



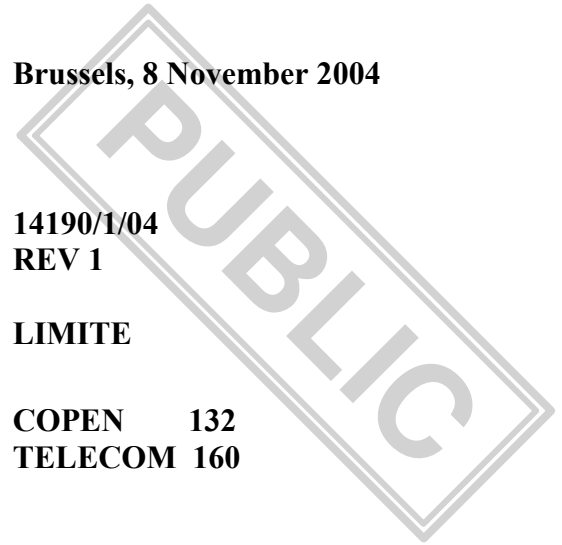
**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 8 November 2004

**14190/1/04
REV 1**

LIMITE

**COPEN 132
TELECOM 160**



NOTE

from : Presidency

to : Article 36 Committee

No. prev. doc. : 13353/04 COPEN 122 TELECOM 150

Subject : Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.

On 19 and 20 October 2004, the Working Party on cooperation in criminal matters examined the draft Framework Decision on the basis of doc. 13353/04 COPEN 122 TELECOM 150, having in mind the exchange of views of the Article 36 Committee on 7 and 8 October 2004. At this stage, the Commission has not yet taken a position on the draft Framework Decision. A revised text is set out in the annex to this note. The text has been established in the light of the discussions in the Working Party as well as the exchange of views on the draft in the Article 36 Committee on 7 and 8 October 2004. Changes compared with doc. 13353/04 COPEN 122 TELECOM 150 are indicated. The Presidency invites CATS to examine the following questions at this stage for the purpose of giving guidance for further proceedings in the Working Party.¹

¹ A background paper of the Presidency on the relation between the legal basis and the issues referred to in these questions will be distributed separately.

Question 1

Scope

Article 1 (1) as set out in doc. 8958/04 CRIMORG 36 TELECOM 82 provides for an approximation of Member States' legislation on the retention of data processed and stored by providers. Article 3 as set out in doc. 8958/04 CRIMORG 36 TELECOM 82 provides that "each Member State shall take the necessary measures to ensure that data processed and stored by (...) providers, is retained". The obligation to retain data is limited to data already currently stored by providers for billing, commercial or any other legitimate purposes. At the meeting of the Working Party on 19 and 20 October 2004, a majority of delegations was in favour of covering not only the data currently stored by providers. Instead, the scope should be extended to all traffic data as defined in Article 2 including data processed but currently not stored. The decision of this matter may affect the procedure to be followed (see question 2 and 3). The Presidency is considering bringing this matter to the Council.

CATS is invited to consider whether the Framework Decision should in principle also cover the retention of data processed but currently not stored by telecommunication providers.

Question 2

Legal basis

The question arises whether the widening of the scope has serious consequences for telecommunication providers which could possibly affect the legal basis for an exclusive procedure in the Third Pillar.

CATS is invited to decide whether the Working Party should consider possible consequences relating to the legal basis of the draft Framework Decision when dealing with the types of data to be retained.

Question 3

Costs

The retention of data for a longer period than the current one and/or the retention of additional data by providers may entail costs. In course of the discussions in the Working Party as well as at the Workshop of the Commission, the question was raised who would have to bear those costs.

Furthermore, the question was raised whether the Framework Decision should address this issue so as to provide for equal regimes on costs for providers throughout the European Union. If the issue of possible costs is left to domestic legislation, Member States' legislation may differ in terms of whether the providers have to bear the costs (in part) or not and may lead to unequal conditions for providers.

The Presidency invites CATS to decide whether the issue of possible costs as a consequence of mandatory retention by providers should be dealt with in the Framework Decision?

Question 4

Period of retention

Article 4 (1) as set out in doc. 13353/04 COPEN 122 TELECOM 150 provides for a retention period of 12 months. Article 4 (3) allows for establishing shorter periods of retention for data in relation to certain means of communication (in particular SMS, EMS and MMS provided as part of telephony service as well as Internet communication including e-mail). A minimum period for the retention of the latter data is not provided for. As the aim of the draft Framework Decision is to approximate Member States' legislation, the Presidency proposes to instruct the Working Party to consider adopting a fixed minimum period for forms of communication referred to in Article 1 (1a) (b) and (c).

CATS is invited to decide whether, in the light of the aimed harmonisation, a minimum period for the retention of traffic-data relating to certain means of telecommunication (e.g. Internet and e-mail) should be established.

Draft Framework Decision

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

THE COUNCIL OF THE EUROPEAN UNION¹

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,²

Having regard to the Opinion of the European Parliament,

Whereas:

(...)

¹ Although some remarks were made on the preamble it needs further examination. FR: Paragraph 6 of the preamble would need re-wording if the scope of retention in the Framework Decision went beyond data, which are already processed and stored. DE stated that the proportionality of the Framework Decision would need examination.

² 8958/04 CRIMORG 36 TELECOM 82, considering CRIMORG 96 TELECOM 149 13227/04 is expected to be submitted to the European Parliament soon.

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.

HAS ADOPTED THE PRESENT FRAMEWORK 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 retention¹ of data processed [and stored]² by providers of a publicly available electronic communications service or a public communications network, for the purpose of (...) ³, investigation, detection and prosecution of [...] criminal offences⁴.

¹ There was no substantial support for the Presidency proposal to use the words “continued retention”.

² During examination of Article 3 the proposal to delete the word “stored” had support by most delegations. It seems logical to re-examine Article 1 with a view to the use of the word “stored”.

³ The reference to "prevention" has been deleted in connection with the deletion of Article 1(3) and the addition of the first indent of Article 3(4). Most delegations agreed with this shift. IE and UK opposed to deleting the word “prevention”.

⁴ Most delegations are against a limitation to certain categories of criminal offences. Therefore the words “terrorist and other serious” used in COPEN 122 should be deleted. AT and PT prefer not deleting the word “serious”.

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

- (a) Telephony excluding Short Message Services, Electronic Media Services and Multi Media Messaging Services.
- (b) Short Message Services, Electronic Media Services and Multi Media Messaging Services provided as part of any telephony service.
- (c) Internet Protocols including Email, Voice over Internet Protocols, world wide web, file transfer protocols, network transfer protocols, hyper text transfer protocols, voice over broadband and subsets of Internet Protocols numbers - network address translation data.

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

3. (...)

4. This Framework Decision is without prejudice to:

- national rules on retention of data (processed and stored by providers of a publicly available electronic communications service or a public communications network) for the purpose of prevention of crime;
- the rules applicable to judicial co-operation in criminal matters with regard to the interception and recording of telecommunications;
- activities concerning public security, defence and national security (i.e. State security);

¹ The text of Article 1(1a)(a), (b) and (c) corresponds to former Article 2(3)(a), (b) and (c). The "chapeau" is re-worded so that it covers the substance of former Article 2(4). NL prefers two categories by bringing the first two categories in one new category.

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

Article 2

Definitions

1. For the purpose of the retention this Framework Decision:
 - (a) ¹The term ‘data’ in this Framework Decision means² traffic data and location data as set out in Article 2 of the Directive 2002/58/EC, including³ (...) subscriber data⁴ and user data related to these data.⁵
 - (b) User data means data relating to any legal or natural person⁶ using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to the service.
 - (c) Subscriber data means data relating to any legal or natural person⁷ subscribing to a publicly available electronic communications service for, private or business purposes, without necessarily having used the service.

¹ The words “The definition of” were deleted.

² UK prefers “includes” instead of “means”. Scrutiny reservation by SE.

³ Proposal of the General Secretariat to use the word “including” here.

⁴ DE proposes to delete “subscriber data” here.

⁵ MT suggests further examination of the definition of ‘data’ in relation to Article 3. FR suggests deleting the last part of the sentence of Article 2(1)(a).

⁶ AT and CZ scrutiny reservation on whether legal person should be included in the definition of the user. In the original proposal user data could only refer to a natural person.

⁷ In the original proposal subscriber data could only refer to a natural person.

2. Data to be retained for the purpose set out in Article 1 include¹:
- (a) Data necessary to trace and identify the source of a communication which includes personal details, contact information and information identifying services subscribed to.²
 - (b) Data necessary to identify the routing and destination of a communication.
 - (c) Data necessary to identify the time and date and duration of a communication.
 - (d) Data necessary to identify the telecommunication.
 - (e) Data necessary to identify the communication device or what purports to be the device.
 - (f) Data necessary to identify the location at the start and throughout the duration of the communication.
3. (...) ³
4. (...) ⁴

¹ Wording proposed by the Presidency. Article 2(2) needs further elaboration. The aim of Article 2(2) is to define what ‘data’ are needed for the purpose of Article 1. Most delegations want more reflection on the desirable level of specificity of these data in this Article.

² Scrutiny reservation SE.

³ See footnote 3 on page 5.

⁴ See footnote 3 on page 5.

Article 3

Retention of data

Each Member State shall take the necessary measures to ensure that, for the purpose of providing judicial co-operation in criminal matters, data as defined in Article 2(2) when¹ processed ² by providers of a public communications network or publicly available electronic communications services is retained in accordance with the provisions of this Framework Decision.

Article 4

Time periods for retention of data

1. Each Member State shall take the necessary measures to ensure that stored data referred to in Article 3 shall be retained for a period of 12 months³ following its generation. Relating to subscriber data, this period shall run from the end of the subscription.⁴
2. Member States may have longer periods for retention of data dependent upon national criteria when such retention constitutes a necessary, appropriate and proportionate measure within a democratic society.

¹ Proposal by the Presidency to relate Article 3 to the definition in Article 2(2). Scrutiny reservations of all delegations.

² A substantial majority favoured deletion of the words “and stored for billing, commercial or any other legitimate purposes” from the earlier draft.

³ IE, PT, MT scrutiny reservation on deletion of a maximum period of retention.

⁴ IE, PT, and IT prefer a longer minimum period. SK prefers a shorter minimum. Most delegations agree with a minimum of twelve months. ES, HU and GR are in favour of a general minimum for all data. FIN referring to the effect of the period on the costs makes a scrutiny reservation to the period.

3. A Member State may allow shorter periods of retention for data types covered by Article 2(2) in relation to means of communication identified in Article 1(1a)(b)¹ and (c) should the Member State not find acceptable, following national procedural or consultative processes, the retention periods set out in paragraph 1 of this Article.²

4. A Member State deciding to make use of paragraph 3 at any time must give notice to the Council and to the Commission stating the alternative time scales being adopted for the data types affected. Any such derogation must be reviewed annually.³

Article 5 (Former Art. 7)⁴

Data Security

Each Member State shall ensure that, regarding data retained under this Framework Decision, providers subject to the retention obligation must comply, as a minimum, to the following data security principles [...]:

- (a) the retained data shall be of the same quality as those data on the network;
- (b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing;

¹ The Presidency invites the Working Party to consider whether the reference to Article 1(1a)(b) should be retained.

² Some delegations ES, HU and GR would prefer more harmonisation here. Most delegations have not yet take a definitive stand on this issue.

³ This paragraph was originally the last sentence of paragraph 3 of this Article.

⁴ Article 5, 6 and 7 in this document is drawn from a redraft proposal by the Belgian delegation. It restructures the matters dealt with in these Articles. Most delegations still have scrutiny reservations concerning the proposed text, but there is general support for the restructuring.

- (c) all data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved;
- (d) (...) ¹

Article 6

Access to retained data

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

- (a) data shall be accessed for specified, explicit and legitimate purposes by competent authorities on a case by case basis in accordance with national law and not further processed in a way incompatible with those purposes;
- (a bis) the process to be followed in order to get access to retained data and to preserve accessed data shall be defined by each Member State in national law; ²
- (a ter) each Member State shall define in national law the categories of offences for which access to retained data is authorised ;
- (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;

¹ Transferred in new Article 7. See footnote 4 on page 10.

² Formerly in previous Article 7. See footnote 4 on page 10.

- (c) data accessed by competent authorities shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the data were collected or for which they are further processed;
- (d) the confidentiality and integrity of the data shall be ensured;
- (e) data accessed shall be accurate and, every reasonable step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

Article 7¹

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

A request made by a Member State to another Member State, for access to data referred to in Article 2, shall be made and responded to in accordance with the instruments on judicial co-operation in criminal matters adopted (under Title VI of the Treaty on European Union)². The requested Member State may make its consent to such a request for access to data subject to any conditions which would have to be observed in a similar national case.³

¹ Originally Article 5. see footnote 4 on page 10.

² To be reviewed according to the discussion in the working group.

³ A provision on the types of crime for which co-operation shall be possible may be inserted here. If not, §1 joined with the MLA regime allows the refusal to execute the request if the access is not possible under national legislation for the type of crime mentioned in the request.

Article 8

Implementation

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

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

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

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.
