Spring Conference of European Data Protection Authorities, Krakow, 25-26 April 2005

DECLARATION

Various initiatives at EU level aim to establish the European Union's objective of an area of freedom, security and justice. In its new multi-annual programme − The Hague Programme − the Union reiterates the need to fight organised cross-border crime and to repress the threat of terrorism.

The 2005 Spring Conference of European Data Protection Authorities is well aware of the need for closer co-operation between law enforcement authorities, within the EU and with third States. At the same time it is evident that the 1981 Council of Europe Convention on data protection (Convention 108) applicable in the Union and in Member States is too general to effectively safeguard data protection in the area of law enforcement. Given the Union's obligation to respect human rights and fundamental freedoms, initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection.

The Conference noted with satisfaction that The Hague Programme subjects the availability principle to strict conditions of respect for data protection principles.

The Conference also welcomes the approach of the Commission in advocating a core set of guiding principles for the treatment of personal data under the Third Pillar, to be developed in close co-operation with data protection authorities. Furthermore, the Conference is encouraged by the steps taken by the Commission towards developing a new legal framework for data protection in the Third Pillar which, it is hoped, will provide an appropriate set of rules applicable to law enforcement activities consistent with the current level of data protection in the First Pillar. When developing these detailed data protection rules, the standard of data protection found in Directive 95/46/EC should serve as a basis.

The need to develop a harmonised data protection approach in the Union would suggest that when the Treaty establishing a Constitution for Europe enters into force there should be a comprehensive European Law on data protection covering all areas of processing personal data.

The new legal instrument would present the most important evolution in data protection law since the adoption of the Data Protection Directive 95/46/EC and it would have large impact on the future architecture of data protection in Europe. In order to avoid a divergence between the First and the Third Pillars which would have a negative impact on enforcement and transparency and in view of the Charter of Fundamental Rights and the forthcoming Constitution for Europe which will abolish the Pillars, the Conference calls to preserve − and where necessary to regain − the coherence, the consistency and the unity of data protection. The principles of Directive 95/46 should form the common core of a comprehensive European data protection law. In particular, as regards its legal provisions, the principle of lawfulness, the data subject's rights, and the principle of enforcement must be emphasised, and as regards its institutional provisions, stress must be put on the need for an EU Working Party composed of representatives of the national and the EU Data Protection supervisory authorities acting independently, entrusted with co-operation, monitoring and advisory missions.

The Conference has adopted the attached position paper on Law Enforcement & Information Exchange in the EU. This paper is addressed specifically to the EU institutions as a constructive contribution to current initiatives, particularly the Commission's work on developing a Third Pillar instrument on data protection. The Conference of EU Data Protection Authorities is, of course, willing to contribute further to ensure that the process results in a practical framework, which also respects fundamental rights.

Position paper on Law Enforcement & Information Exchange in the EU

Background

Ever since the Treaty of Amsterdam committed Member States to creating 'an area of freedom, security and justice', there have been initiatives aimed at improving co-operation between law enforcement authorities.[1] As these EU-wide initiatives often involve the exchange of personal data, this paper has been prepared in an attempt to ensure that there are appropriate safeguards in place to guarantee a high standard of data protection, taking account of the fundamental rights enshrined in existing legal instruments.

EU Initiatives in the Field of Law Enforcement

Policy development in the field of law enforcement continues to be driven by the demands of tackling terrorism and serious crime. The proposals are varied and could have far-reaching implications. Suggestions in a recent Communication from the Commission included a proposal for each Member State to establish a register of all bank accounts, a recommendation that a more direct link should be made between measures to tackle terrorism and those dealing with organised crime, and a proposal to develop a European criminal record.[2]

In another Communication from the Commission it was suggested that there ought to be an EU information policy in the field of law enforcement, with improved access to relevant information throughout the EU and the development of a more intelligence-led approach to law enforcement. One intended result of such an information policy would be to 'promote the effective use of common or horizontal standards on access to data, clearance, confidentiality of information, reliability, data security and data protection, and

[1] Law enforcement authorities: police and judicial authorities and any other such authority with a law enforcement task.

[2] Communication from the Commission on measures to be taken to combat terrorism and other forms of serious crime, in particular to improve exchanges of information 29 March 2004 COM (2004) 221

interoperability standards for national and international databases'.[3] An information policy of this kind would seem likely to result in a convergence of the procedures followed by law enforcement authorities throughout the EU.

Building on the Tampere Programme, the Hague Programme also contains a number of proposals intended to aid the fight against terrorism and organised cross-border crime. It will be crucial to strike the right balance between these proposals and data protection safeguards and it is, therefore, encouraging to see that the Hague Programme highlights the need for 'supervision of respect for data protection, and appropriate control prior to or after the exchange'.[4]

Fundamental Rights

These various proposals, if implemented, would continue an established pattern in EU policy in this area. First, they would result in a significant increase in the exchange of information for the purposes of law enforcement, with much more personal data being exchanged between Member States. Second, the categories of person on whom data are exchanged would increase, as would the range of offences.

The processing of personal data on the scale proposed (often involving the processing of information on those who are not suspected of any crime) requires adequate legal safeguards.

The EU is obliged to respect fundamental rights, as guaranteed by the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union.

---

[3] Communication from the Commission: Towards enhancing access to information by law enforcement agencies 16 June 2004 COM (2004) 429

[4] Presidency Conclusions 4/5 November 2004 (14292/04) Annex 1: The Hague Programme

In addition to the right to respect for private and family life guaranteed by Article 8 of the ECHR and reaffirmed by Article 7 of the Charter of Fundamental Rights, the right to data protection is enshrined in Article 8 of the Charter. The Treaty Establishing a Constitution for Europe, which incorporates the Charter, also guarantees in Article I-51 the right to data protection, and stresses that compliance with data protection rules must be subject to the control of independent authorities. These rights are fundamental and any interference with them is unacceptable unless it is lawful, necessary and proportionate.

The principle of proportionality is a key concept when assessing whether these new measures are necessary. In this context it is important to consider the extent to which terrorism is used as a justification for new initiatives − many of which deal with a range of offences, including some which are significantly less serious. It is important to recognize that derogation from fundamental rights that might be justified to tackle terrorism will not necessarily be justified where other criminal activity is concerned.

Particularly welcome was the suggestion, made by Commissioner Frattini when addressing a joint meeting of the joint supervisory authorities, that the Commission would consider the feasibility of 'an *a priori* assessment of proportionality of any measures to be introduced in future, examining the impact of the proposal on fundamental rights, including the question of personal data protection'.

Data Protection & Law Enforcement in the Third Pillar

In addition to the fundamental rights outlined above, the 1981 Council of Europe Convention on data protection (Convention 108) sets out specific principles of data protection and is applicable in the third pillar.[5] More detailed provisions can be found in a Recommendation on the use of personal data in the police sector, which was adopted by the Council of Europe's Committee of Ministers.[6] Other than these instruments, the

[5] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention 108)
[6] Recommendation No. R (87) 15, of 17 September 1987

intergovernmental conventions setting up third-pillar bodies and information systems − such as the Europol Convention − contain specific provisions dealing with data protection.

EU initiatives requiring the collection, retention or exchange of personal data for law enforcement purposes are bound to highlight differences in the law on data protection throughout the EU. Such discrepancies might have unacceptable consequences from a data protection point of view, and possibly for those trying to tackle crime. For example, it would be unacceptable if a Member State, having received personal data from another Member State, were to retain those data for longer than they would have been retained in the originating Member State − or if the receiving Member State were to use the data for other purposes, or share the data with other countries in a way that would have been prevented in, or unacceptable to, the originating Member State.

Given that sensitive data are being processed on such a large scale, that close co-operation between Member States is being promoted, and that the Council hopes to reach a situation where the mere fact that information crosses borders is not relevant,[7] it is perhaps the case that the provisions of Convention 108 are too general and that there is a need to amplify and give substance to the principles contained in the Convention. The different Recommendations from the Committee of Ministers of the Council of Europe including the Recommendation on the use of personal data in the police sector demonstrate the need to adapt the general principles in order to meet the specific requirements of particular sectors. It should be noted that there have already been some steps taken in this direction. For example, Article 129 of the Convention implementing the Schengen Agreement provides for specific rules regarding police co-operation and the exchange of personal data.

In the light of recent developments, it is necessary to develop rules governing the exchange of personal data between Member States and to create a harmonised standard of data protection applicable to all law enforcement activities.

[7] The Hague Programme, Chapter 2

Personal data processed for law enforcement purposes are particularly sensitive given the consequences that might result from any improper use of these data. Furthermore, the legal environment in which law enforcement authorities operate is changing. For example, the 'availability principle' put forward in the Hague Programme would require law enforcement authorities to disclose personal data to other Member States, rather than just allowing them to do so.

For these reasons, a new legal framework applicable to law enforcement activities − as advocated by the Commission − would have to provide a tailor-made set of rules; simply reaffirming general principles would not be sufficient. Any moves in this direction would, of course, have to take account of the existing legislation (particularly the different national approaches to dealing with data protection in the area of law enforcement), the principles of the Recommendation regulating the use of personal data in the police sector, and the increasing convergence of the first and third pillars. This convergence would suggest that when the Treaty establishing a Constitution for Europe enters into force there should be a comprehensive European law on data protection covering all areas of processing personal data. Until then a framework decision on data protection in the Third Pillar in line with the existing First Pillar data protection standards is the appropriate legal instrument to establish such a comprehensive approach.

When developing more detailed data protection rules, the standard of data protection found in Directive 95/46/EC should serve as the basis, with attention then focusing on the following in particular:

1. **Purpose limitation**

   Personal data should only be collected and processed for legitimate, well-defined and specific law enforcement purposes. The object and purpose of the processing should be defined taking into account the different law enforcement activities.

2. **Data classification**

   Distinction should be made between different categories of information and the purposes for which they can be used. The different categories of data processed should

be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments. Law enforcement data are likely to include sensitive data and should be subject to a high level of scrutiny. A system of data classification may be used to implement special conditions and limitations for the use of some categories of data.

3. Data quality

In view of the character of personal data processed by law enforcement authorities, and the impact they may have on the individual's rights and freedoms, the quality of data must be guaranteed as far as possible. Provisions should be in place to ensure that data are not excessive in relation to the purposes for which they are processed and to keep data up to date. This becomes particularly important when transmitting data to other law enforcement authorities, as the receiving bodies and states might not have access to local resources that would allow them to confirm details, check accuracy and so on. It will be important to ensure that the receivers of personal data are supplied with the necessary information to use the data for the purposes for which they were exchanged and to keep them up to date. This is also recognised in the Hague Programme, which sets out the need for appropriate control prior to and after an exchange of data between Member States. Furthermore, retention periods should be fixed taking into account the categories of data and the purposes for which they are processed.

4. Sensitive data

The processing of personal data solely on the basis that they reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, and the processing of personal data concerning health or sex life should be prohibited. The processing of these data may only be carried out if absolutely necessary for the legitimate, well-defined and specific purpose of a particular law enforcement activity.

5. Non-suspects

The processing of data on persons who are not suspected of having committed any crime (other than victims and witnesses) should only be allowed under certain specific

conditions and when absolutely necessary for a legitimate, well-defined and specific purpose. The processing of data on non-suspects such as when making speculative enquiries or for the purpose of establishing whether or not a suspicion relating to a serious criminal activity might be justified, should be restricted to a limited period, and the further use of these data for other purposes should be prohibited.

6. **Collection by automated means**

   The collection of data by electronic surveillance or other automated means such as data-mining shall be provided for by specific provisions providing for the necessary safeguards

7. **Communication of data between law enforcement authorities within the EU**

   The communication of data between law enforcement authorities to be used for law enforcement purposes should only be permissible when necessary for a justifiable law enforcement task or if a clear legal obligation exists. Communication of personal data between law enforcement authorities in a Member State and between law enforcement authorities within the EU should in principle be restricted to the purpose for which those data are processed.

8. **Communication to other parties in the public and/or private sector within the EU**

   Communication to other parties in the public and/or private sector in a Member State and within the EU should only be allowed if a clear legal obligation exists or if such communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if there is an overriding public interest that requires disclosure under well defined conditions and limitations.

9. **Communication to law enforcement authorities in third states and bodies**

   There ought to be data protection safeguards in place when communicating personal data to law enforcement authorities in third states. Communication could be structured using a harmonized standard for agreements with third states and bodies taking into account the need to guarantee an adequate level of data protection. Furthermore, a

flexible legal instrument should be developed allowing communication in specific situations, even where there is no formal agreement in place. This would include situations where communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or where there is an overriding public interest that requires disclosure under well defined conditions and limitations. The use of this exception and the use of the data transmitted should be monitored.

10. Transparency

The processing of data should be made transparent as far as possible. The principle of transparency should take into account the specific character of law enforcement.

An adequate level of transparency can be achieved by introducing:

- an obligation for the controller to inform the data subject that his data are processed, unless this is impossible or incompatible with the purpose of the processing; and
- a system of notification with the supervisory authorities of any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes; and
- a system of control by the supervisory authorities, affording these authorities powers of inspection and intervention.

11. Legal remedies

Every person has the right to a legal remedy for any breach of the rights guaranteed him by these principles and the right to compensation for any damage suffered by him because of unlawful processing of personal data concerning him.

12. The data subject's rights

The data subject has the right of access, and the right to request rectification or deletion in case the data are excessive or not relevant for the purpose of the processing. Given the potential implications for the individual, it is important that there should be quick and simple procedures to enable the data subject to exercise his rights taking into account the different interests at stake. In view of the increasing exchange of personal data between Member States, these rights should be applied in a harmonised way

regardless of the Member State in which they are exercised and with respect for the different legal systems and traditions. In view of the specific character of law enforcement these rights may, after an assessment on a case by case basis, be restricted if necessary for the prevention, investigation and detection of criminal offences, and the prosecution of offenders, or to protect the rights and freedoms of third parties. In case a restriction is applied, compensatory safeguards such as a control by the supervisory authority should be guaranteed. The supervisory authorities shall co-operate with one another to the extent necessary and to render all necessary assistance to the data subject.

13. Data security

Given the sensitivity of the personal data concerned, it will be crucial to ensure that all appropriate technical and organizational measures are taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of processing. The processing of data should be subject to permanent internal controls using technical solutions such as audit trails.

Supervision

There will have to be supervision on national and at EU level to ensure that there is compliance with data protection requirements. Article I-51 of the Treaty establishing a Constitution of the European Union stipulates that compliance with data protection rules must be 'subject to the control of independent authorities'; but, at the moment, the European Data Protection Supervisor is responsible for monitoring the processing of personal data by Community institutions and bodies only, and the mandates of the joint supervisory authorities are limited to specific areas. It will be essential to develop a system of effective supervision in which all Member States participate. National supervisory authorities and supervisory authorities at EU level should be given the necessary powers and should co-operate to the extent necessary.

Conclusion

The EU Data Protection Authorities recognise that in order to tackle serious crime and terrorism there is a need to improve the system of information exchange within the Member States, between Member States and with third states. We would reiterate, however, that all new measures ought to be proportionate, respecting the fundamental rights of the individual. This paper is addressed specifically to the EU institutions as a constructive contribution to current initiatives, particularly the Commission's work on developing an instrument on law enforcement and data protection. It presents some guiding principles necessary to maintain a high level of data protection in the field of law enforcement and these principles should also serve to enhance co-operation between law enforcement authorities. The EU Data Protection Authorities are, of course, willing to contribute further to ensuring that the process results in a practical framework, which also respects fundamental rights.