COUNCIL OF THE EUROPEAN UNION

Brussels, 24 October 2005

13624/05

LIMITE

COPEN 166
TELECOM 113

NOTE

from :	Presidency
to :	COREPER
No. prev. doc. :	13428/05 COPEN 161 TELECOM 110 13036/05 COPEN 156 TELECOM 102
Subject :	Data retention

Following discussions in COREPER on 19 October the Presidency undertook to present further information providing legal clarity and, to the extent possible, certainty on:

- the consequences, from the perspective of the State aid / competition provisions of the Treaty, of having no provision on the reimbursement of costs in an instrument on data retention (the new instrument); and
- the continued application of the derogation to erase data under Article 15(1) of the 2002 Telecomms Directive in relation to both retention periods and scope of the new instrument.

In light of this, the Presidency invites COREPER to consider the proposals at Annex I for amendments to the draft Directive in the hope that these represent the basis for an agreement. Specifically, the Presidency proposes that:

- Article 1(1): retention of data for the **purposes** of the investigation, detection and prosecution of criminal offences. The draft Directive would not therefore cover retention for the purposes of crime prevention, nor would it be limited to serious crime.

- Article 3(2): **rules on access** to data to be regulated by national law in each Member State subject to the existing obligations imposed by the 1995 Data Protection Directive, as reflected in Recitals 1 and 15 to the draft Directive.

- Articles 7 and new Article X: **retention periods** for all types of data on the list to be based on a minimum of 6 months but allowing Member States to go up to a maximum period of 2 years retention for those data. Thereafter, Member States to have the ability to extend the retention periods in relation to matters falling within the new instrument under the terms of the proposed safeguard clause in the new Article X.

- The revised Article 11 would clarify that **Article 15(1)** of the 2002 Telecomms Directive would continue to apply:
  - in relation to types of data falling outside the scope of the new instrument and
  - for retention for purposes other than those covered by the new instrument.

- Recital 13 and Article 10: no provision on **costs,** with the result that such matters will be left to national arrangements in Member States. To address the need for legal clarity and certainty on the consequences for Member States of making such payments to operators, the Commission has offered the declaratory statement in Annex III to this document.

The Presidency attaches at Annex II the relevant Articles from the Framework Decision. In the light of discussions in COREPER, and without prejudice to the question of whether the Council should adopt a Directive or a Framework Decision, the Presidency will make appropriate amendments.

Finally, in relation to the **list of data** to be retained, and in particular data on location of mobile telephone equipment and unsuccessful call attempts, the Presidency will present a paper for COREPER on 3 November.

ANNEX I: Proposed amendments to the draft Directive as in 12671/05 COPEN 150

This is without prejudice to further changes that may be required on other outstanding issues, such as the list of data.

Article 1

Subject matter and scope

1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications network with respect to the processing and retention of certain data, in order to ensure that the data is available for the purpose of the …, investigation, detection and prosecution of … criminal offences ….

Article 3

Obligation to retain data

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation…..

Article 7

Periods of retention

Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of <u>not less than 6 months and for a maximum of two years</u> from the date of the communication, with the exception of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of six months.

Article 10

Costs

….

Article 11

Modification of Directive 2002/58/EC

In Article 15 of Directive 2002/58/EC a paragraph 1a is inserted, as follows:

"1a. Paragraph 1 does not apply to the retention of data mentioned in Article [4] of Directive 2005/.../EC for the purposes referred to in Article 1(1) of that Directive".

New Article X

Safeguard Clause

1. A Member State facing particular circumstances warranting an extension for a limited period of the maximum retention period referred to in Article 7 may take the necessary urgent measures. The Member State shall immediately notify the Commission and inform the other Member States of the measures taken by virtue of this Article and indicate the grounds for introducing them.

2. The Commission shall, within six months after the notification as referred to in paragraph 1, approve or reject the national measures involved after having verified whether or not they are a means of arbitrary discrimination or disguised restriction of trade between Member States and whether or not they shall constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within this period the national measures shall be deemed to have been approved.

3. When, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission shall immediately examine whether to propose an adaptation of this Directive.

Recitals

(11) Given the importance of traffic data for the …. investigation, detection, and prosecution of … criminal offences …, as demonstrated by research and the practical experience of several Member States, there is a need to ensure that data which are processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a certain period of time.

(12) The categories of information to be retained reflect an appropriate balance between the benefits for the …, investigation, detection, and prosecution of the … criminal offences involved and the level of invasion of privacy they will cause; the applicable retention period of six months rising to two years …, also strikes a reasonable balance between all the interests involved.

(13) …..[recital on costs deleted]

(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the …, investigation, detection and prosecution of … criminal offences …., cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

ANNEX II

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 text has been duplicated here from 12894/1/05 COPEN 153 REV 1 only insofar as it relates to the issues in the covering paper.

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.

3. This Framework Decision is without prejudice to:

- national rules on retention of communication data processed or generated by providers of a publicly available electronic communications service or a public communications network for the purpose of prevention of crime;

- (…)

- the rules applicable to judicial co-operation in criminal matters with regard to the interception and recording of telecommunications;

- the rules applicable to the exchange of information within the framework of police and customs co-operation;

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

Article 3

Retention of communication data

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

Article 4

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.

Article 5

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.

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.

Recitals

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.

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.

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.

The Commission considers that reimbursement by Member States of additional costs incurred by undertakings for the sole purpose of complying with requirements imposed by national measures implementing this Directive for the purposes as set out in the Directive would be compatible with the Treaty in accordance with the provisions of Article 87.3.b"