Declaration adopted by the

European Data Protection Authorities

in Cyprus on 11 May 2007

In the Council of the European Union a proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters is subject of debate.

Creating a harmonised and high level of data protection covering police and judicial activities in the Union is indeed a crucial element for respecting and safeguarding fundamental rights such as the right of protection of personal data when creating an area of freedom, security and justice.

The initiatives in the European Union to improve the fight against serious crime and terrorism have in common the willingness to achieve that within the Union national borders become increasingly less relevant when defining the conditions for exchanging data between competent authorities so that law-enforcement data may be made available by various means including providing direct access to national data bases.

These initiatives clearly demonstrate that the Union's obligation to help improving the fight against serious crime is not limited to setting conditions for the exchange of information between the Member States; the initiatives clearly also have an impact on data processing on a national level preceding any possible exchange. It is evident that any development in this area must be balanced with adequate and harmonised data protection rights and obligations in which mutual trust is a key element.

Throughout the European Union data protection legislation applicable to law enforcement activities differs in nature and substance and therefore certainly does not provide for a harmonised data protection approach of law-enforcement information, data subjects rights and effective independent supervision.

In view of the increasing use of availability of information as a concept for improving the fight against serious crime and the use of this concept both on a national level and between Member States, the lack of a harmonised and high level of data protection regime in the Union creates a situation in which the fundamental right of protection of personal data is not sufficiently guaranteed anymore.

Referring to its Position Paper on law enforcement and information exchange in the EU (April 2005) and recalling its declarations of Krakow (2005), Budapest (2006) and London (2006), all European Data Protection Authorities therefore call upon the Member States represented in the Council of the European Union and the European Parliament to explore every possibility for creating such a harmonised and high level of data protection throughout the European Union.

The European Data Protection Authorities are aware of the fundamental discussion in the Council on the scope of the proposed framework decision: should it apply only to data exchanged between Member States or should it apply to all processing activities by police and judicial authorities.

Reiterating the national impact of the Union's initiatives and the clear risk that limiting the scope to data that are exchanged or may be exchanged between Member States would make the field of application of the proposed framework decision particularly unsure and uncertain, the European Data Protection Authorities **stress that only a comprehensive scope covering all types of processing of personal data could provide individuals with the necessary protection.**

The European Data Protection Authorities **furthermore stress that also on other data protection principles the version of the draft framework decision as presented by the German Presidency on 13 March 2007 does not present a solid and high data protection regime** and has neither taken on board our European data protection Authorities' Opinion issued on 24 January 2006 nor the EP's opinion from May 18, 2006.
Whilst the draft decision has brought about some improvements in view of achieving a harmonised processing framework, it is as yet unsatisfactory as regards the safeguards provided to ensure citizens' right to privacy.
This is especially the case if account is taken of the already existing European data protection legislation, in particular, the legal framework created by those national lawmakers when transposing directive 95/46/EC, also made it applicable to the processing of personal data in the sector at issue.
Furthermore, the European Data Protection Authorities reiterate that it is necessary to preserve the existing data protection safeguards at national level by adopting binding European instruments.

With a view to making a real improvement in the third pillar data protection, the Conference of European data protection Authorities underlines the following key principles to be dealt with in the future important legislation of the framework decision:

- Purpose limitation: necessity to define clearly the legitimate purposes allowing the processing of personal data in the framework of police and judicial cooperation in criminal matters without maintaining any general clause allowing for further processing "for any other purposes". The purpose limitation principle is a key principle in the EU directive and Convention 108.

- Data categories: the processing of special categories of data is prohibited unless specific conditions are met and specific guarantees are foreseeing in the national legislation (Art. 8 EU Directive, Art. 6 Convention 108). Furthermore, appropriate safeguards shall be provided for the processing of biometric and genetic data.

- Categories of data subject: It is a requirement of the principle of proportionality to reintroduce distinctions between the different categories of data subject concerned by the processing for police and law enforcement purposes.

- Regulation of data transfers to third countries: It is a requirement of the adequacy principle that common criteria and a procedure for the adoption of the measures necessary in order to assess the level of data protection in a third country or international body is defined before transferring the personal data and not leave it entirely to the discretion of Member States. Fixing an EU standard in such a procedure is a requirement for achieving harmonisation in Europe and the concept of adequacy findings corresponds to the provision in the Council of Europe Convention of 28 January 1981 for the protection of Individuals.

- Information of the data subject: Information of the data subject shall provide for complete provisions including the identity of the data controller, the possible recipients and the legal basis for processing. Any restrictions shall be precise and limited.

- Right of access: the regime of the right of access must be in line with the requirements of the European Human Rights Convention and the case law. In excluding in some cases the possibility to

have an effective right of appeal, the current proposal is not in line with those requirements. Furthermore the supervisory authorities or appeal jurisdiction shall have the right to communicate information to the data subject in case of unjustified refusal. The exception to the right of access shall also be more limited.

- Notification and prior checking: notification and prior checking of processing to the supervisory authority should, where appropriate, constitute a precondition for processing. Prior checking shall be carried out by the national data supervisory authorities. The possibility of exemptions from publication of notification will have to be considered according to the nature of processing.

- Supervisory authorities: the concept of a JSA shall be understood as an independent supervisory authority. The framework decision shall provide for its composition, tasks and competences. It shall be endowed in particular with consultative, investigative and intervention powers.

The European Data Protection Authorities also recognise the importance of adopting the framework decision as soon as possible. However, the proposal presently under discussion will not provide for a sufficiently harmonised and high level of data protection. The fundamental character of the framework decision not only for safeguarding the rights of the citizens of the European Union but also for law enforcement, justifies a discussion that is not compromised by a strict timeframe.

The European Data Protection Authorities therefore call upon the Council to allow itself more time for the negotiations to develop a framework decision offering a high level of data protection.

The European Data Protection Authorities are, of course, willing to contribute further in the process of adopting such a framework decision and suggest to be heard by the Council working group to explain their positions.