COUNCIL OF THE EUROPEAN UNION

Brussels, 27 September 2005

12660/05

Interinstitutional File: 2004/0813 (CNS)

LIMITE

COPEN 149
TELECOM 95

REPORT

from :	Article 36 Committee
dated :	20-21 September 2005
to :	COREPER/Council
No. prev. doc. :	11586/05 COPEN 121 TELECOM 82 12236/05 COPEN 142 TELECOM 90
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 Declaration of the European Council of 25 March 2004 on combating terrorism provides that an instrument on retention of communication data should be adopted by June 2005. The proposal on data retention made in accordance with this mandate in April 2004 by FR/IR/SE/UK has been dealt with as a matter of priority and urgency under the Irish, Netherlands and Luxembourg Presidencies. It has, however, not been possible to respect the deadline set by the European Council, and efforts have been further intensified under the UK Presidency. In its declaration of 13 July 2005 on the EU response to the London bombings on 7 July 2005, the JHA Council has provided that the draft Framework Decision on data retention should be agreed by October 2005.

The Presidency is strongly committed to reaching agreement on the substance of the proposal at the October 2005 JHA Council. The Presidency also holds the view that serious consideration will need to be given to the proposal for a Directive on data retention, which the Commission adopted on 21 September 2005.

At its meeting on 20-21 September 2005 the Article 36 Committee examined a number of outstanding questions on the above draft on the basis of doc. 12236/05 COPEN 142 TELECOM 90. A specific question regarding the scope of the European Evidence Warrant in relation to data retention was also considered by the Article 36 Committee on the basis of doc. 11586/05 COPEN 121 TELECOM 82 with a view to resolving the reserves on Article 7 of this Framework Decision.

The Chairman informed delegations on the discussions on data retention at the informal JHA Council in Newcastle Gateshead on 8 and 9 September 2005.

The COM informed delegations of the issues which were raised in the proposal for a Directive on data retention which the COM adopted on 21 September 2005.

The text resulting from 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 (including NL) on the draft. The Commission has entered a general scrutiny reservation.

II OUTSTANDING QUESTIONS

The issues which are outstanding are set out below. Reference is made to the Annex for details.

a. Costs and benefits: Recital 16 and Article 1(3)

The JHA Council agreed at its meeting in December 2004 that particular consideration should be given to the proportionality of the draft Framework Decision. The issue of costs and benefits of the measure was discussed at the JHA Council on 2 and 3 June 2005 and again at the informal JHA Council on 8 and 9 September 2005.

Recital 16 leaves it open to each Member State to decide on possible contributions to Industry to cover costs incurred by Industry by the implementation of the Framework Decision and simply encourages Member States to consult with Industry on the practicality and cost of retaining data. Recital 16 remains subject to scrutiny reservations by HU/SK.

The Working Group had considered a Presidency proposal for a new indent of Article 1(3) which provides that Member States may make exceptions from the general obligation to retain data taking into account the market share of the service provider concerned and the size of the network relative to the size of the market. As most delegations were opposed to this proposal, the Presidency withdrew it. However, AT/DE thought that it should be reinserted in the text.

COREPER/Council is invited to agree Recital 16 and Article 1(3) as set out in the Annex.

b. Articles 2, 3 and 8(3) - the list of data to be retained

The main questions remaining are the following:

- In respect of the **Internet,** the list had in the light of discussions in the Working Party on 4 and 5 July 2005 been restricted to cover only Internet e-mail and Internet Telephony (Article 2(4)). This was, in particular, linked to discussions on the practicality and the costs involved in retaining Internet data over extended periods of months. However, some delegations (BE/DK/ES/LT/SE/IT) thought that logs of web browsing, Internet chat and peer-to-peer communications should also be covered. Other delegations (AT/FI/NL/DE) expressed concerns that the inclusion of such data might not only have an impact on the costs incurred but also require more in-depth considerations in respect of a clear distinction between traffic data and content data which might risk delaying discussions.

- At the meeting of the Article 36 Committee on 20-21 September 2005, FI made the proposal to restrain the obligation to retain Internet data to "providers of publicly available electronic communications services". Several delegations (SE/DK/ES/PL) have entered scrutiny reservations on this proposal.

- The revised Article 8(3) proposed by the Presidency provides that Member States for a transitional period of 2 years may choose not to retain data regarding unsuccessful call attempts; enhanced media services and multi-media services; and internet access and internet communication services. DK/ES/FR believe that the transitional period is too long, whereas DE/AT/EE/CZ/LV believe that it does not go far enough to address their concerns at being obliged to retain data on **unsuccessful call attempts**. FI/HU/NL also have reservations.

In order to address the reservations in relation to Internet data set out above, the Presidency proposes the compromise package in the Annex whereby "Internet chat" is included in Article 2(2) along with the wording proposed by FI ("provided by publicly available electronic communications service providers"). In conjunction with that, a "review clause" is inserted in Article 8.

COREPER/Council is invited to agree to this package as means of striking a balance between the divergent positions and to agree the text in Articles 2, 3 and 8, lifting their reserves as set out in the footnotes in the Annex.

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 (DE/FI//LV/NL/PT) have maintained their scrutiny reservations on Article 4 on the basis that the retention periods can only be agreed once Articles 2, 3 and 8 have been agreed and the list of data to be retained consequently finalised.

COREPER/Council is invited to agree on Article 4 as set out in the Annex.

d. Article 5 - Data security and data protection

At the Article 36 Committee meeting the Presidency's proposal to address reservations by some delegations (AT/FI/SI) was agreed, subject to a scrutiny reservation by the COM. The COM thought that Article 5 could be replaced by a reference to Directive 95/46/EC.

COREPER/Council is invited to agree to the current text of Article 5.

e. Article 7 - judicial cooperation

The first sentence of Article 7 of the draft Framework Decision on retention of communication data proposes that Member States should execute cross-border requests for retained communication data in accordance with "applicable instruments on judicial co-operation in criminal matters". These instruments are at present in particular the 1959 Convention on mutual assistance in criminal matters and its Protocols and, for some Member States that have ratified it, the 2000 Convention on mutual assistance in criminal matters between the Member States and its Protocol. In future, the EEW may apply.

The second sentence of Article 7 provides that the requested State may make its consent to a request for retained communication data subject to any conditions which would have to be observed in a similar national case. During discussions on the draft Framework Decision on retention of communication data, several delegations and the Commission called for the deletion of the second sentence, which, in their view, would allow requests for mutual assistance to be refused to a wider extent than provided for under existing instruments. Several other delegations insisted on maintaining the second sentence. This was in particular linked with the possible consequences of the application in the future of the EEW to retained communications data.

Based on the discussions in the Working Party and a proposal made by the Luxembourg Presidency, the Presidency made the following proposal for a compromise solution to the Article 36 Committee (see in detail doc. 1156/05 COPEN 121 TELECOM 82):

- the deletion of the second sentence of Article 7 of the draft Framework Decision on retention of communication data.
- an explicit exclusion of retained communication data from the scope of the first instrument on the EEW.
- a Council declaration stating that retained communication data should be included in the scope of the second instrument on the EEW (proposal to be expected in 2007 according to the Hague Action Plan) under conditions to be determined but that for the present time requests for retained communications data should be executed in accordance with the 1959 European Convention and, as applicable, the 2000 EU Convention on mutual assistance in criminal matters, and their respective Protocols.

Subject to a scrutiny reservation by DK, this was acceptable to a majority of delegations. LV/AT/FR/CZ/SE offered explicit support. However, the NL/IT/DE thought the second sentence of Article 7 should be maintained. COM suggested the deletion of the entire Article 7.

COREPER/Council is invited to find an agreement on the basis of the Presidency compromise proposal.

f. 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.

On 21 September 2005, the Commission adopted 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. In continuation of these discussions, the Presidency suggested at the informal JHA Council on 8 and 9 September 2005 that due consideration would have to be given to the forthcoming Commission proposal.

COREPER/Council is invited to examine the issue of the legal basis with a view to finding an agreement.

III CONCLUSION

COREPER is invited to examine the outstanding issues as set out above.

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].

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.

---

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

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. (…) Recognising that the retention of data no longer required for business purposes can represent practical and financial burdens upon Industry, Member States should ensure that implementation of this Framework Decision involves appropriate consultation with Industry with particular regard to the practicality and cost of retaining that data.[1]

HAS ADOPTED THE PRESENT DECISION:

Article 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, generated or processed (…) 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] Scrutiny reservation by HU/SK.

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;

- (…)[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;

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

[1] The Presidency put forward a proposal for an indent reading:

"national rules on retention of communication data that provide for consideration to be given to 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"

Most delegations were opposed to its inclusion. The Presidency therefore withdrew its proposal. AT/DE thought it should be reinserted in the text.

Article 2[1]

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. [2] the term "Internet Communication Services" means Internet e-mail, Internet chat and Internet Telephony (Voice Over Internet Protocols) provided by publicly available electronic communication service providers[3];

3. the term "telephone service" means calls (including voice, voicemail, conference or data), supplementary services (including call forwarding and call transfer), messaging and multi-media services (including Short Message Services, Enhanced Media Services and Multi-Media Services);

---

1 Scrutiny reserve on Article 2 by GR/EE. Scrutiny reservations on paragraphs 2-6 by AT/CZ/ /PL/CY/SI/LV/HU/FI.

2 Several delegations (BE/DK/ES/LT/SE/IT) have reservations that the draft Framework Decision excludes web server logs, File Transfer Protocol (FTP) logs and traffic data relating to "peer-to-peer" communications. Other delegations (AT/FI/NL/DE) are against the inclusions of these types of data. Scrutiny reservation by PL.

3 Scrutiny reservations by SE/DK/ES.

4. the term “User ID” means an unique identifier located to a person as they subscribe or register to an Internet Access Service or Internet Communication Service;

5. the term “Cell ID” means the identity of the cell from which a mobile telephony call originated or in which it terminated;

6. the term "unsuccessful call attempt” means a communication in a which a telephone call has been successfully connected but is unanswered or there has been a network management intervention.

Article 3[1]

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[2] 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) Concerning Fixed Network Telephony and Mobile Telephony

i) The calling telephone number.

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

b) (…)

---

[1] Scrutiny reservation by FI/CZ/SI/GR. Scrutiny reservation by DE concerning communication data relating to health insurance. DE is working from the premise that the health system which is being prepared pursuant to special legal principles is not covered under the scope of application of the Framework Decision and in any case reserves the right not to apply obligations regarding data retention in the course of national implementation thereof. Scrutiny reservation on paragraphs 2-6 by AT, linked to the deletion of the wording "connection label" in paragraph 2(c).

[2] FI thought "generated or processed" should be replaced by "generated and processed".

c) Concerning Internet Access and Internet Communication Services:

i) (…)[1]

ii) The User ID(s) allocated.

iii) The User ID and telephone number allocated to any communication entering the public telephone network.

iv) Name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, User ID (…) or telephone number was allocated at the time of the communication.

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

a) Concerning Fixed Network Telephony and Mobile Telephony

i) The number(s) dialed (the called telephone number or numbers), and in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed.

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

b) (…)

[1] See Article 3(4)(b)(i)

c) Concerning (…) Internet Communication Services:

i) The (…) User ID or telephone number of the intended recipient of an Internet telephony call.

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

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 (…):

i) The date and time of the log-in and log-off of the Internet Access Service based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet Access Service provider to a communication, and the User ID or the subscriber or registered user.

c) Concerning Internet Communications Services:

i) The date and time of the log-in and log-off of the Internet Communication Service based on a certain time zone.

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 Communication Services

i) The Internet Communication Service used.

6. Data necessary to identify users' communication equipment or what purports to be their equipment.

a) Concerning Fixed Network Telephony

i) The calling and called telephone numbers.

b)[1] 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.

c) Concerning Internet Access and Internet Communication 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.

[1] Scrutiny reservation by ES which is linked to the issue of pre-paid cards.

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) (….)

d) Data identifying, by reference to Cell IDs, the geographic location of cells during the period for which communications data is retained. [2]

8. In ensuring the technical implementation of paragraph 1[3], Member States shall take appropriate measures that are necessary and proportionate (…).

[1] Reservation by AT/DE. Scrutiny reservation by FI.
[2] Scrutiny reservation by LV.
[3] Proposal by the Presidency to address the scrutiny reservations by SE/DK

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 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 DE/FI/LV/NL/PT on Article 4.

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 and shall be subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorised or unlawful disclosure or access, and against all other unlawful forms of processing;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that disclosure of, and access to, the data is undertaken only by authorised persons whose conduct is subject to oversight by a competent judicial or administrative authority;

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

[1] Scrutiny reservation by COM that thought that Article 5 could be replaced by a simple reference to Directive 95/46/EC.

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 refusal of requests for mutual assistance to a wider extent than is provided for under existing instruments. Other delegations maintain that the sentence should be included in Article 7.

The Presidency has proposed, as a compromise solution, to delete the second sentence in conjunction with an explicit exclusion of retained communication data from the scope of the first instrument on the European Evidence Warrant and a Council Declaration stating that retained communication data should be included in the scope of the second instrument on the EEW. Several delegations (LV/AT/FR/CZ/SE) supported this proposal. NL/IT/DE were against the deletion of the second sentence. Scrutiny reservation by DK. COM thought the whole Article should be deleted. See also point II.e of the cover note.

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, relating to:

(a) unsuccessful call attempts 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.

---

1 Scrutiny reservations by some delegations (AT/ DE/EE/FI/HU/).

2 Scrutiny reservations by some delegations (DK/ES/FR) that the transitional period of two years is too long.

3 Reservation by AT/DE/EE/CZ/LV on the obligation to retain unsuccessful call data, and scrutiny reservation by NL.

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. The Council shall thereafter review the list of data to be retained in particular with reference to the possibility of including additional types of Internet data.

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.

_____