COUNCIL OF THE EUROPEAN UNION

Brussels, 16 November 2005

14328/05

LIMITE

COPEN 177
TELECOM 132

NOTE

from :	Presidency
to :	COREPER
Subject :	Data retention: trialogue discussions with the European Parliament

Annex I contains a report of the discussions which took place with the European Parliament in Strasbourg on 15 November. The Presidency noted the positive tone of the meeting and the ongoing political willingness to work for a deal on the draft Directive by the end of this year, but it was also clear that the European Parliament is looking for flexibility from the Council on a number of key issues as set out in the report. The Presidency would welcome views from COREPER on whether and the extent to which flexibility exists within the Council in the areas identified, particularly in relation to (i) scope; (ii) unsuccessful calls; (iii) penal sanctions; and (iv) data protection / data security.

In particular the Presidency believes that it would be useful to explore in COREPER the question of additional safeguards on data protection and data security, including sanctions for breaches of those safeguards. To that end, the Presidency has prepared some proposals in Annex II which it invites COREPER to agree as a basis for further discussions with the European Parliament. Those proposals draw heavily on what was agreed for inclusion in the draft Framework Decision and / or reflect existing obligations in the 1995 Data Protection Directive.

The Presidency also notes that the European Parliament attaches considerable importance to an adequate review mechanism in the draft Directive properly informed through the collection of statistics on the use of retained data. To that end, the Presidency invites COREPER to agree as a minimum the Commission proposal in Article 9 of the draft Directive on the collection of statistics.

If COREPER can agree these provisions (Annex II and Article 9 of the draft Directive), the Presidency will use them as a basis for the second trialogue meeting scheduled for 22 November.

The Presidency is conscious that there are other outstanding issues of substance to which COREPER needs to return, in particular the scope of the obligation to retain data which is generated or processed. COREPER will consider these at future date.

ANNEX I

REPORT OF TRIALOGUE MEETING WITH THE EUROPEAN PARLIAMENT ON 15 NOVEMBER 2005

On 15 November 2005 the Presidency met with representatives of the European Parliament and in the presence of the European Commission at a trialogue meeting. In accordance with the mandate given by COREPER and document 14023/05 COPEN 172 TELECOM 123, the Presidency set out the "centre of gravity" in the Council and the elements that any Directive would have to include. The Presidency made clear in particular that the discussions in the Council were based on the premise that Article 15(1) of Directive 2002/58/EC would continue to be applicable in relation to data not covered by the draft Directive and in relation to retention of data for purposes other than those covered by the draft Directive.

The representatives of the European Parliament informed the Presidency that the members of the LIBE committee had tabled 238 amendments to the Commission proposal for the Directive. The LIBE committee was now working to consolidate these into a more limited number of compromise amendments (approximately 24) that would replace some, but not necessarily all, of the initial amendments. Once finalised the LIBE committee undertook to forward these to the Presidency, who will circulate them to delegations.

The key elements of the amendments were as follows:

1. Data should be retained for the purpose of investigation, detection and prosecution of serious criminal offences, where "serious criminal offences" would be defined by way of reference to the offences listed in Article 2(2) of the Framework Decision on the European Arrest Warrant, and not for prevention purposes.
2. The list of data should be shifted from the Annex to the body of the text of the draft Directive and the references to comitology procedures should be deleted.
3. The draft Directive would replace Article 15(1) of Directive 2002/58/EC with the effect that the list of data in the draft Directive would be a "maximum list" and that Member States could not provide, on a national basis, for the retention of other data.
4. Location data should be limited to data at the start of a communication.

5. The list of data should, concerning Internet data, be limited to log-on and log-off data (i.e. the IP address).
6. Data on unsuccessful call attempts should not be included, but Member States should have the possibility to provide for their retention on the basis of national legislation.
7. The draft Directive should contain detailed provisions on access to the retained data, including provisions to the effect that: access should only be allowed where undertaken for the purpose of investigating, detecting or prosecuting a serious offence by a competent national authority; that the data should be accessed by way of a "push system"; that the authorisation by a competent national authority was required; that the access by other government bodies or other parties should be prohibited; and that data-mining should be prohibited.
8. It was essential to include detailed provisions on data security and data protection and that (criminal) sanctions for their infringements should be introduced.
9. The retention period should be between 6 months and 12 months - whether these periods should be understood as a minimum and a maximum period for all data covered by the draft Directive or whether there should be different retention periods depending on the categories of data (Internet data, telephone data) needed to be discussed further.
10. All additional costs (investment and operating costs) incurred by providers, including the costs for additional data protection and data security measures, should be reimbursed by Member States.
11. The obligation to collect statistics proposed by the Commission should be extended and serve as a basis for revision of the draft Directive. A "sunset clause" should provide for the expiry of the draft Directive after a specified period unless its continuation was agreed by co-decision with the EP.

The Commission noted that it has not yet taken a formal position on the possible amendment to be made to its original proposal. It nonetheless made clear its full commitment to work flexibly with the Council and EP on the instrument. On the derogation in Article 15(1) of the Directive 2002/58/EC, it was the Commission's view that the derogation should continue to operate for those purposes outside the scope of the current draft Directive. For purposes falling within the scope of the draft Directive, the derogation under Article 15(1) should no longer apply. The Commission also took note of the European Parliament's views on comitology, showing flexibility.

The Presidency undertook to report on its discussion with the EP to the Council and to explore in COREPER the scope for flexibility, including on such issues as data protection / security and penal sanctions. On access, the Presidency noted the Council's view that access was best regulated at national level. The Presidency noted the risk that moving away from the centre of gravity would have within the Council on its ability to reach agreement. It was agreed that a further meeting between the Council, the Commission and the Parliament would take place on 22 November.

ANNEX II

I Additional recitals:

(15bis) It should also be recalled that the obligations incumbent on providers concerning measures to ensure data quality which derive from Article 6 of Directive 95/46/EC as well as the obligations on providers and controllers concerning measures to ensure confidentiality, security and protection of data which derive from Articles 16 and 17 of Directive 95/46/EC, are fully applicable to the data retained in accordance with the present Directive.

(16bis) In this context, it should be recalled that Article 24 of Directive 95/46/EC imposes an obligation on Member States to sanction infringements of the provisions adopted pursuant to Directive 95/46/EC; Article 15(2) of Directive 2002/58 imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58; Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems provides that the intentional illegal access to information systems, including to retained data, shall be made punishable as a criminal offence.

(16ter) It should be borne in mind that the right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC, to receive compensation from the controller which derives from Article 23 of Directive 95/46/EC, applies also in relation to the unlawful processing of any personal data which is retained pursuant to the present Directive.

(17bis) It should be borne in mind that the 2001 Council of Europe Convention on Cybercrime as well as the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data may also cover data retained pursuant to this Directive.

II Additional provisions in the text:

Article 7bis

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with the present Directive:

(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 or alteration, unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that access to the data is undertaken only by specially authorised personnel;

(d) that providers undertake regular and systematic self-auditing to ensure that the applicable rules on data protection are respected; and

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

Article 8bis

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive regarding the security of the stored data.

2. These authorities shall act with complete independence in exercising the functions referred to in paragraph 1.

Article 11bis

Remedies, liability and sanctions

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall in particular take the necessary measures to ensure that intentional access to or transfer of data retained in accordance with the present Directive which is not authorised by the provider of publicly available electronic communication services or of the public communications network responsible for retention, or which is not permitted under national law, shall be punishable by effective, proportionate and dissuasive sanctions.

_____