



**COUNCIL OF
THE EUROPEAN UNION**

**Brussels, 24 June 2002 (28.06)
(OR. da)**

10358/02

**CRIMORG 49
MI 119**

NOTE

from : Incoming Presidency
to : Multidisciplinary Group on Organised Crime (MDG)
Subject : Draft Council conclusions on information technology-related measures
concerning the investigation and prosecution of organised crime

THE COUNCIL OF THE EUROPEAN UNION

- (1) POINTS OUT that a high level of safety within an area of freedom, security and justice depends on it being possible to carry out criminal investigations and prosecutions sufficiently thoroughly and effectively.
- (2) NOTES that because of the significant growth in the possibilities afforded by telecommunications, information relating to the use of telecommunications is now a particularly important and useful tool in the investigation and prosecution of criminal organisations.

- (3) FINDS that general access by all the inhabitants of the European Union to 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 such access should only be subjected to those limitations and restrictions which are necessary having regard to national security, the fundamental rights of citizens, the investigation of serious crimes or other serious concerns relating to regional and global development.
- (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 this technology increasingly to be improperly used by criminal organisations.
- (5) POINTS OUT that the confidentiality of telecommunications can only be restricted where necessary to safeguard national interests or national security or to investigate serious offences.
- (6) 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 abuse of the new technologies.
- (7) REFERS to the Council conclusions of 20 September 2001, which highlight the need to ensure that law enforcement authorities are able to investigate criminal acts involving the use of electronic communications systems, 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.

- (8) REITERATES the requirement for implementation of communications interception measures to respect the right to privacy laid down in Member States' national laws and accordingly highlights the provisions of Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, adopted by the European Parliament and the Council on 15 December 1997.
- (9) URGES that within the very near future, binding rules should be established on the approximation of Member States' rules on the obligation of telecommunications services providers to keep information concerning telecommunications in order to ensure that such information is available when it is of significance for a criminal investigation.
- (10) CONSIDERS that such binding rules must be established taking account of the requirements regarding privacy and the processing 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, 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.
- (11) RECOMMENDS that the necessary mechanisms to monitor developments in the information technology field be established with a view to putting forward proposals as soon as possible for measures and initiatives to ensure that the law enforcement authorities are able to react immediately and effectively to the new challenges arising from future developments in the possibilities of information technology.
- (12) RECOMMENDS that, to the greatest possible extent, the Member States follow developments within the communications and information technology field and constantly ensure that the law enforcement authorities receive further training in this area.

- (13) URGES the Member States to increase their efforts to ensure that decisions on the interception of telecommunications and on access to information concerning telecommunications are taken with the greatest possible speed, especially in the case of mobile telecommunications, where the communicating parties can move from country to country without warning, with the consequent need for close and speedy cooperation between the Member States.
- (14) RECOMMENDS that the Member States and the Union constantly seek possible solutions to the problems posed for law enforcement authorities by the increased use of encryption, so as to take the necessary account both of citizens' lawful interest in keeping their communications private, and of the law enforcement authorities' ability to investigate and prosecute organised crime effectively.
-