COUNCIL OF THE EUROPEAN UNION

Brussels, 23 October 2002

12721/1/02 REV 1

LIMITE

CRIMORG 86

NOTE

from :	Presidency
to :	Multidisciplinary Group on Organised Crime (MDG)
No. prev. doc. :	10358/02 CRIMORG 49 MI 119 10405/02 CRIMORG 51 MI 121
Subject :	Draft Council conclusions on information technology and the investigation and prosecution of organised crime

The Presidency's proposal has been initially discussed at the MDG meeting on 8/9 July 2002. As a result of the discussion a new document that has taken account of the remarks and comments made by delegations has been drafted by the Presidency. A number of delegations have maintained or again laid down scrutiny reservations (France, Italy, Spain, Austria, Finland, Ireland, Greece, the Netherlands and Portugal).

After the meeting the Presidency has decided to further develop the document by taking account of the remarks and comments received from delegations and the Commission services. A number of amendments have therefore been made to the text in the Annex. In keeping with the concerns voiced by several delegations, the Presidency has also changed the order of the recommendations and merged some of them into one. The MDG agreed that a new document would be needed in order to contribute any written comments and the Presidency hereby presents this document. Delegations are requested to submit their comments and observations in writing **no later than 1st November 2002** to the attention of Mr. Peter Nath, 175 rue de la Loi, B-1048 Brussels, Belgium; tel. +32-2-285-6677, facsimile +32-2-285-8832, email: peter.nath@consilium.eu.int.

_____

THE COUNCIL OF THE EUROPEAN UNION

(1) CONSIDERS that the maintaining and developing of the Union as an area of freedom, security and justice as laid down in Article 2 of the Treaty of European Union and the creation of the high level of safety in this area which is the general objective of Article 29 of the Treaty depends on the possibility to carry out criminal investigations and prosecutions sufficiently, thoroughly and effectively, while respecting human rights and fundamental freedoms as laid down in Article 6 of the Treaty.

(2) CONSIDERS that general use by all the inhabitants of the European Union of the possibilities afforded by the constant developments in the information technology field is an essential element in economic and social development throughout the European Union, and that the confidentiality of electronic communications should be limited only when such limitations constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security and defence, public security and the prevention, investigation, detection and prosecution of criminal offencesf[1].

(3) CONSIDERS it essential that any legislation on electronic communications respects the requirements regarding privacy and the protection of personal data which stem from the European Convention on Human Rights of 4 November 1950; the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data; Community law, notably the general principles of Community law, including those referred to in Article 6 (1) and (2) of the Treaty of the European Union, Article 15 (1) of Directive 2002/58/EC[2] on the processing of personal data and the protection of privacy in the electronic communications sector, and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; the rights and principles set out by the Charter of Fundamental Rights of the European Union[3].

---

1 This was previously recommendation 7.
2 OJ L 201, 31.7.2002, p. 46.
3 This was previously recommendation 6.

(4) NOTES with concern that the technological innovations brought about by the continuous development of the internet and other electronic communications services as well as the increase in electronic banking, in parallel with their great benefits to society, also make it possible for criminal organisations to further exploit these technologies[1].

(5) NOTES 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 useful tool in the investigation and prosecution of crime in particular organised crime[2].

(6) URGES all parties concerned (governments, parliaments, law enforcement, industry, data protection authorities and other interested parties), as a matter of priority, to engage in an open and constructive dialogue aimed at finding solutions to the issue of traffic data retention that satisfies both the need for effective tools for prevention, detection, investigation and prosecution of criminal offences and the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy, data protection and secrecy of correspondence. In this connection the EU Forum on Cyber-crime set up by the European Commission could be used to enhance coordination between key stakeholders[3].

(7) AGREES that [...] rules [...] on the approximation of Member States' legislation on the obligation of electronic communication services providers to retain specific traffic data concerning electronic communications for a limited time should be established and implemented in light of the dialogue between the parties concerned, in order to ensure that such traffic data is available when it is necessary for the prevention, detection, investigation and prosecution of criminal offences [...][4].

---

1 This was previously recommendation 8.
2 This was previously recommendation 3.
3 This was previously recommendation 4.
4 This was previously recommendation 5.

(8) RECOMMENDS that the Member States and the European Union while respecting the right to free encryption constantly seek possible solutions in partnership with industry to the problems faced by law enforcement authorities through the increased use of encryption, so as to strike the right balance between the citizens' right to privacy and to secrecy of their correspondence and the judicial and law enforcement authorities' ability to investigate and prosecute organised crime effectively[1].

(9) POINTS OUT that it is expressly stated in the political guidelines in the Action Plan to combat organised crime adopted by the Council on 28 April 1997 that there is a need to pave the way for a policy ensuring that law enforcement and judicial authorities have the possibility to prevent and combat the criminal misuse of new technologies.

(10) REFERS to the Council conclusions of 20 September 2001, which highlight the need to ensure that judicial and law enforcement authorities are able to investigate criminal acts involving the use of electronic communications [...], while striking a balance between the protection of personal data and the law enforcement authorities' need to gain access to data for the purposes of criminal investigations and prosecutions.

(11) RECOMMENDS that, to the greatest possible extent, the Member States and the European Union follow developments within the communications and information technology field and constantly ensure that the law enforcement authorities receive further training in this area. In this connection maximum use should be made of the possibilities offered by the Framework Programme on police and judicial cooperation in criminal matters (AGIS), managed by the Commission in co-operation with the Member States[2].

---

1 This was previously recommendation 16.
2 This was previously recommendation 14.

(12) URGES the Member States to increase their efforts to comply with the provisions laid down in the Council Act of 29 May 2000[1] to ensure that decisions on the interception of electronic communications and on access to data concerning electronic communications are taken with the greatest possible speed and in respect of fundamental rights and freedom of individuals, especially in the case of mobile electronic communications, where the free movement of mobile users across borders is not matched by a legal seamless interception system, with the consequent need for close and speedy cooperation between the Member States[2].

_____

[1] Council Act of 29 May 2000, establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States and the European Union, Title III (Interception of Communications), in: OJ C 197/1, 12.7.2000, pp. 1-23.

[2] This was previously recommendation 15.