



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 19 December 2005

15691/05

**Interinstitutional File:
2005/0182 (COD)**

**CODEC 1176
COPEN 197
TELECOM 146**

NOTE

from: General Secretariat
to: Permanent Representatives Committee/Council
Subject: Proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provisions of public electronic communication services and amending Directive 2002/58/EC
– Outcome of the European Parliament's first reading
(Strasbourg, 12 to 15 December 2005)

I. INTRODUCTION

In accordance with the provisions of Article 251(2) of the EC Treaty and the joint declaration on practical arrangements for the codecision procedure¹, a number of informal contacts have taken place between the Council, the European Parliament and the Commission with a view to reaching an agreement on this dossier at first reading, thereby avoiding the need for a second reading and conciliation.

In this context, the PPE-ED and PSE political groups presented 42 compromise amendments to the proposal for the directive. These amendments had been agreed during the informal contacts referred to above.

¹ OJ C 148, 28.5.1999, p.1.

II. VOTE

The plenary adopted the 42 compromise amendments to the proposal for the directive. All other amendments tabled to the proposal for the directive were rejected by the plenary. The amendments adopted correspond to what was agreed between the three institutions and ought therefore to be acceptable to the Council. Consequently, once the legal linguists¹ have scrutinized the text, the Council should be in a position to adopt the legislative act.

The text of the amendments adopted and the European Parliament legislative resolution are annexed to this note.

¹ Delegations with legal-linguistic observations can send them to the secretariat of the Council's legal-linguistic service (secretariat.jl-codecision@consilium.eu.int) until 13.1.2006.

Data retention ***I

European Parliament legislative resolution on the 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 (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

(Codecision procedure: first reading)

The European Parliament,

- having regard to the Commission proposal to the European Parliament and the Council (COM(2005)0438)¹,
 - having regard to Article 251(2) and Article 95 of the EC Treaty, pursuant to which the Commission submitted the proposal to Parliament (C6-0293/2005),
 - having regard to Rule 51 of its Rules of Procedure,
 - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Industry, Research and Energy and the Committee on the Internal Market and Consumer Protection (A6-0365/2005),
1. Approves the Commission proposal as amended;
 2. Calls on the Commission for an impact assessment study covering all internal market and consumer protection issues;
 3. Considers that, concerning access to data, the present directive constitutes just a necessary first step and calls on the Council for loyal cooperation for the swift adoption of appropriate guarantees in the context of the framework decision on data protection and data treatment in judicial and police co-operation in criminal matters;
 4. Considers that the Member States have the right to apply their national constitutional principles and considers especially that professional secrecy will also be respected in the application of the present directive;
 3. Calls on the Commission to refer the matter to Parliament again if it intends to amend the proposal substantially or replace it with another text;
 4. Instructs its President to forward its position to the Council and Commission.

¹ Not yet published in the OJ.

Amendment 51

RECITAL 7

(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.

deleted

Amendment 52

RECITAL 9 a (new)

(9a) Under Article 8 of the European Convention of Human Rights, everyone has the right to respect for his private life and his correspondence. Interference by a public authority with the exercise of that right may only be made in accordance with the law and if it is necessary in a democratic society, inter alia, in the interests of national security, public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proven to be such a necessary and effective investigative tool for law enforcement in investigations in several Member States and in particular into serious cases such as organized crime and terrorism, it is therefore necessary to ensure availability of retained data to law enforcement for a certain period of time under the conditions provided for in the present Directive. The adoption of an instrument on data retention is therefore a necessary measure in accordance with the requirements of Article 8 of the European

Convention of Human Rights.

Amendment 53
RECITAL 10

(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.

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

Amendment 54
RECITAL 11

(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.

(11) Given the importance of traffic data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure *at a European level* 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 *under the conditions provided for in the present Directive*.

Amendment 55
RECITAL 12

(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.

deleted

Amendment 56
RECITAL 12 a (new)

(12a) Article 15(1) of Directive 2002/58/EC would continue to apply in relation to data, including data related to unsuccessful call attempts, which are not specifically required to be retained under the present Directive and therefore fall outside the scope of this Directive, and for retention for purposes, including judicial purposes, other than that covered by this Directive.

Amendment 57
RECITAL 13

(13) Given the fact that retention of data generates significant additional costs for electronic communications 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.

(13) This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that is the content of the information communicated. Retention of data should be done in a way avoiding data to be retained more than once. Generating or processing data, when supplying the communications services concerned (Article 3), refers to data which is accessible. In particular when retaining data related to Internet e-mail and Internet Telephony, the scope may be limited to the providers' own services or the network providers'.

Amendment 58
RECITAL 14

(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.

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to *obtain advice and encourage the sharing of experience of best practice* on these matters the Commission *intends to establish a group* composed of *Member States'* law enforcement authorities, associations of the electronic communications industry, *European Parliament representatives* and data protection authorities, *including the European Data Protection Supervisor*.

Amendment 59
RECITAL 15 a (new)

(15a) It should also be recalled that the obligations incumbent on service providers concerning measures to ensure data quality which derive from Article 6 of Directive 95/46/EC as well as their obligations concerning measures to ensure confidentiality and security of processing of data which derive from Articles 16 and 17 of Directive 95/46/EC, are fully applicable to data being retained within the meaning of the present Directive.

Amendment 60
RECITAL 16

(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.***

(16) It is essential that Member States provide legislative measure 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.

Amendment 61
RECITAL 16 a (new)

(16a) In this context, it should be recalled that Article 24 of Directive 95/46/EC imposes an obligation on Member States to sanction infringements of the provisions adopted pursuant to Directive 95/46/EC; Article 15(2) of Directive 2002/58/EC imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58/EC; Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems provides that the intentional illegal access to information systems, including to data retained therein, shall be made punishable as a criminal offence.

Amendment 62
RECITAL 16 b (new)

(16b) It should be borne in mind that the right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC, to receive compensation, which derives from Article 23 of Directive 95/46/EC, applies also in relation to the unlawful processing of any personal data pursuant to the present Directive.

Amendment 63
RECITAL 17

(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.

deleted

Amendment 64
RECITAL 17 a (new)

(17a) It should be borne in mind that the 2001 Council of Europe Convention on Cybercrime as well as the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also cover data being retained within the meaning of the present Directive.

Amendment 65
RECITAL 18

(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.

(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 investigation, detection and prosecution of serious **crime as defined by each Member State in national law**, 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.

Amendment 66
RECITAL 19 a (new)

(19a) Considering that the obligations on providers of electronic communications services should be proportionate, the Directive requires that they only retain such data which are generated or processed in the process of supplying their communications services; to the extent that such data is not generated or processed by those providers, there can be no obligation to retain it. This Directive is not intended to harmonise the technology for retaining data, the choice of which will be a matter to be resolved at national level.

Amendment 67
RECITAL 19 b (new)

(19b) It should be remembered that Paragraph 34 of the Inter-institutional agreement on better law-making¹ states that the Council "will encourage the Member States to draw up, for themselves and in the interests of the community, their own tables which will, as far as possible, illustrate the correlation between directives and the transposition measures and to make them public".

¹ OJ C 321, 31.12.2003, p. 1.

Amendment 68/rev
RECITAL 19 c (new)

(19c) The present Directive is without prejudice to the power of Member States to adopt legislative measure concerning the right of access to and use of data by national authorities as designated by them. Issues of access to data retained pursuant to this Directive by national public authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be the subject of national law, or action pursuant to Title VI of the Treaty on European Union, always noting that such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as they are guaranteed by the ECHR. Article 8 ECHR, as interpreted by the European Court of Human Rights, requires that interference by public authorities with privacy rights must respond to requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner which is adequate, relevant and not excessive in relation to the purpose of the interference.

Amendment 69
ARTICLE 1, PARAGRAPH 1

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.***

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 retention of certain data ***which are generated or processed by them***, in order to ensure that the data ***are*** available for the purpose of the investigation, detection and prosecution of serious ***crime, as defined by each Member State in its national law.***

Amendment 70
ARTICLE 2, PARAGRAPH 2, POINT (B A) (new)

(ba) "telephone service" means calls (including voice, voicemail, conference or data), supplementary services (including call forwarding and call transfer), messaging and multi-media services (including Short Message Services, Enhanced Media Services and Multi-Media Services).

Amendment 71
ARTICLE 2, PARAGRAPH 2, POINT (B B) (new)

(bb) "User ID" means an unique identifier allocated to a person as they subscribe or register to an Internet Access Service or Internet Communication Service;

Amendment 72
ARTICLE 2, PARAGRAPH 2, POINT (B C) (new)

(bc) "Cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated;

Amendment 73
ARTICLE 2, PARAGRAPH 2, POINT (B D) (new)

(bd) "unsuccessful call attempt" means a communication where a telephone call has been successfully connected but is unanswered or there has been a network management intervention;

Amendment 74
ARTICLE 3, PARAGRAPH 1

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.

1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that ***the data specified in Article 4, to the extent it is*** 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 ***the*** communication services ***concerned***, are retained in accordance with the provisions of this Directive.

Amendment 75
ARTICLE 3, PARAGRAPH 2

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

2. This shall include the retention of data specified in Article 4 in relation to unsuccessful call attempts where that data is generated or processed, and stored (as regards telephony data) or logged (as regards Internet data) by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned. This Directive shall not require the retention of data in relation to unconnected calls.

Amendment 76
ARTICLE 3 a (new)

Article 3a

Access to data

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. The process to be followed and the conditions to be fulfilled in order to get access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in national law, subject to relevant provisions of Union law or public international law, in particular the European Convention on Human Rights, as interpreted by the European Court of Human Rights.

Amendment 77

ARTICLE 4, PARAGRAPH 1, POINTS (A) TO (F), AND PARAGRAPH 2

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

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

(1) Concerning Fixed Network Telephony and Mobile Telephony

(a) The calling telephone number;

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

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

(a) The User ID(s) allocated.

(b) The User ID and telephone number allocated to any communication entering the public telephone network.

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

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

(b) data necessary to identify the destination of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony:

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

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

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

(a) The User ID or telephone number of the intended recipient(s) of an Internet telephony call.

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

(c) data necessary to identify the date, time and duration of a 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 Access service based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet Access Service provider to a communication, and the User ID of the subscriber or registered user.

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

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

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

(1) Concerning Fixed Network Telephony and Mobile Telephony:

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

(a) The Internet service used.

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

(e) data necessary to identify *users' communication equipment* or what purports to be *their equipment*:

(1) Concerning Fixed Network Telephony

(a) The calling and called telephone numbers.

(2) Concerning Mobile Telephony

(a) The calling and called telephone numbers.

(b) The International Mobile Subscriber Identity (IMSI) of the calling party.

(c) The International Mobile Equipment Identity (IMEI) of the calling party.

(d) The International Mobile Subscriber Identity (IMSI) of the called party.

(e) The International Mobile Equipment Identity (IMEI) of the called party.

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

(3) 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 of the originator of the communication.

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

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

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

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

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

Amendment 78
ARTICLE 4, PARAGRAPH 2 a (new)

2a. No data revealing the content of the communication can be retained pursuant to this Directive.

Amendment 79
ARTICLE 5

Article 5

Revision of the annex *deleted*

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

Amendment 80
ARTICLE 6

Article 6

Committee *deleted*

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.

Amendment 81
ARTICLE 7

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.*

Member States shall ensure that the categories of data referred to in Article 4 are retained for *periods of not less than 6 months and for a maximum of two years* from the date of the communication.

Amendment 82
ARTICLE 7 a (new)

Article 7a

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with the present Directive:

(a) the retained data shall be of the same quality and shall be subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, or accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that access to the data is undertaken only by specially authorised personnel; and

(d) the data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved.

Amendment 83
ARTICLE 8

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.

Member States shall ensure that the data ***as specified in Article 4*** 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.

Amendment 84
ARTICLE 8 a (new)

Article 8a

Supervisory authority

1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7a of this Directive regarding the security of the stored data. These authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. These authorities shall act with complete independence in exercising the functions referred to in paragraph 1.

Amendment 85
ARTICLE 10

Article 10

deleted

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.

Amendment 86
ARTICLE 11

Article 15, paragraph 1a (Directive 2002/58/EC)

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.*

1a. Paragraph 1 *does* not apply to *data specifically required to be retained by Directive 2005/./EC for the purposes referred to in Article 1(1) of that Directive.*

Article 11a

Future measures

1. A Member State facing particular circumstances warranting an extension for a limited period of the maximum retention period referred to in Article 7 may take the necessary measures. The Member State shall immediately notify the Commission and inform the other Member States of the measures taken by virtue of this Article and indicate the grounds for introducing them.

2. The Commission shall, within six months after the notification as referred to in paragraph 1, approve or reject the national measures involved after having verified whether or not they are a means of arbitrary discrimination or disguised restriction of trade between Member States and whether or not they shall constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within this period the national measures shall be deemed to have been approved.

3. When, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may examine whether to propose an adaptation of this Directive.

Amendment 88
ARTICLE 11 b (new)

Article 11b

Remedies, liability and sanctions

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall in particular take the necessary measures to ensure that the intentional access to or transfer of data retained in accordance with the present Directive which is not permitted under national law adopted pursuant to this Directive, shall be punishable by sanctions, including administrative or criminal sanctions, which are effective, proportionate and dissuasive.

Amendment 89
ARTICLE 12, PARAGRAPH 1

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.

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 *further developments in electronic communications technology* and 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 *list of data in Article 4, and the periods* of retention provided for in Article 7. *The results of the evaluation will be made publicly available.*

Amendment 90
ARTICLE 13, PARAGRAPH 1, SUBPARAGRAPH 1

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.**

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than **18 months** after its adoption at the latest. They shall forthwith communicate to the Commission the text of those provisions.

Amendment 91
ARTICLE 13, PARAGRAPH 2 a (new)

2a. Each Member State may for a period of up to 18 months from the expiry of the deadline referred to in paragraph 1 defer application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State which intends to make use of this paragraph shall, by way of a declaration, notify the Commission to that effect upon adoption of this Directive. The declaration shall be published in the Official Journal of the European Union.

Amendment 92
ANNEX

This Annex is deleted