COUNCIL OF THE EUROPEAN UNION

Brussels, 24 February 2005

6566/05

LIMITE

COPEN 35
TELECOM 10

REPORT

from :	Working Party on cooperation in criminal matters
to :	Article 36 Committee
No. prev. doc. :	15098/04 COPEN 142 TELECOM 172
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 prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.

The Council discussed on 2 December 2004 which data should be covered by the draft Framework Decision on data retention. The Council instructed its preparatory bodies to examine option 2 referred to in 15098/04 COPEN 142 TELECOM 172, which implies an obligation for service providers to retain relevant data defined in a common list in the Framework Decision, provided that the data is processed/generated by the service provider in the process of supplying the telecommunications service concerned. Particular consideration should be given to the proportionality of the measure in relation to costs, privacy (data protection) and efficacy. It was recalled that the Commission had entered a scrutiny reservation on the legal basis for the proposal.[1]

[1] 15556/04 PV/CONS 75 JAI 527 + COR 1.

At the meeting of the Article 36 Committee on 7 February 2005, the Commission entered a reservation on the legal basis. The Commission observed that the draft contained an obligation for service providers to keep traffic data for a specified period of time as well as provisions on access to and exchange of this data by authorities competent in criminal matters. The reservation by the Commission concerned the first part, the obligation for service providers to keep traffic data for a specified period of time, which in the view of the Commission would need to be based on a proposal for a Directive under Article 95 TEC.

The Working Party on cooperation in criminal matters continued at its meeting on 17 and 18 February 2005 its examination of the draft Framework Decision on the basis of the above and the text set out in 14190/1/04 REV 1 COPEN 132 TELECOM 160.

Regarding the legal basis, the Commission maintained its reservation. The Presidency took that the Commission had not yet officially transmitted its position in writing to the Council, and that the Commission so far had not submitted a proposal for a Directive. The Presidency concluded that on the present basis work on the draft Framework Decision should continue in line with the conclusions drawn at the Council on 2 December 2004, and recalled that the European Council Declaration of 25 March 2004 provided that measures on retention of traffic data should be examined with a view to their adoption by June 2005.

The European Parliament has been invited to give its opinion on the draft.

Several delegations have entered general scrutiny reservations and general parliamentary scrutiny reservations on the draft.

The Article 36 Committee is at this stage invited to examine the following provisions:

- *Article 1 - scope and aim*
- *Article 7 - requests to access data for the purpose of judicial cooperation in criminal matters.*

The outstanding questions are set out in footnotes to the said provisions in the 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 prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.[1]

Article 1[2]

Scope and Aim

1. This Framework Decision aims to facilitate judicial[3] co-operation in criminal matters by approximating Member States' legislation on the retention of [communication][4] data[5], generated or processed[6] 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.[7] [8]

---

1 The preamble has not been reproduced and will be examined at a later stage.

2 Scrutiny reservations on Article 1 by several delegations.

3 SE called for the introduction of a reference to police co-operation.

4 The Presidency proposed to replace "data" by "communication data" in Article 1 and elsewhere in the text (possibly including the title of the draft) to make it clearer what data is included and in particular to make it apparent that content data is not included. Many delegations supported this approach. However, a number of delegations entered scrutiny reservations.

5 [Communication] data is defined in Article 2. Article 3 provides that it is the [communication] data referred to in Article 2(2) which shall be retained. LT proposed to introduce a reference to Article 2 in Article 1.

6 The words "generated or processed" was proposed by the Presidency in the light of the outcome of the JHA Council on 2 December 2004. Scrutiny reservations by some delegations. DE thought data related to failed attempts to establish a communication should be excluded. FI was concerned regarding costs.

7 AT/DE thought the text should be limited to "serious criminal offences".

8 UK maintained a reservation on the deletion of the reference to "prevention".

2. This Framework Decision shall apply to all means of electronic communication, including in particular:

(a) Telephony excluding Short Message Services, Electronic Media Services and Multi Media Messaging Services.

(b) Short Message Services, Electronic Media Services and Multi Media Messaging Services provided as part of any telephony service.

(c) Internet Protocols including Email, Voice over Internet Protocols, world wide web, file transfer protocols, network transfer protocols, hyper text transfer protocols, voice over broadband and subsets of Internet Protocols numbers - network address translation data.

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

3. 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;

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

[- national rules relating to the retention of [communication] data types which are not held by communication service providers for business purposes.][1]

[1] Some delegations thought the fourth indent could be deleted, and asked for an explanation on its inclusion from the delegations having proposed the draft Framework Decision.

Article 2[1]

Definitions

1. For the purpose of (…) this Framework Decision, the term '[communication] data' in this Framework Decision means:

(a) traffic data and location data as set out in Article 2 of the Directive 2002/58/EC (…).

(b) User data (…) relating to any user of a publicly available electronic communications service, for private or business purposes, without the user necessarily having subscribed to the service.

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

[1] Revised text proposed by the Presidency in the light of comments made. AT/DE would prefer to exclude data relating to unsuccessful attempts to establish telecommunications. IT/GR/FI entered scrutiny reservations on the question of costs caused by retention.

2. [Communication] data to be retained for the purpose set out in Article 1 include: [1] [2] [3]

(a) Data necessary to trace and identify the source of a communication which includes personal details, contact information and information identifying services subscribed to.

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

(c) Data necessary to identify the time and date and duration of a communication.

(d) Data necessary to identify the telecommunication.

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

(f) Data necessary to identify the location at the start and throughout the duration of the communication.

---

[1] The Presidency proposes regarding the list the following:
1) a functional list, not going in technical details, along the lines of the present Article 2(2),
2) the new Article 3(2), and
3) agreement to establish a handbook on technical aspects regarding the implementation of Articles 2(2) and 3.
Many delegations reacted positively to this approach. However, many delegations entered scrutiny reservations. In particular, the exact wording of Article 3(2) and the link between the draft and the handbook would need further consideration. The Presidency has reworded Article 3(2) following the meeting for the purpose of further consideration. The Legal Service of the Council expressed reservations on the approach proposed and pointed to the possibility of establishing a technically more detailed list in the draft and providing for a mechanism to revise that list.

[2] AT proposed the following version of Article 2(2):
" For the purpose of this Framework Decision data retention should in any case be limited to those traffic data , which are created at the provider during the process of connecting the user to the network and are necessary for attributing a network-address (used at a given time) to the respective subscriber ("access data").
These data includes the data listed in the annex of this framework decision."

[3] Scrutiny reservations by several delegations on the list. The Presidency invited delegations to communicate to the Presidency and the Secretariat:
- any proposals they may have for amendments to the list in Article 2(2)
- any other information (manuals, codes of practice etc) they consider would be of interest during discussions the list.

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 as referred to in Article 2(2) when 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.[1] Member States shall take appropriate measures for the purpose of the technical implementation of paragraph 1.

Article 4[2]

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 36 months in accordance with national criteria when such retention constitutes a necessary, appropriate and proportionate measure within a democratic society.

---

[1] See footnote to Article 2(2).

[2] The Presidency has revised Article 4 in the light of comments made for the purpose of further discussions.

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

4. Any Member State which decides to make use of paragraph 3 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 annually.

Article 5[1]

Data Security

Each Member State shall ensure that, regarding [communication] data retained under this Framework Decision, providers subject to the retention obligation must comply, as a minimum, 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] It was agreed to re-examine Article 5 at a later stage. Some delegations (AT/HU) announced they would submit written proposals.

Article 6[1]

Access to retained [communication]data

Each Member State shall ensure that access 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;

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

(a ter) (...)

(b) 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;

(c) 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;

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

(e) data accessed shall be accurate and, every reasonable 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;

[1] It was agreed to re-examine Article 6 at a later stage.

Article 7

Request to access [communication] data for the purpose of judicial co-operation in criminal matters

A request made by a Member State to another Member State, for access to [communication] data referred to in Article 2, shall be made and responded to in accordance with the applicable instruments on judicial co-operation in criminal matters (...)[1]. The requested Member State may make its consent to such a request for access to data subject to any conditions which would have to be observed in a similar national case. [2]

Article 8

Implementation

Member States shall take the necessary measures to comply with this Framework Decision by […..June 2007] within two years following the date of adoption.

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.

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.

---

[1] Scrutiny reservations by some delegations on the deletion of the last part of the sentence ("..instruments on judicial cooperation in criminal matters adopted under Title VI of the Treaty on European Union").

[2] BE, supported by some delegations, thought the second sentence should be deleted. BE argued that the sentence would allow for refusing mutual assistance on the grounds of double criminality and thereby would be in contradiction to the obligations under the 1959 European Convention on mutual assistance in criminal matters and the 1990 Schengen Convention. Several delegations entered scrutiny reservations. DK entered a reservation on the possible deletion of the second sentence.

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.

_____