COUNCIL OF THE EUROPEAN UNION

Brussels, 27 July 2005

11510/05

Interinstitutional File: 2004/0813 (CNS)

LIMITE

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC

COPEN 115
TELECOM 81

PUBLIC

OUTCOME OF PROCEEDINGS

of :	Working Party on Cooperation in Criminal Matters
dated :	4 and 5 July 2005
No. prev. Doc. :	10609/05 COPEN 102 TELECOM 64
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 INTRODUCTION

The Working Party on cooperation in criminal matters examined on 4 and 5 July 2005 Articles 1-5 and 8 of the above draft on the basis of 10609/05 COPEN 102 TELECOM 64.

The Working Party also discussed the costs and benefits involved in retaining communication data in preparation of discussions in the Article 36 Committee on 7 and 8 July 2005 and at the informal JHA Council in September 2005.

The text resulting from these proceedings is set out in the Annex. The outstanding questions are set out under II below and in footnotes in the Annex.

The European Parliament has been invited to give its opinion on the draft. It rejected the draft on 7 June 2005.

Several delegations have entered general scrutiny reservations and general parliamentary scrutiny reservations on the draft. The Commission has entered a general scrutiny reservation.

II OUTSTANDING QUESTIONS

Reference is made to the Annex for details.

a. Article 1 - scope and aim

Article 1 is subject to:

- a general scrutiny reservation by **DELETED**, and
- a scrutiny reservation on the expression "communication data" and a suggestion for a recital on the term "processed" by **DELETED**.
- a scrutiny reservation by **DELETED** on the fourth indent of Article 1(4).

b. Articles 3 and 8(3) - the list of data to be retained

Substantial progress was made on the list. In particular, the scope of the list was clarified and narrowed down regarding Internet data and regarding unanswered telephone calls (see new definitions in Article 2). This is expected to have a positive influence on future discussions on costs.

During the meeting however those delegations not comprising technical experts indicated that they would need time to consult on the proposed changes. The Presidency has amended the list in the Annex to reflect discussions and would welcome, by no later than **28 August 2005**, comments from all delegations on this new proposal. These should be sent to the Council Secretariat (**DELETED**) and copied to the Presidency (**DELETED**).

The main question remaining is the transitional measures in Article 8(3) for unanswered telephone calls, Internet access and Internet Communication services, which were proposed to meet concerns expressed by in particular **DELETED**. In addition, a number of delegations have entered scrutiny reservations on Article 3 in general or on specific points.

c. Article 4 - 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 have maintained their scrutiny reservations on the provisions, and **DELETED** has maintained a reservation as it did not want a minimum period for retention and thought that a minimum period of 3 months (rather than 6 months) would suffice.

d. 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 was 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.

The **DELETED** indicated at the JHA Council on 2 and 3 June 2005 that it would prepare for discussion of costs and benefits at the informal JHA Council in September 2005 with a view to formal discussions of the whole draft at the October JHA Council.

The **DELETED** submitted information on experience in the **DELETED** of using historic communication data for law enforcement purposes and of the costs involved in the retention of data. Other delegations were invited to do the same with a view to preparing the informal September JHA Council.

The Presidency proposed a revised text for Recital 16, an amended version of which is set out in the Annex. Several delegations entered reservations on the draft recital tabled at the meeting and thought that the matter of possible contributions to Industry to cover costs should be left entirely with the Member States and should not be addressed in the draft.

e. Article 5 - Data security and data protection

DELETED would examine if they could lift their reservations in the light of changes made to the text.

f. Article 7 - judicial cooperation

The second sentence of Article 7 provides that concerning mutual assistance requests for data retained pursuant to the Framework Decision the requested State may make its consent to such a request subject to any conditions which would have to be observed in a similar national case.

Discussions at the JHA Council on 2 and 3 June 2005 showed that further examination of the second sentence was needed. IR lifted its reservation. The situation is on that basis as follows:

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 (**DELETED)** thought the sentence should be retained.

The Luxembourg Presidency suggested that a way forward may be to address this matter in the context of the European evidence warrant than in the draft Framework Decision on communication data retention and proposed to agree on the following solution regarding Article 7:

- the second sentence of Article 7 is deleted.
- communication data not already in the possession of the executing authority prior to the issuing of an EEW covering the communication data is excluded from the scope of the first instrument on the EEW, with a view to its inclusion in a later instrument under conditions to be determined.

Many delegations could accept this approach. **DELETED** and COM entered reservations.

g. Legal basis

The proposal for a Framework Decision implies an obligation for Member States to ensure that specified communication data is retained for a specified period of time. This obligation may cover data which otherwise would have to be erased pursuant to Directive 2002/58/EC on privacy and electronic communications.

The proposal for a Framework Decision is based on Article 31(1)(c) and 34(2)(b) TEU. The Commission reserved at an early stage of the negotiations a scrutiny reservation on the legal basis, and maintained that position at the JHA Council on 2 December 2004. After having studied the question, the Commission has entered a reservation on the legal basis. The Commission services have in 7735/05 COPEN 64 JUR 138 given the reasons for this reservation. In the view of the Commission, the parts of the proposal providing for a harmonisation of the categories of data to be retained and the period for retaining such data fall within EC competence and would need to be adopted on the basis of Article 95 TEC.

The Legal Service of the Council has given its opinion on the question in 7688/05 JUR 137 COPEN 62 TELECOM 21. The Legal Service has come to the conclusion that the harmonisation of data to be stored by service providers during a given period and setting up the duration of that period are matters for the Community's sphere of competence, and has specified that these aspects may not be the subject of a Framework Decision based on Title VI TEU, as such a Framework Decision would affect the provisions of Directive 2002/58/05 and would thus be adopted in breach of Article 47 TEU. It follows from the conclusions that other parts of the draft Framework Decision, such as Article 6 (access to retained communication data) and Article 7 (requests for transmission of retained communication data under judicial cooperation in criminal matters), do fall within Title VI TEU.

The Commission is in the process of preparing a proposal for a Directive on retention of communication data.

At the JHA Council on 2 and 3 June 2005, a majority of delegations thought that the draft instrument belonged in the third pillar.

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.

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]:

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] The recitals have not been fully examined.

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] Presidency proposal drawing on the **DELETED** 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 95/46/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 should 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, it is open to Member States to take measures to reduce that burden through making appropriate contributions towards the costs incurred by Industry to comply with any obligations arising from the implementation of this Framework Decision.[1]

HAS ADOPTED THE PRESENT DECISION:

Article 1[2]

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[3], generated or processed[4] 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 not apply to the content of exchanged communications, including information consulted using an electronic communications network.

---

1 Several delegations entered reserves on the proposal for a Recital.

2 Scrutiny reservation on Article 1 by **DELETED**.

3 **DELETED** entered a scrutiny reservation on the application of the expression "communication", which is defined in Directive 2002/58/EC.

4 **DELETED** 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;

- national rules on retention of communication data that provide for consideration to be given to the necessity and proportionality of imposing any obligation to retain communication data upon a provider of a publicly available electronic communications service or a public communications network, taking account of either or both the market share of the provider and the size of the network relative to the size of the market; [1]

- 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 and customs cooperation;[2]

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

[1] Presidency proposal.
[2] Scrutiny reservation by **DELETED**.

Article 2

Definitions

For the purpose of this Framework Decision,

1. 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.[1] the term “telephone service” means services which include voice calls, data calls, conference calls, voicemail calls, Short Message Services, Enhanced Media Services and Multi-Media Services;

3. the term "unsuccessful telephone calls” means any telephone calls which are connected to its destination but are unanswered, because the called party does not take the call or the called party is engaged upon another call;

4. the term "Internet Communication Services" means Internet e-mail and Internet Telephony.

[1] New text inserted to clarify the scope of the list of data to be retained in Article 3 in particular narrowing the scope of Internet services covered.

Article 3 [1] [2]

Retention of communication data

1. Each Member State shall take the necessary measures to ensure that, for the purpose set out in Article 1, at least the following communication data are retained to the extent it is generated or processed by providers of a publicly available electronic communications service or a public communications network in the process of supplying communication services:–

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

a).[3] Concerning Fixed Network Telephony

i) The calling telephone number.

ii) Name and address of the subscriber or registered user[4].

b).[5] Concerning Mobile Telephony

i) The calling telephone number.

ii) Name and address of the subscriber or registered user.

c).[1] Concerning Internet Access and Internet Communication Services:

---

1 Scrutiny reservations by some delegations.
Scrutiny reservation by **DELETED** concerning communication data relating to health insurance and road toll.
Some delegations underlined the importance of keeping the content of communications out of the scope (see in this context Article 1(3)).

2 Changes made are indicated as compared with the Working Document discussed at the meeting.

3 Scrutiny reservation by **DELETED**.

4 Proposal by **DELETED** to add "at the time of the connection" here and elsewhere through the text.

5 Scrutiny reservation by **DELETED**.

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

ii) The User ID of the source of a communication.[2]

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

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

3. Data necessary to identify the destination of a communication:

a). Concerning Fixed Network Telephony[3]

i) The called telephone number or numbers.

ii) Names and addresses of the subscribers or registered users.

b). Concerning Mobile Telephony

i) The called telephone number or numbers.

ii) Names and addresses of the subscribers or registered users.

c).[4] Concerning Internet Access and Internet Communication Services:

i) The Connection Label or User ID, of the intended recipient of a communication.[5]

ii) Name and address of the subscriber or registered user of the Connection Label or User ID of the intended recipient of the communication.

---

1 Scrutiny reservation by **DELETED**, which wanted to ensure coherence between the wording of (a)(3) and (b)(3).

2 Scrutiny reservation by **DELETED**.

3 Scrutiny reservation by **DELETED**.

4 Scrutiny reservation by **DELETED**, which wanted to ensure coherence between the wording of (a)(3) and (b)(3).

5 Scrutiny reservation by **DELETED**.

4. Data necessary to identify the date, time and duration of a communication.

   a). Concerning Fixed Network Telephony and Mobile Telephony:

      i) The date and time of the start and end of the communication.

   b). Concerning Internet Access and Internet Communication Services:

      i) The date and time of the log-in and log-off of Internet sessions based on a certain time zone.[1]

5. Data necessary to identify the type of communication:

   a). Concerning Fixed Network Telephony and Mobile Telephony
   i) The telephone service used.

   b) Concerning Internet Access and Internet Communication Services

      i) The Internet Communication Service used.[2]

6. Data necessary to identify the communication device or what purports to be the device.

   a) Concerning Fixed Network Telephony

      i) The calling and called telephone numbers.

   b)[3] Concerning Mobile Telephony

      i) The calling and called telephone numbers.

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

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

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

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

---

1 Scrutiny reservation by **DELETED**.
2 Presidency proposal. See also the new Article 2, point 2.
3 Scrutiny reservation by **DELETED**.

c) Concerning Internet Access and Internet Services

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

ii) The asymmetric digital subscriber line (ADSL) or other end point of the originator of the communication.

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

7. Data necessary to identify the location of mobile equipment.

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

b) The location label (Cell ID) at the end of the communication.[1]

c) ….[2]

d) Data mapping between Cell IDs and their geographic location at the time of the communication.

8. Member States shall take appropriate measures that are necessary and proportionate for the purpose of the technical implementation of paragraph 1.

[1] Scrutiny reservation by **DELETED**.

[2] **DELETED** proposes as c) "Location labels (Cell ID) throughout the communications". Scrutiny reservations by **DELETED** on this proposal.

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, 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. Any Member State which decides to make use of paragraphs 2 or 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 at least every 5 years.

---

[1] Scrutiny reservations by **DELETED** on Article 4.

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

Article 5[1]

Data security and data protection

Each Member State shall ensure that communication data retained under this Framework Decision is subject, as a minimum, to the rules implementing Article 17 of 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 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;[2]

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

---

1 **DELETED**, supported by some delegations (**DELETED**), 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).
DELETED would examine if the new explicit reference to Article 17 of Directive 95/46/EC could meet its concerns.
DELETED entered a scrutiny reservation, but would examine if the change from "the rules adopted pursuant to Directive 95/46/EC to "the rules implementing Directive 95/46/EC" meet concerns expressed by that delegation.
COM thought Article 5 could be replaced by a simple reference to Directive 95/46/EC.
Scrutiny reservations by some delegations.

2 **DELETED** thought it could be considered to include wording to the effect that the measures must match those taken regarding the network concerned.

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 (**DELETED**) 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.[1] Each Member State may for a period of up to two years[2] from the expiry of the deadline referred to in paragraph 1 defer from its application of this Framework Decision the retention of communications data relating to any or all of the following communication data:

(a) unanswered telephone calls on Fixed Network Telephony or Mobile Telephony;[3]

(b) Enhanced Media Services and Multi-Media Services on Fixed Network Telephony or Mobile Telephony;

(c) Internet Access and Internet Communication 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.

---

1 Scrutiny reservations by some delegations (**DELETED**).

2 Scrutiny reservations by some delegations (**DELETED**) that the additional transitional period of two years was too long.

3 Reservation by **DELETED** and scrutiny reservation by **DELETED**.

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.