

DRAFT

**COPEN XXX
TELECOM XXX**

OUTCOME

of JHA Council

on : 2 December

No. prev. doc. : 15101/1/05 COPEN 191 TELECOM 141 REV 1

No. Cion prop. : 12671/05 COPEN 150 TELECOM 96 CODEC 803

Subject : Data retention

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 Commission¹,

Having regard to the opinion of the European Economic and Social Committee²,

Having regard to the opinion of the Committee of the Regions³,

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 data⁴ 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

¹ OJ C [...], [...], p. [...].

² OJ C [...], [...], p. [...].

³ OJ C [...], [...], p. [...].

⁴ OJ L 281, 23.11.1995, p. 31.

sector⁵ translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

⁵ OJ L 201, 30.7.2002, p. 37.

- (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.
- (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) *[deleted]*
- (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.

(9bis) 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 retention of data is therefore a necessary measure in accordance with the requirements of Article 8 of the European Convention on Human Rights.

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

(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.

(12) *[deleted]*

(12bis) 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.

- (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.**
- (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*** ~~create a platform~~ composed of representatives of the ***Member States'*** law enforcement authorities, associations of the electronic communications industry, ***European Parliament representatives*** and data protection authorities, ***including the European Data Protection Supervisor***.
- (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'.
- (15bis) 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.
- (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; [...]

(16bis) 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.

(16ter) 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.

(17) *[deleted]*

(17bis) 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.

(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.

- (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),
- (A) 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.
- (20) It should be remembered that Paragraph 34 of the Inter-institutional agreement on better law-making (OJ C 321, 31.12.2003) 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".
- (Z) **The present Directive is without prejudice to the power of Member States to adopt legislative measures 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.

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 [...] 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* ~~criminal offences~~ [...].**

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/EC⁶, 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.
 - (c) "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);
 - (d) "User ID" means an unique identifier allocated to a person as they subscribe or register to an Internet Access Service or Internet Communication Service;
 - (e) "Cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated;
 - (f) "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.

⁶ OJ L 108, 24.4.2002, p. 33.

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 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.
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.**

Article 3bis

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.

Article 4

Categories of data to be retained

1. 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:

- (1) Concerning Fixed Network Telephony and Mobile Telephony
 - (a) The calling telephone number;
 - (b) Name and address of the subscriber or registered user;
- (2) [...]
- (3) 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 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) [...]
- (3) 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.

- (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:

- (1) Concerning Fixed Network Telephony and Mobile Telephony
 - (a) The telephone service used [...]
- (2) Concerning Internet e-mail and Internet telephony
 - (a) The Internet service used.

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.
- (c) [...]

f). Data necessary to identify the location of mobile 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.

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

Article 5

Revision of the annex

[deleted]

Article 6

Committee

[deleted]

Article 7

Periods of retention

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 [...].

Article 7bis

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.

Article 8

Storage requirements for retained data

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.

Article 8bis

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 7bis 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.

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

[deleted]

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 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.**”

New Article X

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.

Article 11bis

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.

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 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.
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 18 months after its adoption at the latest. They shall forthwith communicate to the Commission the text of those provisions [...]

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

3. 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 email. 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.

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,

Annex

[deleted]

The Commission considers that reimbursement by Member States of additional costs incurred by undertakings for the sole purpose of complying with requirements imposed by national measures implementing this Directive for the purposes as set out in the Directive would be compatible with the Treaty in accordance with the provisions of Article 87.3.b.

Declaration ad Article 1

In defining "serious crime" in national law Member States **shall have due regard** to the crimes listed in article 2(2) of the Framework Decision on the European Arrest Warrant (2002/534/JHA) and crime involving telecommunication.

Joint declaration by the Council and the Commission in relation to article 12 (evaluation) of the draft Directive

The Commission will invite Member States and the European Parliament, the European Data Protection Supervisor and representatives from the electronic communications industry to regular review meetings to exchange information about technological developments, costs and effectiveness of application of the Directive. The first meeting will take place before end 2006.

During this process, Member States will be invited to inform partners of their experiences in implementing the Directive and share best practices. On the basis of the outcome of such meetings, the Commission will consider presenting any necessary proposals, including with regard to any difficulties which may have emerged for Member States in relation to the technical and practical implementation of the Directive, in particular its application to Internet e-mail and Internet telephony data.