COUNCIL OF THE EUROPEAN UNION

Brussels, 24 May 2005

8864/1/05 REV 1

LIMITE

COPEN 91 TELECOM 33

NOTE

from :	Presidency
to :	Council
No. prev. doc. :	8864/05 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 INTRODUCTION

Coreper examined on 19 May 2005 the above draft Framework Decision on the basis of 8864/05 COPEN 91 TELECOM 33. In accordance with the instructions given by Coreper, Articles 2(2) and 6 were examined by the JHA Counsellors on 20 May 2005.

The text resulting from the proceedings is set out in the Annex.

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 Commission has entered a general scrutiny reservation.

The Council is invited to examine the questions set out under II below. Certain other questions are set out in footnotes to the text.

II QUESTIONS SUBMITTED TO THE COUNCIL

a. Article 2 - list of communication data to be retained
Article 4 - time periods for retention of communication data

The Presidency proposal for Article 2 set out in the Annex is based on a proposal made to integrate the substance of a list proposed by the German delegation (see 7833/05 COPEN 69 TELECOM 22) in Article 2(2).

This approach was in general, and without prejudice to an examination by experts of certain technical details of the list, acceptable to delegations.

However, two delegations (DE/AT) thought that the list, as regards telephony, should be limited to successful outgoing calls. A large majority of the other delegations did not favour such a limitation.

Subject to scrutiny reservations by a number of delegations, the time periods in Article 4 were acceptable to most delegations.

Article 4(1) provides in general retention of communication data for a period of 12 months. Article 4(3) provides that Member States in exceptional circumstances may provide for a shorter period. The period must, however, be of at least 6 months. UK/CZ thought that the minimum period of 6 months may be too long for certain types of data. SE entered a scrutiny reservation and would prefer to exclude telephony from the scope of Article 4(3).

The Council is invited to:

- *confirm agreement on the Presidency approach regarding Article 2. This approach implies a minimum list of the communication data to be retained. The list should be mainly functional (focusing on what it should be possible to read from the data) with, however, some technical specifications concerning different types of telecommunications. The technical specifications should be kept to a minimum so as to avoid a need for a frequent update of the list.*
- *examine whether the list in Article 2(2), as regards telephony, should be limited to successful outgoing calls, or whether a shorter list should be considered for unsuccessful outgoing calls.*
- *agree that a specific and flexible procedure be established by the Working Party, with a view to ensuring that the list of Article 2(2) would not be rendered obsolete due to technological developments.*
- *agree on Article 4. In case no agreement is reached on paragraph 3 of Article 4, the Council is invited to ask the Working Party to examine for which data a minimum lower than 6 months may be necessary, having in mind that paragraph 3 should only apply exceptionally for specific data.*

b. Article 6 - access to retained communication data
Article 7 - judicial cooperation

Article 6 was slightly reworded at the JHA Counsellors meeting in order to meet concerns expressed by AT. The new wording was, subject to scrutiny reservations by some delegations, met by positive first reactions. The Commission entered a reservation and thought Article 6 should be deleted.

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. Several delegations and the Commission 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.

It appeared that the delegations in favour of the second sentence could accept applying the present mutual assistance arrangements on communication data. That kind of data already exists and can already at present be subject to a mutual assistance request. But it would be a new situation if this data would be covered by the European Evidence Warrant. The present draft of the EEW appears to cover communication data. The application of the EEW on this data could, for some Member States, imply a restriction of the scope for refusing to deliver communication data as compared with the present situation.

In the light of the discussions, the Presidency suggested that a way forward may be to address this matter in the context of the EEW rather than in the draft Framework Decision on communication data retention. In order not to delay the adoption of the first instrument on the EEW, it could be considered to exclude communication data not already in the possession of the executing authority prior to the issuing of the warrant and deal with such data in a second stage.[1] Many delegations could accept this approach. ES and COM entered a reservation.

The Presidency invites Coreper/Council to:

- *agree on Article 6 set out in the Annex*
- *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.*

[1] This would involve the inclusion of a reference to communication data in Article 3(2) of the EEW draft. Article 3(2) of the EEW draft would apply. References are based on 8416/05 COPEN 79.

c. 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 data retention.

The four delegations of the Member States having submitted the proposal for a Framework Decision (FR/UK/SE/IR), supported by some delegations that thought that the proposal had been correctly based on Title VI TEU. Several delegations entered scrutiny reservations on the issue, which would need to be examined at higher level.

Coreper/Council is invited to examine the question of the legal basis and its possible impact on proceedings, having in mind that the European Council in its declaration of 25 March 2004 on combating terrorism has called for the adoption of an instrument on data retention by June 2005.

III. CONCLUSION

Coreper/Council is invited to examine the questions under II above with a view to reaching final agreement on the draft as soon as possible, having in mind that the European Council in its declaration of 25 March 2004 on combating terrorism has called for the adoption of an instrument on data retention by June 2005.

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] [2]

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 adequate manner

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 preamble will be examined at a later stage.

[2] 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 involving the use of electronic communications systems. This proposal relates only to data generated as a consequence of a communication 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 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 a certain additional period 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, 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 has been acceded to by the member states and to which reference are made in the instruments on judicial co-operation in criminal matters adopted under Title VI of the Treaty on European Union.

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. The 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 the Framework Decision involves appropriate consultation with the Industry.

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.[4]

---

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 DE proposed the following new recital:
"10. The mere storage of traffic and location data represents a significant intrusion into the personal liberties of the users of telecommunications services - particularly those contained in Directives 95/46/EC and 2002/58/EC as well as those in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. As such, in an area of freedom, security and justice, the introduction of a legal obligation on the part of network operators and service providers to store such data for a certain period of time is justifiable only if this is necessary to preserve important interests within a democratic society. Notwithstanding additional statuary regulations with regard to access to stored data in the Member States, this necessity emerges from the great importance of the subsequent assessment of traffic and location data, particularly for solving terrorist crimes and other serious offences. This is because historical traffic and location data often offer the only promising investigative approach for an effective resolution of such crimes, and their availability for a determined period of time may be reliably ensured only with a statutory storage obligation."

2. This Framework Decision shall apply to all means of electronic communication[1], including in particular:

(a)[2] Telephony excluding Short Message Services, Enhanced Messaging Services and Multi Media Messaging Services.

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

(c) Internet access and internet services .

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

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.[3]

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

---

[1] AT proposed "…to all means of publicly available telecommunication in public networks". Some delegations reacted positively. Others thought it would confuse and that Article 1(1) covered the point. Scrutiny reservation by ES/SE/SK.

[2] Points (a) and (b) may be merged, depending on the outcome of discussions on Article 4(3).

[3] 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 user[1] of 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 legal or natural person subscribing to a publicly available electronic communications service for, private or business purposes, without necessarily having used the service.

[1] Scrutiny reservation by UK.

2.[1] [2] [3] Communication data to be retained for the purpose set out in Article 1 include:[4]

(a) Data necessary to trace and identify the source of a communication which includes personal details, contact information and information identifying services subscribed to[5], and which shall at least include the following data:

1. Concerning fixed Network Telephony

a) The calling and called telephone number.

b) Names and addresses of the callers, to whom the telephone numbers were registered at the time of the connection.

c) Telephone service used.

2. Concerning Mobile Telephony

a) The calling and called telephone number and if available the equipment label (IMEI).

b) Telephone service used.

c) Names and addresses of the callers, to whom the telephone numbers were registered at the time of the connection.

3. Concerning Internet

a) The dynamic and static IP address allocated by the Internet access provider to a connection.

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

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

---

[1] See point II.a of the cover note. Article 2(2)(b), (c), (d), (e) and (f) may be amended/deleted depending on the final version of Article 2(2)(a). FI has made some suggestions which will be further discussed by the experts.

[2] Reservations by some delegations on point (b) - "routing" - and point (f) - "throughout the duration".

[3] DE/AT thought that in respect of telephony only successful outgoing calls should be covered.

[4] AT proposed the following text:
"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."

[5] UK proposed: "Data necessary to trace and identify the source of a communication and user data or subscriber data related to that source.". SE proposed: "Data necessary to trace and identify the source of a communication and user data and subscriber details related to that source.".

(b) Data necessary to identify the routing and destination of a communication.[1]

(c) Data necessary to identify the time and date and duration of a communication, and which shall at least include the following data:

Concerning Fixed Network Telephony, Mobile Telephony and Internet:

a) Start,

b) duration or end of the connection,

as indicated by the date and time thereof based on a certain time zone.

(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[2] and which shall at least include the following data:

Concerning Mobile Telephony: the location label (Cell ID) at the start of the connection.

---

[1] SE proposed: "Data necessary to identify the intermediate and final destination of communication.".

[2] UK proposed: "Data necessary to identify the location at the start, the end and, where it exists, throughout the duration of the communication".

Article 3[1]

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.[2] Member States shall take appropriate measures for the purpose of the technical implementation of paragraph 1.

[1] It has been suggested that Articles 3 and 4 could be merged.

[2] The inclusion or otherwise of Article 3(2) depends on further discussions on Article 2.

Article 4[1] [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 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[3] in relation to means of communication identified in Article 1(2)[4] 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 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 See point II.a of the cover note.

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

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

4 Scrutiny reservation by SE, which thought that the reference to Article 1(2) should be replaced by a reference to Article 1(2)(b) and (c) (the former text).

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 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, supported by UK, 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. Some support was expressed for the two first indents of the proposal by SE.

Article 6[1]

Access to retained communication data

Each Member State shall ensure that access <u>for the purposes referred to in Article 1</u>[2] 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 <u>and the conditions to be fulfilled</u>[3] in order to get access to retained data and to preserve accessed data shall be defined by each Member State in national law;

(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 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;

---

1 See point II.b of the cover note.
2 Change made to meet concerns by AT. Scrutiny reservations by some delegations.
3 Scrutiny reservations by DE/SE.

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]

Article 8

Implementation

Member States shall take the necessary measures to comply with this Framework Decision (…) 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] See point II.b of the cover note.

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.

_____