‘Article 20

Contracts

1. Member States shall ensure that, when subscribing to services providing connection to a public communications network and/or publicly available electronic communications services, consumers, and other end-users so requesting, have a right to a contract with an undertaking or undertakings providing such connection and/or services. The contract shall specify in a clear, comprehensive and easily accessible form at least:

(a) the identity and address of the undertaking;

(b) the services provided, including in particular,

— whether or not access to emergency services and caller location information is being provided, and any limitations on the provision of emergency services under Article 26,

— information on any other conditions limiting access to and/or use of services and applications, where such conditions are permitted under national law in accordance with Community law,

— the minimum service quality levels offered, namely the time for the initial connection and, where appropriate, other quality of service parameters, as defined by the national regulatory authorities,

— information on any procedures put in place by the undertaking to measure and shape traffic so as to avoid filling or overfilling a network link, and information on how those procedures could impact on service quality,

— the types of maintenance service offered and customer support services provided, as well as the means of contacting these services,

— any restrictions imposed by the provider on the use of terminal equipment supplied;

(c) where an obligation exists under Article 25, the subscriber’s options as to whether or not to include his or her personal data in a directory, and the data concerned;

(d) details of prices and tariffs, the means by which up-to-date information on all applicable tariffs and maintenance charges may be obtained, payment methods offered and any differences in costs due to payment method;

(e) the duration of the contract and the conditions for renewal and termination of services and of the contract, including:

— any minimum usage or duration required to benefit from promotional terms,

— any charges related to portability of numbers and other identifiers,

— any charges due on termination of the contract, including any cost recovery with respect to terminal equipment,

(f) any compensation and the refund arrangements which apply if contracted service quality levels are not met;
(g) the means of initiating procedures for the settlement of disputes in accordance with Article 34;

(h) the type of action that might be taken by the undertaking in reaction to security or integrity incidents or threats and vulnerabilities.

Member States may also require that the contract include any information which may be provided by the relevant public authorities for this purpose on the use of electronic communications networks and services to engage in unlawful activities or to disseminate harmful content, and on the means of protection against risks to personal security, privacy and personal data, referred to in Article 21(4) and relevant to the service provided.

2. Member States shall ensure that subscribers have a right to withdraw from their contract without penalty upon notice of modification to the contractual conditions proposed by the undertakings providing electronic communications networks and/or services. Subscribers shall be given adequate notice, not shorter than one month, of any such modification, and shall be informed at the same time of their right to withdraw, without penalty, from their contract if they do not accept the new conditions. Member States shall ensure that national regulatory authorities are able to specify the format of such notifications.

Article 21

Transparency and publication of information

1. Member States shall ensure that national regulatory authorities are able to oblige undertakings providing public electronic communications networks and/or publicly available electronic communications services to publish transparent, comparable, adequate and up-to-date information on applicable prices and tariffs, on any charges due on termination of a contract and on standard terms and conditions in respect of access to, and use of, services provided by them to end-users and consumers in accordance with Annex II. Such information shall be published in a clear, comprehensive and easily accessible form. National regulatory authorities may specify additional requirements regarding the form in which such information is to be published.

2. National regulatory authorities shall encourage the provision of comparable information to enable end-users and consumers to make an independent evaluation of the cost of alternative usage patterns, for instance by means of interactive guides or similar techniques. Where such facilities are not available on the market free of charge or at a reasonable price, Member States shall ensure that national regulatory authorities are able to make such guides or techniques available themselves or through third party procurement. Third parties shall have a right to use, free of charge, the information published by undertakings providing electronic communications networks and/or publicly available electronic communications services for the purposes of selling or making available such interactive guides or similar techniques.

3. Member States shall ensure that national regulatory authorities are able to oblige undertakings providing public electronic communications networks and/or publicly available electronic communications services to inter alia:

(a) provide applicable tariff information to subscribers regarding any number or service subject to particular pricing conditions; with respect to individual categories of services, national regulatory authorities may require such information to be provided immediately prior to connecting the call;

(b) inform subscribers of any change to access to emergency services or caller location information in the service to which they have subscribed;

(c) inform subscribers of any change to conditions limiting access to and/or use of services and applications, where such conditions are permitted under national law in accordance with Community law;

(d) provide information on any procedures put in place by the provider to measure and shape traffic so as to avoid filling or overfilling a network link, and on how those procedures could impact on service quality;

(e) inform subscribers of their right to determine whether or not to include their personal data in a directory, and of the types of data concerned, in accordance with Article 12 of Directive 2002/58/EC (Directive on privacy and electronic communications); and

(f) regularly inform disabled subscribers of details of products and services designed for them.

If deemed appropriate, national regulatory authorities may promote self- or co-regulatory measures prior to imposing any obligation.

4. Member States may require that the undertakings referred to in paragraph 3 distribute public interest information free of charge to existing and new subscribers, where appropriate, by the same means as those ordinarily used by them in their communications with subscribers. In such a case, that information shall be provided by the relevant public authorities in a standardised format and shall, inter alia, cover the following topics:

(a) the most common uses of electronic communications services to engage in unlawful activities or to disseminate harmful content, particularly where it may prejudice respect for the rights and freedoms of others, including infringements of copyright and related rights, and their legal consequences; and
(b) the means of protection against risks to personal security, privacy and personal data when using electronic communications services.

Article 22

Quality of service

1. Member States shall ensure that national regulatory authorities are, after taking account of the views of interested parties, able to require undertakings that provide publicly available electronic communications networks and/or services to publish comparable, adequate and up-to-date information for end-users on the quality of their services and on measures taken to ensure equivalence in access for disabled end-users. That information shall, on request, be supplied to the national regulatory authority in advance of its publication.

2. National regulatory authorities may specify, inter alia, the quality of service parameters to be measured and the content, form and manner of the information to be published, including possible quality certification mechanisms, in order to ensure that end-users, including disabled end-users, have access to comprehensive, comparable, reliable and user-friendly information. Where appropriate, the parameters, definitions and measurement methods set out in Annex III may be used.

3. In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks.

National regulatory authorities shall provide the Commission, in good time before setting any such requirements, with a summary of the grounds for action, the envisaged requirements and the proposed course of action. This information shall also be made available to the Body of European Regulators for Electronic Communications (BEREC). The Commission may, having examined such information, make comments or recommendations thereupon, in particular to ensure that the envisaged requirements do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the requirements.

Article 23

Availability of services

Member States shall take all necessary measures to ensure the fullest possible availability of publicly available telephone services provided over public communications networks in the event of catastrophic network breakdown or in cases of force majeure. Member States shall ensure that undertakings providing publicly available telephone services take all necessary measures to ensure uninterrupted access to emergency services;

15) the following Article shall be inserted:

‘Article 23a

Ensuring equivalence in access and choice for disabled end-users

1. Member States shall enable relevant national authorities to specify, where appropriate, requirements to be met by undertakings providing publicly available electronic communication services to ensure that disabled end-users:

(a) have access to electronic communications services equivalent to that enjoyed by the majority of end-users; and

(b) benefit from the choice of undertakings and services available to the majority of end-users.

2. In order to be able to adopt and implement specific arrangements for disabled end-users, Member States shall encourage the availability of terminal equipment offering the necessary services and functions;

16) Article 25 shall be amended as follows:

(a) the title shall be replaced by the following:

‘Telephone directory enquiry services';

(b) paragraph 1 shall be replaced by the following:

‘1. Member States shall ensure that subscribers to publicly available telephone services have the right to have an entry in the publicly available directory referred to in Article 5(1)(a) and to have their information made available to providers of directory enquiry services and/or directories in accordance with paragraph 2;'

(c) paragraphs 3, 4 and 5 shall be replaced by the following:

‘3. Member States shall ensure that all end-users provided with a publicly available telephone service can access directory enquiry services. National regulatory authorities shall be able to impose obligations and conditions on undertakings that control access of end-users for the provision of directory enquiry services in accordance with the provisions of Article 5 of Directive 2002/19/EC (Access Directive). Such obligations and conditions shall be objective, equitable, non-discriminatory and transparent.'
4. Member States shall not maintain any regulatory restrictions which prevent end-users in one Member State from accessing directly the directory enquiry service in another Member State by voice call or SMS, and shall take measures to ensure such access in accordance with Article 28.

5. Paragraphs 1 to 4 shall apply subject to the requirements of Community legislation on the protection of personal data and privacy and, in particular, Article 12 of Directive 2002/58/EC (Directive on privacy and electronic communications).

17) Articles 26 and 27 shall be replaced by the following:

‘Article 26

Emergency services and the single European emergency call number

1. Member States shall ensure that all end-users of the service referred to in paragraph 2, including users of public pay telephones, are able to call the emergency services free of charge and without having to use any means of payment, by using the single European emergency call number “112” and any national emergency call number specified by Member States.

2. Member States, in consultation with national regulatory authorities, emergency services and providers, shall ensure that undertakings providing end-users with an electronic communications service for originating national calls to a number or numbers in a national telephone numbering plan provide access to emergency services.

3. Member States shall ensure that calls to the single European emergency call number “112” are appropriately answered and handled in the manner best suited to the national organisation of emergency systems. Such calls shall be answered and handled at least as expeditiously and effectively as calls to the national emergency number or numbers, where these continue to be in use.

4. Member States shall ensure that access for disabled end-users to emergency services is equivalent to that enjoyed by other end-users. Measures taken to ensure that disabled end-users are able to access emergency services whilst travelling in other Member States shall be based to the greatest extent possible on European standards or specifications published in accordance with the provisions of Article 17 of Directive 2002/21/EC (Framework Directive), and they shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in this Article.

5. Member States shall ensure that undertakings concerned make caller location information available free of charge to the authority handling emergency calls as soon as the call reaches that authority. This shall apply to all calls to the single European emergency call number “112”. Member States may extend this obligation to cover calls to national emergency numbers. Competent regulatory authorities shall lay down criteria for the accuracy and reliability of the caller location information provided.

6. Member States shall ensure that citizens are adequately informed about the existence and use of the single European emergency call number “112”, in particular through initiatives specifically targeting persons travelling between Member States.

7. In order to ensure effective access to “112” services in the Member States, the Commission, having consulted BEREC, may adopt technical implementing measures. However, these technical implementing measures shall be adopted without prejudice to, and shall have no impact on, the organisation of emergency services, which remains the exclusive competence of Member States.

Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 37(2).

‘Article 27

European telephone access codes

1. Member States shall ensure that the “00” code is the standard international access code. Special arrangements for making calls between locations adjacent to one another across borders between Member States may be established or continued. End-users in the locations concerned shall be fully informed of such arrangements.

2. A legal entity, established within the Community and designated by the Commission, shall have sole responsibility for the management, including number assignment, and promotion of the European Telephony Numbering Space (ETNS). The Commission shall adopt the necessary implementing rules.

3. Member States shall ensure that all undertakings that provide publicly available telephone services allowing international calls handle all calls to and from the ETNS at rates similar to those applied for calls to and from other Member States.”

18) the following Article shall be inserted:

‘Article 27a

Harmonised numbers for harmonised services of social value, including the missing children hotline number

1. Member States shall promote the specific numbers in the numbering range beginning with “116” identified by Commission Decision 2007/116/EC of 15 February 2007
on reserving the national numbering range beginning with "116" for harmonised numbers for harmonised services of social value (¹). They shall encourage the provision within their territory of the services for which such numbers are reserved.

2. Member States shall ensure that disabled end-users are able to access services provided under the "116" numbering range to the greatest extent possible. Measures taken to facilitate disabled end-users' access to such services whilst travelling in other Member States shall be based on compliance with relevant standards or specifications published in accordance with Article 17 of Directive 2002/21/EC (Framework Directive).

3. Member States shall ensure that citizens are adequately informed of the existence and use of services provided under the "116" numbering range, in particular through initiatives specifically targeting persons travelling between Member States.

4. Member States shall, in addition to measures of general applicability to all numbers in the "116" numbering range taken pursuant to paragraphs 1, 2, and 3, make every effort to ensure that citizens have access to a service operating a hotline to report cases of missing children. The hotline shall be available on the number "116000".

5. In order to ensure the effective implementation of the "116" numbering range, in particular the missing children hotline number "116000", in the Member States, including access for disabled end-users when travelling in other Member States, the Commission, having consulted BEREC, may adopt technical implementing measures. However, these technical implementing measures shall be adopted without prejudice to, and shall have no impact on, the organisation of these services, which remains of the exclusive competence of Member States.

Those measures, designed to amend non-essential elements of this Directive by suppletively it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 37(2).


19) Article 28 shall be replaced by the following:

'Article 28

Access to numbers and services

1. Member States shall ensure that, where technically and economically feasible, and except where a called subscriber has chosen for commercial reasons to limit access by calling parties located in specific geographical areas, relevant national authorities take all necessary steps to ensure that end-users are able to:

(a) access and use services using non-geographic numbers within the Community; and

(b) access all numbers provided in the Community, regardless of the technology and devices used by the operator, including those in the national numbering plans of Member States, those from the ETNS and Universal International Freephone Numbers (UIFN).

2. Member States shall ensure that the relevant authorities are able to require undertakings providing public communications networks and/or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues;'

20) Article 29 shall be amended as follows:

(a) paragraph 1 shall be replaced by the following:

'1. Without prejudice to Article 10(2), Member States shall ensure that national regulatory authorities are able to require all undertakings that provide publicly available telephone services and/or access to public communications networks to make available all or part of the additional facilities listed in Part B of Annex I, subject to technical feasibility and economic viability, as well as all or part of the additional facilities listed in Part A of Annex I;'

(b) paragraph 3 shall be deleted;

21) Article 30 shall be replaced by the following:

'Article 30

Facilitating change of provider

1. Member States shall ensure that all subscribers with numbers from the national telephone numbering plan who so request can retain their number(s) independently of the undertaking providing the service in accordance with the provisions of Part C of Annex I.

2. National regulatory authorities shall ensure that pricing between operators and/or service providers related to the provision of number portability is cost-oriented, and that direct charges to subscribers, if any, do not act as a disincentive for subscribers against changing service provider.

3. National regulatory authorities shall not impose retail tariffs for the porting of numbers in a manner that would distort competition, such as by setting specific or common retail tariffs.
4. Porting of numbers and their subsequent activation shall be carried out within the shortest possible time. In any case, subscribers who have concluded an agreement to port a number to a new undertaking shall have that number activated within one working day.

Without prejudice to the first subparagraph, competent national authorities may establish the global process of porting of numbers, taking into account national provisions on contracts, technical feasibility and the need to maintain continuity of service to the subscriber. In any event, loss of service during the process of porting shall not exceed one working day. Competent national authorities shall also take into account, where necessary, measures ensuring that subscribers are protected throughout the switching process and are not switched to another provider against their will.

Member States shall ensure that appropriate sanctions on undertakings are provided for, including an obligation to compensate subscribers in case of delay in porting or abuse of porting by them or on their behalf.

5. Member States shall ensure that contracts concluded between consumers and undertakings providing electronic communications services do not mandate an initial commitment period that exceeds 24 months. Member States shall also ensure that undertakings offer users the possibility to subscribe to a contract with a maximum duration of 12 months.

6. Without prejudice to any minimum contractual period, Member States shall ensure that conditions and procedures for contract termination do not act as a disincentive against changing service provider;.

22) Article 31(1) shall be replaced by the following:

‘1. Member States may impose reasonable “must carry” obligations, for the transmission of specified radio and television broadcast channels and complementary services, particularly accessibility services to enable appropriate access for disabled end-users, on undertakings under their jurisdiction providing electronic communications networks used for the distribution of radio or television broadcast channels to the public where a significant number of end-users of such networks use them as their principal means to receive radio and television broadcast channels. Such obligations shall only be imposed where they are necessary to meet general interest objectives as clearly defined by each Member State and shall be proportionate and transparent.

The obligations referred to in the first subparagraph shall be reviewed by the Member States at the latest within one year of 25 May 2011, except where Member States have carried out such a review within the previous two years.

Member States shall review "must carry" obligations on a regular basis;.

23) Article 33 shall be amended as follows:

(a) paragraph 1 shall be replaced by the following:

‘1. Member States shall ensure as far as appropriate that national regulatory authorities take account of the views of end-users, consumers (including, in particular, disabled consumers), manufacturers and undertakings that provide electronic communications networks and/or services on issues related to all end-user and consumer rights concerning publicly available electronic communications services, in particular where they have a significant impact on the market.

In particular, Member States shall ensure that national regulatory authorities establish a consultation mechanism ensuring that in their decisions on issues related to end-user and consumer rights concerning publicly available electronic communications services, due consideration is given to consumer interests in electronic communications;.

(b) the following paragraph shall be added:

‘3. Without prejudice to national rules in conformity with Community law promoting cultural and media policy objectives, such as cultural and linguistic diversity and media pluralism, national regulatory authorities and other relevant authorities may promote cooperation between undertakings providing electronic communications networks and/or services and sectors interested in the promotion of lawful content in electronic communication networks and services. That cooperation may also include coordination of the public interest information to be provided pursuant to Article 21(4) and the second subparagraph of Article 20(1);.

24) Article 34(1) shall be replaced by the following:

‘1. Member States shall ensure that transparent, non-discriminatory, simple and inexpensive out-of-court procedures are available for dealing with unresolved disputes between consumers and undertakings providing electronic communications networks and/or services arising under this Directive and relating to the contractual conditions and/or performance of contracts concerning the supply of those networks and/or services. Member States shall adopt measures to ensure that such procedures enable disputes to be settled fairly and promptly and may, where warranted, adopt a system of reimbursement and/or compensation. Such procedures shall enable disputes to be settled impartially and shall not deprive the consumer of the legal protection afforded by national law. Member States may extend these obligations to cover disputes involving other end-users;.
25) Article 35 shall be replaced by the following:

'Article 35

Adaptation of annexes

Measures designed to amend non-essential elements of this Directive and necessary to adapt Annexes I, II, III, and VI to technological developments or changes in market demand shall be adopted by the Commission in accordance with the regulatory procedure with scrutiny referred to in Article 37(2).'

26) Article 36(2) shall be replaced by the following:

'2. National regulatory authorities shall notify to the Commission the universal service obligations imposed upon undertakings designated as having universal service obligations. Any changes affecting these obligations or of the undertakings affected under the provisions of this Directive shall be notified to the Commission without delay.'

27) Article 37 shall be replaced by the following:

'Article 37

Committee procedure

1. The Commission shall be assisted by the Communications Committee set up under Article 22 of Directive 2002/21/EC (Framework Directive).

2. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.'

28) Annexes I, II, III shall be replaced by the text appearing in Annex I to this Directive, and Annex VI shall be replaced by the text appearing in Annex II to this Directive;

29) Annex VII shall be deleted.

Article 2

Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications)

Directive 2002/58/EC (Directive on privacy and electronic communications) is hereby amended as follows:

1) Article 1(1) shall be replaced by the following:

'1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.'

2) Article 2 shall be amended as follows:

(a) point (c) shall be replaced by the following:

'(c) “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;'

(b) point (e) shall be deleted;

(c) the following point shall be added:

'(h) “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.'

3) Article 3 shall be replaced by the following:

'Article 3

Services concerned

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.'

4) Article 4 shall be amended as follows:

(a) the title shall be replaced by the following:

'Security of processing';

(b) the following paragraph shall be inserted:

'1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

— ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

— protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,
— ensure the implementation of a security policy with respect to the processing of personal data,

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.);

(c) the following paragraphs shall be added:

‘3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Without prejudice to the provider’s obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which

the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so.

Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.

5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article.

Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2);

5) Article 5(3) shall be replaced by the following:

‘3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service;’;

6) Article 6(3) shall be replaced by the following:

‘3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or
marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.’;

7) Article 13 shall be replaced by the following:

‘Article 13
Unsolicited communications

1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.

4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2). Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.’;

8) the following Article shall be inserted:

‘Article 14a
Committee procedure

1. The Commission shall be assisted by the Communications Committee established by Article 22 of Directive 2002/21/EC (Framework Directive).

2. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof;

9) in Article 15, the following paragraph shall be inserted:

‘1b. Providers shall establish internal procedures for responding to requests for access to users’ personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.’;

10) the following Article shall be inserted:

‘Article 15a
Implementation and enforcement

1. Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.
2. Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.

3. Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

4. The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows.

The national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures.°

Article 3

Amendment to Regulation (EC) No 2006/2004

In the Annex to Regulation (EC) No 2006/2004 (the Regulation on consumer protection cooperation), the following point shall be added:


Article 4

Transposition

1. Member States shall adopt and publish by 25 May 2011 the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of those measures.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 5

Entry into force

This Directive shall enter into force on the day following its publication in the Official Journal of the European Union.

Article 6

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 25 November 2009.

For the European Parliament
The President
J. BUZEK

For the Council
The President
Á. TORSTENSSON
ANNEX I

ANNEX I

DESCRIPTION OF FACILITIES AND SERVICES REFERRED TO IN ARTICLE 10 (CONTROL OF EXPENDITURE), ARTICLE 29 (ADDITIONAL FACILITIES) AND ARTICLE 30 (FACILITATING CHANGE OF PROVIDER)

Part A: Facilities and services referred to in Article 10

(a) Itemised billing

Member States are to ensure that national regulatory authorities, subject to the requirements of relevant legislation on the protection of personal data and privacy, may lay down the basic level of itemised bills which are to be provided by undertakings to subscribers free of charge in order that they can:

(i) allow verification and control of the charges incurred in using the public communications network at a fixed location and/or related publicly available telephone services; and

(ii) adequately monitor their usage and expenditure and thereby exercise a reasonable degree of control over their bills.

Where appropriate, additional levels of detail may be offered to subscribers at reasonable tariffs or at no charge.

Calls which are free of charge to the calling subscriber, including calls to helplines, are not to be identified in the calling subscriber’s itemised bill.

(b) Selective barring for outgoing calls or premium SMS or MMS, or, where technically feasible, other kinds of similar applications, free of charge

i.e. the facility whereby the subscriber can, on request to the designated undertaking that provides telephone services, bar outgoing calls or premium SMS or MMS or other kinds of similar applications of defined types or to defined types of numbers free of charge.

(c) Pre-payment systems

Member States are to ensure that national regulatory authorities may require designated undertakings to provide means for consumers to pay for access to the public communications network and use of publicly available telephone services on pre-paid terms.

(d) Phased payment of connection fees

Member States are to ensure that national regulatory authorities may require designated undertakings to allow consumers to pay for connection to the public communications network on the basis of payments phased over time.

(e) Non-payment of bills

Member States are to authorise specified measures, which are to be proportionate, non-discriminatory and published, to cover non-payment of telephone bills issued by undertakings. These measures are to ensure that due warning of any consequent service interruption or disconnection is given to the subscriber beforehand. Except in cases of fraud, persistent late payment or non-payment, these measures are to ensure, as far as is technically feasible that any service interruption is confined to the service concerned. Disconnection for non-payment of bills should take place only after due warning is given to the subscriber. Member States may allow a period of limited service prior to complete disconnection, during which only calls that do not incur a charge to the subscriber (e.g. ‘112’ calls) are permitted.
(i) **Tariff advice**

i.e. the facility whereby subscribers may request the undertaking to provide information regarding alternative lower-cost tariffs, if available.

(g) **Cost control**

i.e. the facility whereby undertakings offer other means, if determined to be appropriate by national regulatory authorities, to control the costs of publicly available telephone services, including free-of-charge alerts to consumers in case of abnormal or excessive consumption patterns.

**Part B: Facilities referred to in Article 29**

(a) **Tone dialling or DTMF (dual-tone multi-frequency operation)**

i.e. the public communications network and/or publicly available telephone services supports the use of DTMF tones as defined in ETSI ETR 207 for end-to-end signalling throughout the network both within a Member State and between Member States.

(b) **Calling-line identification**

i.e. the calling party's number is presented to the called party prior to the call being established.

This facility should be provided in accordance with relevant legislation on protection of personal data and privacy, in particular Directive 2002/58/EC (Directive on privacy and electronic communications).

To the extent technically feasible, operators should provide data and signals to facilitate the offering of calling-line identity and tone dialling across Member State boundaries.

**Part C: Implementation of the number portability provisions referred to in Article 30**

The requirement that all subscribers with numbers from the national numbering plan, who so request can retain their number(s) independently of the undertaking providing the service shall apply:

(a) in the case of geographic numbers, at a specific location; and

(b) in the case of non-geographic numbers, at any location.

This Part does not apply to the porting of numbers between networks providing services at a fixed location and mobile networks.

---

**ANNEX II**

**INFORMATION TO BE PUBLISHED IN ACCORDANCE WITH ARTICLE 21**

**(TRANSPARENCY AND PUBLICATION OF INFORMATION)**

The national regulatory authority has a responsibility to ensure that the information in this Annex is published, in accordance with Article 21. It is for the national regulatory authority to decide which information is to be published by the undertakings providing public communications networks and/or publicly available telephone services and which information is to be published by the national regulatory authority itself, so as to ensure that consumers are able to make informed choices.

1. Name(s) and address(es) of undertaking(s)

   i.e. names and head office addresses of undertakings providing public communications networks and/or publicly available telephone services.

2. Description of services offered

2.1. Scope of services offered
2.2. Standard tariffs indicating the services provided and the content of each tariff element (e.g. charges for access, all types of usage charges, maintenance charges), and including details of standard discounts applied and special and targeted tariff schemes and any additional charges, as well as costs with respect to terminal equipment.

2.3. Compensation/refund policy, including specific details of any compensation/refund schemes offered.

2.4. Types of maintenance service offered.

2.5. Standard contract conditions, including any minimum contractual period, termination of the contract and procedures and direct charges related to the portability of numbers and other identifiers, if relevant.

3. Dispute settlement mechanisms, including those developed by the undertaking.

4. Information about rights as regards universal service, including, where appropriate, the facilities and services mentioned in Annex I.

---

ANNEX III

QUALITY OF SERVICE PARAMETERS

Quality-of-Service Parameters, Definitions and Measurement Methods referred to in Articles 11 and 22

For undertakings providing access to a public communications network

<table>
<thead>
<tr>
<th>PARAMETER (Note 1)</th>
<th>DEFINITION</th>
<th>MEASUREMENT METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply time for initial connection</td>
<td>ETSI EG 202 057</td>
<td>ETSI EG 202 057</td>
</tr>
<tr>
<td>Fault rate per access line</td>
<td>ETSI EG 202 057</td>
<td>ETSI EG 202 057</td>
</tr>
<tr>
<td>Fault repair time</td>
<td>ETSI EG 202 057</td>
<td>ETSI EG 202 057</td>
</tr>
</tbody>
</table>

For undertakings providing a publicly available telephone service

| Call set up time (Note 2)               | ETSI EG 202 057| ETSI EG 202 057   |
| Response times for directory enquiry services | ETSI EG 202 057| ETSI EG 202 057   |
| Proportion of coin and card operated public pay-telephones in working order | ETSI EG 202 057| ETSI EG 202 057   |
| Bill correctness complaints             | ETSI EG 202 057| ETSI EG 202 057   |
| Unsuccessful call ratio (Note 2)         | ETSI EG 202 057| ETSI EG 202 057   |

Version number of ETSI EG 202 057-1 is 1.3.1 (July 2008)

Note 1

Parameters should allow for performance to be analysed at a regional level (i.e. no less than level 2 in the Nomenclature of Territorial Units for Statistics (NUTS) established by Eurostat).

Note 2

Member States may decide not to require up-to-date information concerning the performance for these two parameters to be kept if evidence is available to show that performance in these two areas is satisfactory.'
ANNEX II

‘ANNEX VI

INTEROPERABILITY OF DIGITAL CONSUMER EQUIPMENT REFERRED TO IN ARTICLE 24

1. Common scrambling algorithm and free-to-air reception

All consumer equipment intended for the reception of conventional digital television signals (i.e. broadcasting via terrestrial, cable or satellite transmission which is primarily intended for fixed reception, such as DVB-T, DVB-C or DVB-S), for sale or rent or otherwise made available in the Community, capable of descrambling digital television signals, is to possess the capability to:

— allow the descrambling of such signals according to a common European scrambling algorithm as administered by a recognised European standards organisation, currently ETSI,

— display signals that have been transmitted in the clear provided that, in the event that such equipment is rented, the renter is in compliance with the relevant rental agreement.

2. Interoperability for analogue and digital television sets

Any analogue television set with an integral screen of visible diagonal greater than 42 cm which is put on the market for sale or rent in the Community is to be fitted with at least one open interface socket, as standardised by a recognised European standards organisation, e.g. as given in the Cenelec EN 50 049-1:1997 standard, permitting simple connection of peripherals, especially additional decoders and digital receivers.

Any digital television set with an integral screen of visible diagonal greater than 30 cm which is put on the market for sale or rent in the Community is to be fitted with at least one open interface socket (either standardised by, or conforming to a standard adopted by, a recognised European standards organisation, or conforming to an industry-wide specification) e.g. the DVB common interface connector, permitting simple connection of peripherals, and able to pass all the elements of a digital television signal, including information relating to interactive and conditionally accessed services.’