COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 21.9.2005
COM(2005) 438 final

2005/0182 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC

(presented by the Commission)

{SEC(2005) 1131}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Grounds for and objectives of the proposal

Citizens increasingly perform daily activities and transactions using electronic communications networks and services. These communications generate 'traffic data' or 'location data' which include for example details about the location of the caller, the number called, the time and duration of the call. When combined with data enabling the identification of the subscriber or user of the service, the availability of such traffic data is important for purposes related to law enforcement and security, such as the prevention, investigation, detection and prosecution of serious crime, such as terrorism and organised crime.

However, with changes in business models and service offerings, such as the growth of flat rate tariffs, pre-paid and free electronic communications services, traffic data may not always be stored by all operators to the same extent as they were in recent years, depending on the services they offer. This trend is reinforced by recent offerings of Voice over IP communication services, or even flat rate services for fixed telephone communications. Under such arrangements, the operators would no longer have the need to store traffic data for billing purposes. If traffic data are not stored for billing or other business purposes, they will not be available for public authorities whenever there is a legitimate case to access the data. In other words, these developments are making it much harder for public authorities to fulfil their duties in preventing and combating organised crime and terrorism, and easier for criminals to communicate with each other without the fear that their communications data can be used by law enforcement authorities to thwart them.

It has now become urgent to adopt harmonised provisions at EU level on this subject. A certain number of Member States have adopted, or plan to adopt, national measures requiring some or all operators to retain given types of data so that they can be used for the purposes identified above when necessary. Differences in the legal, regulatory, and technical provisions in Member States concerning the retention of traffic data present obstacles to the Internal Market for electronic communications as service providers are faced with different requirements regarding the types of data to be retained as well as the conditions of retention. These provisions should therefore be further harmonised in accordance with Article 14 of the EC-Treaty.

• General context

The necessity to have rules at EU level that guarantee the availability of traffic data for anti-terrorism purposes across the 25 Member States was confirmed by the European Council in its Declaration on combating terrorism of 25 March 2004. Following the Madrid terrorist bombings, the European Council instructed the Council to examine 'proposals for establishing rules on the retention of communications traffic data by service providers' with a view to adoption in 2005. The priority attached to adopting an appropriate legal instrument on this subject was recently confirmed in the Conclusions of the European Council of 16 and 17 June, as

well as at the special JHA Council meeting of 13 July 2005 following the London terrorist bombings.

- **Existing provisions in the area of the proposal**

Directive 2002/58/EC on Privacy and Electronic Communications harmonises through its Articles 6 and 9 the personal data protection rules which are applicable to the processing of traffic and location data generated by the use of electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission, except for the data necessary for billing or interconnection payments; subject to consent, certain data may also be processed for marketing purposes and the provision of value added services. Article 15(1) stipulates that Member States may provide for restrictions of the scope of (amongst others) Articles 5, 6 and 9, when such restrictions constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

- **Consistency with the other policies and objectives of the Union**

The proposal is in line with Community law and with the Charter on Fundamental Rights. Even though it is clear that the proposed Directive will have an effect on the privacy right of citizens as guaranteed under Article 7 of the Charter, as well as on the right to protection of personal data as guaranteed under Article 8 of the Charter, the interference with these rights is justified in accordance with of Article 52 of the Charter. Specifically, the limitations on these rights provided for by the proposal are proportionate and necessary to meet the generally recognised objectives of preventing and combating crime and terrorism.

Furthermore, the proposal limits its effects on the private life of citizens: firstly through clearly establishing the purpose for which the data which are retained can be used, secondly through limiting the categories of data which need to be retained, and thirdly through limiting the period of retention. A further important safeguard is that this Directive is not applicable to the content of communications - this would amount to interception of telecommunications, which falls outside the scope of this legal instrument.

The processing of the personal data retained by the service and network providers under the provisions of this Directive are covered by the general and specific data protection provisions established under Directives 95/46/EC and 2002/58/EC - which means in practice that specific additional provisions on general data protection principles and data security are not necessary. It also means that the processing of such data will be under the full supervisory powers of the data protection authorities established in all Member States.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

Consultation methods, main sectors targeted and general profile of respondents

Starting in 2001 with the meetings of the Cybercrime Forum, the issue of traffic data retention has been the subject of consultation with representatives of law enforcement authorities, the electronic communications industry and data protection experts.

On 14 June 2004, an ad hoc roundtable meeting was organised under the auspices of the Forum for the Prevention of Organised crime, in which representatives from law enforcement, industry and data protection organisations took part. On 30 July 2004, a joint consultation document on traffic data retention was presented by DG INSFO and DG JLS, in preparation of a public workshop on the issue held on 21 September 2004. Contributions and reactions from various sides – in particular from industry and civil rights associations - were received in response to the joint consultation document. The public workshop of 21 September provided further input to the Commission.

In the preparation of the proposal, the Commission has also drawn on the wide-ranging public debate on this issue, including discussions at the European Parliament.

Summary of responses and how they have been taken into account

The consultation process confirmed that retention of traffic communications data is an essential tool for law enforcement authorities to prevent and combat crime and terrorism. Law enforcement authorities indicated that for their purposes, retention periods should be as long as necessary, and comprise as much data as necessary. Especially in complex investigations into serious crimes, which can take up to a number of years to conclude, older traffic data is still regularly required. A number of examples were given of cases where such data had proven to be essential for criminal investigations, mostly into crimes such as bombings or murders.

Representatives of the European representative organisations of the telecommunications and internet industry, as well as individual electronic communications companies, argued that whilst they were willing to co-operate with law enforcement, and had been doing so, long retention periods would generate considerable costs and data preservation would be sufficient. They pleaded anyway for retention periods no longer than six months since a large amount of data requested by law enforcement authorities is not older than six months, and for mechanisms to compensate them for the additional costs incurred.

Representatives from data protection authorities and civil rights associations argued that data retention is an interference with the private life of citizens, which is why retention periods should be kept as short as possible. In general terms, they questioned whether periods of retention longer than six months can be considered to

be proportional. They also expressed concerns about the finality and aims of the retention, which should be clearly specified.

The current proposal constitutes a balanced approach and rests on the enclosed impact assessment. The retention periods of 1 year for mobile and fixed telephony traffic data and six months for traffic data related to Internet usage will cover the main needs of law enforcement, whilst limiting the associated costs for industry and the intrusion into the private life of citizens. A retention period of six months for all data would have been too short, since even if a large part of the requests from law enforcement authorities relate to data not older than six months, data older than six months is generally requested in relation with the most serious offences, such as terrorism, organised crime or homicide.

- **Collection and use of expertise**

There was no need for external expertise.

- **Impact assessment**

Various options have been considered. In 2002, the Council had explicitly called for a dialogue at national and EU level aimed at finding solutions to the issue of traffic data retention that satisfies both the need for effective tools for prevention, detection, investigation and prosecution of criminal offences and the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy, data protection and secrecy of correspondence. Although public consultation and debate on this issue has been wide-spread, including discussions at the European Parliament, no common solutions have emerged from this.

Not taking an initiative on data retention would leave the current patchwork of data retention provisions in place. Soft law has been discarded since it does not provide for the right level of legal certainty. A third pillar initiative on data retention obligations was discarded since it would have been incompatible with existing Community law. A legislative approach has also been called for by the European Council in its Declaration on combating terrorism.

The option of a proposal for a directive provides the harmonisation level needed in the internal market. Compared to a regulation, it leaves in a sensitive area some margin of manoeuvre to Member States on the implementation. A regulation would have been too stringent, notably in view of the different technical architectures used by the various operators in different countries. The directive will leave sufficient margin to Member States to adapt to national constraints. In any case, the status quo is no longer tenable in view of the obstacles to the free provision of services created by the diverging national provisions in this area. The choice for this legal instrument, and the specific legal basis of Article 95 EC, have also been indicated through the legal analysis laid down in Commission Staff Working Paper SEC(2005) 420 of 22 March 2005. The Commission carried out an impact assessment, available on http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3. LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed action**

The proposed Directive is intended to harmonise obligations for providers of publicly available electronic communications services or of a public communications network to retain certain traffic data, so that they may be provided to the competent authorities of the Member States for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.

- **Legal basis**

Article 95 of the EC-Treaty.

- **Subsidiarity principle**

The subsidiarity principle applies insofar as the proposal does not fall under the exclusive competence of the Community.

The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reason(s).

Harmonisation of retention periods for traffic data cannot be achieved by the Member States themselves. EU action – which was called for by the European Council - will ensure that traffic data will be retained across the European Union and can be made available to law enforcement authorities.

As the effectiveness of law enforcement investigations is heavily dependant on international co-operation, and different national choices have negative effects of different national choices on the electronic communications market, European wide harmonisation of traffic data retention schemes is the most appropriate policy choice. The cost reimbursement principle will allow creating a level playing field for the electronic communication providers in the internal market.

Community action will better achieve the objectives of the proposal for the following reason(s).

EU action will better achieve the objectives of the proposal through ensuring that traffic data will be retained across the European Union and can be made available to law enforcement authorities under the same conditions. This will also be of benefit to the electronic communications industry, especially those companies offering services in multiple Member States, since they can standardise their technology.

The qualitative indicators which demonstrate that the objective can better be achieved by the Union are the effectiveness of law enforcement authorities in preventing and combating crime and terrorism, in particular in cases like organised crime and terrorism which are often cross border.

The proposal is limited to what Member States cannot satisfactorily achieve and what the Union does better through its limitation to the scope of the retention obligations on providers of electronic communications services or of a publicly available communications network. The proposal leaves the choice to the Member States of which authorities should have access to data retained and under which conditions. Access to and exchange of information between relevant law enforcement authorities is a matter which falls outside the scope of the EC-Treaty.

In this context it is worth mentioning that the Commission is currently preparing draft legislative proposals under the Treaty on European Union relating to the principle of availability of information for law enforcement purposes and to the establishment of data protection principles for the Third Pillar. It should further be noted that no access should be granted to 'retained data' under this Directive for other than law enforcement purposes i.e. no access to retained data for service providers of electronic communications.

The proposal therefore complies with the subsidiarity principle.

- **Proportionality principle**

The proposal complies with the proportionality principle as its impact on citizens and industry has been limited to the maximum extent possible. It should be recalled that this instrument deals only with traffic data which is processed by the providers of electronic communications. The content of the electronic communications is excluded from the scope of this Directive.

The respect of fundamental rights and freedoms, and in particular the right to life, and the strict limitation of the invasion of privacy has been the key driver to find the most appropriate balance between all interests involved, such as the social, economical, security and privacy context.

Therefore this proposal for a Directive has taken account of the issues of proportionality, most notably in terms of the retention periods proposed, the distinction between telephone and internet data, the limitation in the categories of data to be retained, and the cost reimbursement scheme. In particular the proposal strictly limits the purposes for which the retained data may be provided to law enforcement authorities. Data protection legislation will be fully applicable to the retained data, whereas the impact on individual rights and economic operators is limited by choosing a limited set of traffic data that needs to be retained. Furthermore the shorter retention period for traffic data generated through use of the Internet, as opposed to traffic data generated by usage of 'standard' mobile and fixed telephony takes into account current business practices by substantially reducing the volumes of data that needs to be retained.

The financial and administrative burden on national governments, economic operators and citizens has been minimised in a number of ways. Firstly, the Directive provides for harmonisation, which will mean reduced costs of compliance for providers of electronic communications services or of a public communications network. Secondly, costs have been minimised through strict limitations in the retention periods, as well as in the data sets to be retained. Given the importance of the measure in terms of preventing and combating crime and terrorism, the additional

costs to be borne by the Member States through the provision on cost reimbursement are considered to be proportionate (see the impact assessment).

It should also be highlighted that this Directive does not prejudge the possibility of Member States to request for specific data preservation measures for instance in case a suspect or criminal organisation has already been identified or in the event of specific events such as terrorist attacks.

- **Choice of instruments**

Proposed instruments: directive.

Other means would not be adequate for the following reason(s).

This issue of the correct legal basis for a proposal on traffic data retention has recently been addressed in a Commission Staff Working Paper. In short, the position outlined in this document is that the issue of retention of traffic data has already been dealt with in previous legal instruments based on a first-pillar legal basis, such as Directives 2002/58/EC and 95/46/EC mentioned above. The analysis continues to state that it was only due to the fact that no political agreement on the actual length of retention could be reached that this issue was not harmonised more fully in Directive 2002/58/EC, and concludes that therefore any further legal instruments on retention of traffic data as such (as opposed to provision regulating the exchange of and access to such data by law enforcement) must also take place on a first pillar legal basis. This logic is in accordance with Article 47 of the Treaty on European Union, which regulates the relationship between the Treaty on European Union and the EC Treaty, stipulating that no legal instruments adopted under the Treaty on European Union may affect the legislative framework adopted under the EC Treaty.

4. BUDGETARY IMPLICATION

The proposal has no implication for the Community budget.

5. ADDITIONAL INFORMATION

- **Review/revision/sunset clause**

The proposal includes a review clause. To assist the Commission in its reviewing task the creation of a Platform on data retention is envisaged. Such a group could bring together technical experts on electronic communications, as well as representatives from law enforcement and data protection authorities.

- **Correlation table**

The Member States are required to communicate to the Commission the text of national provisions transposing the Directive as well as a correlation table between those provisions and this Directive.

2005/0182 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC

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[1],

Having regard to the opinion of the European Economic and Social Committee[2],

Having regard to the opinion of the Committee of the Regions[3],

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

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data[4] requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector[5] translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

(3) Articles 5, 6 and 9 of Directive 2002/58/EC define the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments; subject to consent, certain data may also be processed for marketing purposes and the provision of value added services.

---

1 OJ C […], […], p. […].
2 OJ C […], […], p. […].
3 OJ C […], […], p. […].
4 OJ L 281, 23.11.1995, p. 31.
5 OJ L 201, 30.7.2002, p. 37.

(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1)(2)(3) and (4), and Article 9 of the Directive; any such derogations need to be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security) defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

(5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably.

(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.

(7) The Conclusions of the Justice and Home Affairs Council of 20 September 2001 call for ensuring that law enforcement authorities are able to investigate criminal acts which involve the use of electronic communications and to take legal measures against perpetrators of these crimes, while striking a balance between the protection of personal data and the needs of law enforcement authorities to gain access to data for criminal investigation purposes.

(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications is particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.

(9) The Declaration on combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(10) The declaration adopted by the special informal Council of 13 July 2005 reinforces the need to adopt measures related to the retention of electronic communications traffic data as soon as possible.

(11) Given the importance of traffic data for the prevention, investigation, detection, and prosecution of serious criminal offences, such as terrorism and organised crime, as demonstrated by research and the practical experience of several Member States, there is a need to ensure that data which are processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a certain period of time.

(12) The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious

offences involved and the level of invasion of privacy they will cause; the applicable retention period of one year, respectively six months where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.

(13) Given the fact that retention of data generates significant additional costs for electronic communication providers, whilst the benefits in terms of public security impact on society in general, it is appropriate to foresee that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission envisages to create a platform composed of representatives of the law enforcement authorities, associations of the electronic communications industry and data protection authorities.

(15) It should be recalled that Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive; Article 30(1)(c) of Directive 95/46/EC requires the consultation of the 'Article 29 Working Party'.

(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.

(17) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[6].

(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(19) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union; in particular, this Directive together with Directive 2002/58/EC, seeks to ensure full respect of the fundamental rights to respect the private life and communications of citizens and the protection of personal data (Articles 7 and 8 of the Charter),

---

6 OJ L 184, 17.7.1999, p. 23.

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Subject matter and scope

1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications network with respect to the processing and retention of certain data, in order to ensure that the data is available for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.

2. This Directive shall apply to traffic and location data of both private and legal persons, as well as the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2
Definitions

1. For the purpose of this Directive the definitions in Directive 95/46/EC, in Directive 2002/21/EC [7], as well as in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

a) 'data' means traffic data and location data, as well as the related data necessary to identify the subscriber or user;

b) 'user' means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service.

Article 3
Obligation to retain data

1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying communication services are retained in accordance with the provisions of this Directive.

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention,

[7] OJ L 108, 24.4.2002, p. 33.

investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.

Article 4
Categories of data to be retained

Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication;

(b) data necessary to trace and identify the destination of a communication;

(c) data necessary to identify the date, time and duration of a communication;

(d) data necessary to identify the type of communication;

(e) data necessary to identify the communication device or what purports to be the communication device;

(f) data necessary to identify the location of mobile communication equipment.

The types of data to be retained under the abovementioned categories of data are specified in the Annex.

Article 5
Revision of the annex

The Annex shall be revised on a regular basis as necessary in accordance with the procedure referred to in Article 6(2).

Article 6
Committee

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

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

3. The period laid down in Article 5(6) of Decision 1999/468/EC shall be three months.

Article 7
Periods of retention

Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of one year from the date of the communication, with the exception of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of six months.

Article 8
Storage requirements for retained data

Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9
Statistics

Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis. Such statistics shall include

– the cases in which information has been provided to the competent authorities in accordance with applicable national law,

– the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data;

– the cases where requests for data could not be met.

Such statistics shall not contain personal data.

Article 10
Costs

Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.

Article 11
Amendment of Directive 2002/58/EC

In Article 15 of Directive 2002/58/EC the following paragraph 1a is inserted:

”1a. Paragraph 1 shall not apply to obligations relating to the retention of data for the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, deriving from Directive 2005/../EC*. * OJ L nr. …. of ….”.

Article 12
Evaluation

1. Not later than three years from the date referred to in Article 13(1), the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account the statistical elements provided to the Commission pursuant to

Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to the period of retention provided for in Article 7.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

Article 13
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [no later than 15 months after its adoption at the latest]. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

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 14
Entry into force

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

Article 15
Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

Annex

Types of data to be retained under the categories identified in Article 4 of this Directive:

a) Data necessary to trace and identify the source of a communication:

(1) Concerning Fixed Network Telephony:

(a) The calling telephone number;

(b) Name and address of the subscriber or registered user;

(2) Concerning Mobile Telephony:

(a) The calling telephone number;

(b) Name and Address of the subscriber or registered user;

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

(a) The Internet Protocol (IP) address, whether dynamic or static, allocated by the Internet access provider to a communication;

(b) The User ID of the source of a communication;

(c) The Connection Label or telephone number allocated to any communication entering the public telephone network;

(d) Name and address of the subscriber or registered user to whom the IP address, Connection Label or User ID was allocated at the time of the communication.

b) Data necessary to trace and identify the destination of a communication:

(1) Concerning Fixed Network Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(2) Concerning Mobile Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

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

(a) The Connection Label or User ID of the intended recipient(s) of a communication;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s) who are the intended recipient(s) of the communication.

c) Data necessary to identify the date, time and duration of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony:

(a) The date and time of the start and end of the communication.

(2) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The date and time of the log-in and log-off of the Internet sessions based on a certain time zone.

d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony:

(a) The telephone service used, e.g. voice, conference call, fax and messaging services.

(2) Concerning Mobile Telephony:

(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service.

e) Data necessary to identify the communication device or what purports to be the communication device:

(1) Concerning Mobile Telephony:

(a) The International Mobile Subscriber Identity (IMSI) of the calling and called party;

(b) The International Mobile Equipment Identity (IMEI) of the calling and called party.

(2) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The calling telephone number for dial-up access;

(b) The digital subscriber line (DSL) or other end point identifier of the originator of the communication;

(c) The media access control (MAC) address or other machine identifier of the originator of the communication.

f) Data necessary to identify the location of mobile communication equipment:

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

(2) Data mapping between Cell IDs and their geographical location at the start and end of the communication.