COUNCIL OF THE EUROPEAN UNION

Brussels, 29 June 2005

10609/05

Interinstitutional File: 2004/0813 (CNS)

LIMITE

COPEN 102
TELECOM 64

NOTE

from :	Incoming Presidency
to :	Working Party on Cooperation in Criminal Matters
No. prev. doc. :	8864/1/05 REV 1 COPEN 91 TELECOM 33
Subject :	Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of investigation, detection and prosecution of crime and criminal offences including terrorism.

I JUNE 2005 JHA COUNCIL

The JHA Council examined at its meeting on 2 and 3 June 2005 the above draft Framework Decision on the basis of 8864/1/05 REV 1 COPEN 91 TELECOM 33. The Council agreed that retention of communication data is an important element in the fight against crime and terrorism and that EU legislation on the matter is necessary. However, a number of issues remained outstanding. Following a long debate, the Presidency drew the following conclusions:

- In order to make rapid progress, a step by step approach may be preferable concerning the communication data to be retained. A first step could be the retention of communication data related to fixed and mobile telephony. Concerning internet and unsuccessful outgoing calls, a transitional period to be determined could be granted to Member States which could not immediately ensure the retention of the relevant communication data.

- Regarding the list of communion data to be retained (Article 2), there was general agreement on the approach proposed by the Presidency. This approach involved a minimum list constituting a functional list with, however, some technical indications included. The details of the list needed further examination by experts.
- There was a need for further contacts between service providers and law enforcement authorities to obtain more information on the costs involved in retaining the relevant communication data.
- Most delegations could accept the periods for retention proposed by the Presidency (Article 4). The normal period would be 12 months, but it would be possible for Member States to provide for longer periods (up to 48 months) or shorter periods (not below 6 months) in specified circumstances.
- Regarding the legal basis, a majority of delegations thought the draft instrument belonged in the third pillar.

The UK indicated that it would prepare for discussion of the file at the informal JHA Council in September 2005 with a view to formal discussions at the October 2005 JHA Council.

Several delegations maintained general scrutiny reservations and general parliamentary scrutiny reservations on the draft. The Dutch minister informed the Council of the opinion of the Dutch Parliament on the matter and indicated that he was not able to give any definitive position on the subject under discussion at this point.

II FOLLOW-UP

In light of the conclusions from the June JHA Council the incoming Presidency proposes to focus on the following topics at the meeting of the Working Party on co-operation in criminal matters on 4 and 5 July 2005:

- The list of communication data to be retained, including the application of a step by step approach concerning the list;
- Exceptions to the periods of retention;
- The costs and benefits involved in retaining communication data; and
- Data security.

The aim of the meeting is to resolve the outstanding issues on the detail of Articles 1-5 and to prepare for a debate on the costs and benefits of data retention at the informal JHA Council in September 2005. The outstanding issues on legal base and rules on judicial co-operation (Article 7) will be taken at the Article 36 Committee / COREPER / JHA Council.

a. The list of data to be retained

The incoming Presidency intends to examine the list in detail at the meeting. It has for that purpose established the revised version of Articles 2, 3 and 8 set out in the Annex. The revised Article 3 contains the list of communication data to be retained, including fixed and mobile telephony, internet data and data related to unsuccessful outgoing calls. Article 8 provides for a transitional period regarding internet and unsuccessful outgoing calls.

b. Periods of retention

At the JHA Council in June there was support for the approach to the retention periods in Article 4. However a number of delegations expressed interest in the idea set out in the covering note to 8864/1/05 REV 1 COPEN 91 TELECOM 33 of creating an exception to the six-month retention period for specific data types. On the basis of that debate and in order to take forward further discussions the incoming Presidency proposes amendments to Article 4 set out in the Annex.

c. Costs and benefits

The JHA Council agreed at its meeting in December 2004 that particular consideration should be given to the proportionality of the draft Framework Decision. In this regard, there is a need for more detailed information on the costs involved in retaining communication data and on the expected benefits of having the data available for law enforcement purposes.

Discussion at the June JHA Council established that it is necessary to get a clear a picture of the costs involved in retaining the types of communication data covered by Article 2. The incoming Presidency proposes to examine the issue of costs with a view to:

- Taking stock of the information available,

- Discussing how to proceed in order to supplement that information, having in mind that precise, reliable and detailed information is necessary for the purpose of comparing the costs of with the benefits of the measure.

To this end, the incoming Presidency also proposes the revised text of Recital 16 set out in the Annex.

Regarding the expected costs and benefits of this measure, the UK will in advance of the meeting on 4 and 5 July 2005 circulate a separate paper with detailed information on its experience in using communication data for the purpose of investigations into criminal matters in the UK. This will include both statistics on the retained data sought by law enforcement authorities, including its age and the offences involved, and the costs that have been generated in ensuring such data is available. The incoming Presidency invites other delegations to give detailed information at the meeting on experience with the use of communication data in their countries and, if possible, to send that information to the general Secretariat in advance of the meeting (e-mail bent.mejborn@consilium.eu.int).

d. Data security

The incoming Presidency would like to examine the footnotes to Article 5 with a view to finalising this provision.

ANNEX

Draft Framework Decision

on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of (…) investigation, detection and prosecution of crime and criminal offences including terrorism.[1]

THE COUNCIL OF THE EUROPEAN UNION

Having regard to the Treaty on European Union, and in particular Article 31(1)(c) and Article 34 (2)(b) thereof,

Having regard to the initiative of the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom,

Having regard to the Opinion of the European Parliament,

Whereas:

1. Offering a high level of protection in an area of liberty, security and justice requires that the (…) investigation, detection and prosecution of crime and criminal offences be carried out in an (...) efficient and effective manner which respects the fundamental human rights of individuals.

2. The plan of action of the Council and the Commission on the best ways to implement the provisions of the Treaty of Amsterdam on the establishment of an area of liberty, security and justice, the conclusions of the European Council at Tampere on 15-16 October 1999, the European Council at Santa Maria da Feira on 19-20 June 2000, the European Commission in its scoreboard and the European Parliament in its resolution of 19 May 2000 call for an intervention in the area of high tech crime.

[1] In the light of comments made by the Legal Service in Coreper on 19 May 2005, the Presidency has, subject to further scrutiny, removed the reference to "prevention" from the title of the draft instrument and from certain recitals.

3. The conclusions of the Council of 20 September 2001 call for care to be taken to ensure that the forces of law and order are able to investigate criminal acts which involve the use of electronic communications systems and to take measures against the perpetrators of these crimes, while maintaining a balance between the protection of personal data and the needs of the law and order authorities to have access to data for criminal investigation purposes. It is noted in the conclusions of the Council of 19 December 2002 that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications is now a particularly important and valuable tool in the (…) investigation, detection and prosecution of crime and criminal offences, in particular organised crime and terrorism.

4. 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 with a view to adoption by June 2005.

5. It is essential to retain data existing on public communications networks, generated in consequence of a communication, hereafter referred to as data, for the (…) investigation, detection and prosecution of crimes and criminal offences, in particular those offences involving the use of electronic communications systems. This (...) Framework Decision relates only to data generated as a consequence of a communication or a communication service and does not relate to data that is the content of the information communicated. In particular, it is necessary to retain data in order to trace the source of illegal content such as child pornography and racist and xenophobic material; the source of attacks against information systems; and to identify those involved in using electronic communications networks for the purpose of organised crime and terrorism.

6. Preservation of specific data relating to specified individuals in specific cases is not sufficient to meet these requirements. In investigations, it may not be possible to identify the specific data required or the individual involved until many months or years after the original communication. It is therefore necessary to retain certain types of data, which are already processed and stored for billing, commercial or any other legitimate purposes, for (...) additional periods of time in anticipation that they might be required for a future criminal investigation or judicial proceedings. This Framework Decision therefore concerns the retention of data and does not relate to the preservation of data.

7. In recognition of the importance of the need to retain data, Article 15 of Directive 2002/58/EC permits the adoption of legislative measures allowing, under certain conditions, retention of data for the purposes of the prevention, investigation, detection or prosecution of crime and criminal offences. This Framework Decision is not related to other objectives set out in Article 15 of this Directive and therefore does not provide for rules on data retention for the purpose of safeguarding national security (i.e. State Security), defence and public security. Nor is it related to the unauthorised use of the electronic communication system when such use does not constitute a criminal offence.

8. Many Member States have passed legislation concerning a priori retention of data for the purposes of prevention, investigation, detection or prosecution of crime and criminal offences. Work in this area is under way in other Member States. The content of this legislation varies considerably between Member States.

9. The differences between the legislation in Member States is prejudicial to co-operation between the competent authorities in the (…) investigation, detection and prosecution of crime and criminal offences. To ensure effective police and judicial co-operation in criminal matters, it is therefore necessary to ensure that all Member States take the necessary steps to retain certain types of data for a length of time within set parameters for the purposes of (…) investigating, detecting and prosecuting crime and criminal offences including terrorism. Such data should be available to other Member States in accordance with the instruments on judicial co-operation in criminal matters adopted under Title VI of the Treaty on European Union. This should also include instruments which were not adopted under this Title but which (...) have been acceded to by the Member States and to which references are made in the instruments on judicial co-operation in criminal matters adopted under Title VI of the Treaty on European Union.

9bis. In an area of freedom, security and justice, obligations upon Industry to retain data are justifiable only if necessary to preserve important interests within a democratic society. This necessity arises from the importance of analysing specific historic data in the investigation, detection and prosecution of terrorist crimes and other serious offences. Where that data may provide the only approach for an effective resolution of such crimes, its availability for a determined period of time may be reliably ensured only with a statutory storage obligation[1].

[1] Proposal from incoming Presidency drawing on the DE text previously at footnote 4 to Article 1 in 8864/1/05 COPEN 91 REV 1 TELECOM 33.

10. Such a priori retention of data and access to this data may constitute an interference in the private life of the individual. However, such an interference does not violate the international rules applicable with regard to the right to respect to privacy and the handling of personal data contained, in particular, in the European Convention on the Protection of Human Rights of 4 November 1950, the Convention of the Council of Europe no.108 on the protection of persons in respect of the automated handling of personal data of 28 January 1981, and the Directives 5/46/EC, 97/66/EC and 2002/58 EC where such interference is provided for by law and where it is appropriate, strictly proportionate to the intended purpose and necessary within a democratic society, and subject to adequate safeguards for the (…) investigation, detection and prosecution of crime and criminal offences including terrorism.

11. Taking into account both the need to ensure that data is retained a priori in an efficient and harmonised way and the need to allow Member States ample room to make their own individual assessments given the differences that exist between criminal justice systems, it is appropriate to establish parameters for the a priori retention of data.

12. Data may be a priori retained for different periods of time depending on its type. The retention periods for each type of data will be dependant on the usefulness of the data in relation to the (…) investigation, detection, and prosecution of crime and criminal offences and the cost of retaining the data. The retention periods shall be proportionate in view of the needs for such data for the purposes of (…) investigating, detecting and prosecuting crime and criminal offences as against the intrusion into privacy that such retention will entail from disclosure of that retained data.

13. The drawing up of any lists of the types of data to be retained must reflect a balance between the benefit to the (…) investigation, detection, and prosecution of crime and criminal offences of keeping each type of data against the level of invasion of privacy which will result.

14. (...) This Framework Decision does not apply to access to data at the time of transmission, that is by the monitoring, interception or recording of telecommunications.

15. Member States must ensure that access to retained data takes account of privacy rules as defined in international law applicable to the protection of personal data.

16. Member States shall ensure that implementation of (...) this Framework Decision involves appropriate consultation with the Industry with particular regard to the practicality and cost of retaining data. Recognising that the retention of data no longer required for business purposes can represent practical and financial burdens upon Industry, Member States should consider making appropriate contributions towards the costs incurred by Industry to comply with any mandatory or voluntary obligations arising from the implementation of this Framework Decision.

HAS ADOPTED THE PRESENT DECISION:

Article 1[1]

Scope and Aim

1. This Framework Decision aims to facilitate judicial co-operation in criminal matters by approximating Member States' legislation on the retention of communication data[2], generated or processed[3] by providers of a publicly available electronic communications service or a public communications network, for the purpose of investigation, detection and prosecution of criminal offences.

2. This Framework Decision shall apply to communication data generated or processed by providers of a publicly available electronic communications service or a public communications network (...).

3. This Framework Decision shall not apply to the content of exchanged communications, including information consulted using an electronic communications network.

---

1 Scrutiny reservations on Article 1 by FI/IT.

2 AT entered a scrutiny reservation on the application of the expression "communication", which is defined in Directive 2002/58/EC. The Chairman suggested that as the expression used in the draft was "communication data", and not just "communication", the text did not interfere with the definition of "communication" in the Directive.

3 AT proposed the following recital: "the term "processed" should cover only such data which is necessary to establish, maintain and manage connections for this service (traffic data relating to subscribers and users processed by the provider of a public communications network or publicly available electronic communications service); data which is not necessary for such purpose should not be included (e.g. subject lines of an email)."
Scrutiny reservation by some delegations.

4. This Framework Decision is without prejudice to:

- national rules on retention of communication data processed or generated by providers of a publicly available electronic communications service or a public communications network for the purpose of prevention of crime;

- the rules applicable to judicial co-operation in criminal matters with regard to the interception and recording of telecommunications;

- the rules applicable to the exchange of information within the framework of police cooperation;[1]

- activities concerning public security, defence and national (i.e State security);

[1] Scrutiny reservation by DK.

Article 2

Definitions

1. For the purpose of this Framework Decision, the term "communication data" means:

(a) traffic data and location data as defined in Article 2 of the Directive 2002/58/EC;

(b) user data, which means data relating to any (...) natural or legal person using a publicly available electronic communications service, for private or business purposes, without the user necessarily having subscribed to the service;

(c) subscriber data, which means data relating to any (...) natural or legal person subscribing to a publicly available electronic communications service for, private or business purposes, without necessarily having used the service.

2. (...)

Article 3

Retention of communication data

1. Each Member State shall take the necessary measures to ensure that, for the purpose of providing judicial co-operation in criminal matters, communication data (...) generated or processed by providers of a publicly available electronic communications service or a public communications network is retained in accordance with the provisions of this Framework Decision.

2. Communication data to be retained for the purpose set out in Article 1 shall at least include the following data:

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

1. Concerning Fixed Network Telephony

a) The calling (...) telephone number.

b) Names and addresses of the users or subscribers to whom the telephone number was registered at the time of the connection.

c) (...)

2. Concerning Mobile Telephony

a) The calling (...) telephone number (...).

b) (...)

b) Names and addresses of the users or subscribers to whom the telephone number was registered at the time of the connection.

3. Concerning Internet Access and Internet Services

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

b) The Connection Label or User ID via which the connection to the Internet access provider was made.

c) (...)

d) The User ID, e.g. e-mail address, of the source of a communication.

e) The Connection Label or telephone number allocated to any communication entering the public telephone network.

f) Name and address of the user or subscriber to whom the IP Address, Connection Label or User ID was allocated at the time of the connection.

(b) Data necessary to identify the (...) destination of a communication.

1. Concerning Fixed Network Telephony

a) The called telephone number or numbers.

b) Names and addresses of the users or subscribers to whom the telephone numbers were registered at the time of the connection.

2. Concerning Mobile Telephony

a) The called telephone number or numbers.

b) Names and addresses of the users or subscribers to whom the telephone numbers were registered at the time of the connection.

3. Concerning Internet Access and Internet Services

a) The Connection Label or User ID, e.g. e-mail address, of the recipient of a communication.

b) Name and address of the user or subscriber to whom the IP Address, Connection Label or User ID was allocated at the time of the connection.

(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 and Internet Services

a) The date and time of the log-in and log-off of 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, Short Message Service, Enhanced Media Service or Multi-Media Service.

2. Concerning Mobile Telephony:

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

b) Whether the communication was terminated explicably or inexplicably.

3. Concerning Internet Access and Internet Services

a) The Internet Service used, e.g. e-mail, chat or web browsing.

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

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.

3. Concerning Internet Access and Internet Services

a) The calling telephone number for dial-up access.

b) The asymmetric digital subscriber line (ADSL) or other end point 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 equipment at the start and the end of the communication.

a) location label (Cell ID) at the start and end of the connection.

b) data mapping between Cell IDs and their geographic location at the time of the communication.

3. Member States shall take appropriate measures for the purpose of the technical implementation of paragraph 1.

Article 4 [1]

Time periods for retention of communication data

1. Each Member State shall take the necessary measures to ensure that communication data referred to in Article 3 shall be retained for a period of 12 months following its generation. Relating to subscriber data, this period shall run from the end of the subscription.

2. By derogation from paragraph 1, any Member State may provide for retention of communication data referred to in Article 3 for longer periods of up to 48 months in accordance with national criteria when such retention constitutes a necessary, appropriate and proportionate measure within a democratic society.

3. By derogation from paragraph 1, and subject to paragraph 4, any Member State may provide for retention of communication data referred to in Article 3 for shorter periods of at least 6 months[2] (…) should the Member State not find acceptable, following national procedural or consultative processes, the retention period set out in paragraph 1 of this Article.

[4. By derogation from paragraph 1 and paragraph 3, any Member State may provide for retention of communication data relating to Fixed Network Telephony and Mobile Telephony messaging services and multi-media services for shorter periods of at least 6 months should the Member State not find acceptable, following national procedural or consultative processes, the retention period set out in paragraph 1 of this Article.]

5. By derogation from paragraph 1, any Member State may exceptionally provide for retention of communication data for shorter periods of less than 6 months, where that data is ordinarily retained for business purposes for less than 7 days, should the Member State not find acceptable, following national

[1] Scrutiny reservations by NL/CZ/IT/SI/SK/ES/DE/LV/MT/FI/PT on Article 4.

[2] Reservation by CZ , which did not want a minimum and in any case thought that 3 months would be enough. Scrutiny reservation by UK.

procedural or consultative processes, the retention period set out in paragraph 1 of this Article.

6. Any Member State which decides to make use of paragraphs 2, 3, [4] or 5 must notify the Council and the Commission of the retention periods provided for with specification of the communication data concerned. Any such derogation must be reviewed at least every 5 years.

Article 5[1]

Data Security

Each Member State shall ensure that communication data retained under this Framework Decision is subject, as a minimum, to the rules adopted pursuant to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movements of such data, to the provisions of Article 4 of Directive 2002/58/EC and to the following data security principles:

(a) the retained data shall be of the same quality 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, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing;

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

---

[1] HU referred to its proposals in 6909/05 COPEN 45 TELECOM 14.
AT, supported by some delegations (FI/SI), proposed the following:
Each Member State shall ensure that data retained under this Framework Decision shall be subject, as a minimum, to the following data security principles and regard shall be given to the provisions of Article 4 of Directive 2002/58/EC:
(a) (unchanged)
(b) (unchanged)
(c) the data shall not be disclosed to anybody who is not legally responsible for the investigation or for the control legitimacy of investigations;
(d) shall effectively guarantee by technical and organisational measures, that access to the data retained is only granted to authorised persons and in every single case only for a pre-defined and limited period of time after legitimacy of access was checked by the competent judicial authority.
(e) (former (c) unchanged).
SE proposed to delete Article 5 and introduce the following recital:
"9a. When processing personal data, providers of publicly available electronic telecommunications services or public communications networks are bound by national provisions on data protection providing a high level of data protection, in particular rules adopted pursuant to Directive 95/46/CE on the protection of individuals with regard to the processing of personal data and the free movements of such data, and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. These rules must be observed when personal data is processed according to this Framework Decision."
Several delegations entered scrutiny reservations on Article 5. Some delegations thought the provision could be deleted.

Article 6

Access to retained communication data

Each Member State shall ensure that access for the purposes referred to in Article 1 to communication data retained under this Framework Decision shall be subject, as a minimum, to the following rules and shall establish judicial remedies in line with the provisions of Chapter III on 'Judicial remedies, liability and sanctions' of Directive 95/46/EC:

(a) data shall be accessed for specified, explicit and legitimate purposes by competent authorities on a case by case basis in accordance with national law and not further processed in a way incompatible with those purposes;

(b) the process to be followed and the conditions to be fulfilled in order to get access to retained data and to preserve accessed data shall be defined by each Member State in national law;

(c) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are accessed. Data shall be processed fairly and lawfully;

(d) data accessed by competent authorities shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the data were collected or for which they are further processed;

(e) the confidentiality and integrity of the data shall be ensured;

(f) data accessed shall be accurate and, every necessary step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

Article 7

Request for transmission of retained communication data under judicial co-operation in criminal matters

Each Member State shall execute requests from other Member States for transmission of communication data, retained pursuant to Articles 3 and 4, in accordance with the applicable instruments on judicial co-operation in criminal matters. [The requested Member State may make its consent to such a request for communication data subject to any conditions which would have to be observed in a similar national case.][1]

[1] Several delegations and the Commission have called for the deletion of this sentence, which, in their view, would allow for refusing requests for mutual assistance to a wider extent than provided under existing instruments. However, other delegations (NL/SE/DK/IR/DE/LT/LV/AT/IT) thought the sentence should be retained.

Article 8

Implementation

1. Member States shall take the necessary measures to comply with this Framework Decision within two years of its entry into force.

2. By the same date Member States shall transmit the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision. The General Secretariat of the Council shall communicate to the Member States the information received pursuant to this Article.

3. Each Member State may for a period of up to four years from the date of entry into force of this Framework Decision defer from its application of this Framework Decision the retention of communications data relating to either or both:

(a) connected ineffective communications, e.g. unsuccessful or unanswered telephone calls, on Fixed Network Telephony or Mobile Telephony, and
(b) Internet Access and Internet Services.

Any Member State which intends to make use of this paragraph shall, by way of a declaration, notify the General Secretariat of the Council to that effect upon adoption of this Framework Decision. The declaration shall be published in the Official Journal of the European Union.

4. The Commission shall by [1st January 2008] submit a report to the Council assessing the extent to which the Member States have taken necessary measures in order to comply with this Framework Decision.

Article 9

Entry into force

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