

**Public Seminar in European Parliament:
"An Efficient and Accountable Police Cooperation in the EU: the way forward"**

Brussels, 18 December 2006

"Data Protection - Are Current Standards for Police Cooperation Satisfactory?"

Contribution by Mr Peter HUSTINX, European Data Protection Supervisor

I. Police cooperation and data protection

1. This seminar aims at discussing efficient and accountable police cooperation. The invitation rightly points at the Articles 29 and 30 EU and at the fact that a real common approach is still lacking. This neither ensures optimal results, nor adequate protection of rights of individuals.
2. It is my conviction that both go hand in hand. No optimal police cooperation without adequate data protection. This link is also visible in Article 30 TEU - more precisely subparagraph (1) (b). No European rules on the processing and exchange of police information without appropriate provisions on data protection. This is not just an intention, but an obligation from the Treaty itself.
3. In practice however, this order is most often reversed. Legislation is adopted in order to facilitate exchange of information, whereas the negotiations on the Framework Decision on Data Protection are far from being concluded.
4. As you will be aware, I have issued two opinions on this Framework Decision. In the second opinion, dating from only a few weeks ago, I expressed serious concerns about the level of protection resulting from the negotiations in Council. These concerns are shared by many in the European Parliament, as illustrated by the resolution prepared by the rapporteur Madame Roure.
5. I would like to use this occasion to underline some of the essential points made earlier in these opinions. Both opinions can be found on my website¹.

¹ Opinion of 19 December 2005 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005)475 final), OJ C 47, 25.02.2006, p. 27, also available at:

http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/c_047/c_04720060225en00270047.pdf

Second Opinion of 29 November 2006 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters., available at:

http://www.edps.europa.eu/legislation/Opinions_A/06-11-29_2ndOpinion_third_pillar_EN.pdf

II. Current standards are inadequate

6. In the first place, the current standards are inadequate. There is no common legal framework on the level of the European Union in the area of police cooperation that meets basic criteria of consistency and effectiveness. Of course, there are some basic rules since all Member States have to comply with Council of Europe Convention 108. This is also expressed in Schengen and Europol Conventions². Besides that, in most Member States the principles of Directive 95/46 also apply to police data.
7. However, the current situation can be seen as a patchwork: different rules for different situations, no guarantees for adequate protection in all Member States. Such a patchwork is by nature not adequate: it is essential to have harmonised rules in case of exchange of information between the States, in an area of freedom, security and justice where the borders between the Member States are losing value.
8. Moreover, as we all know, the data processed in the area of police are quite often of a highly sensitive nature. The police needs to collect, store and exchange information in such a way that investigations can be carried out effectively. Where the police needs powers to fulfil their task, the citizen is entitled to protection. The result of the need to protect society against crime may not be that the police proceeds without any control. In a democratic state under the rule of law, one needs adequate checks and balances. Data protection constitutes such checks and balances.
9. It should be added that large discrepancies between data protection in the first and the third pillar would not only affect the citizens' right to protection of personal data, but would also affect the efficiency of law enforcement and the mutual trust between the Member States.

III. Need for a wide scope

10. Secondly, the common standards in the Framework Decision need a wide scope. It is not acceptable to limit the protection to data that are exchanged between Member States and exclude domestic data.
11. This has been a major point of discussion on which I took a firm stance. As stated in the second opinion: a more limited scope is unworkable and would, if introduced, require difficult and precise distinctions within the databases of law enforcement authorities, only leading to additional complexity and costs for those authorities and moreover harming the legal certainty of individuals.
12. There is also a strategic argument in favour of the adoption of a solid Framework Decision, applicable to all processing. Solid EU-legislation protecting the citizen in all EU-internal situations would also strengthen the position of the EU in negotiations with third countries. It is difficult to ask from the United States to treat our passenger data with due care - if we are not even able or prepared to guarantee protection within our own territory.

² See e.g. Article 14.1 Europol Convention: "... each Member State shall ensure a standard of data protection which at least corresponds to the standard resulting from the implementation of the principles of the Council of Europe Convention of 28 January 1981, and, in doing so, shall take account of Recommendation No R (87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987 concerning the use of personal data in the police sector."

IV. Consistency with Directive 95/46

13. A third point is the need for consistency with Directive 95/46, the data protection directive for the first pillar. There are many arguments brought in the discussion why this first pillar-instrument would not be appropriate for police work. For instance that the right of the data subject to be informed about the processing of his data would not be compatible with police practice.
14. These arguments are not convincing at all. The data protection principles contain exceptions that enable executing other important public interests, such as effective law enforcement. Exceptions are needed and foreseen, but the citizen is entitled to protection - and not only to a weak protection - when the police process his data.
15. There is another reason why consistency is needed. The third pillar is not separated by a sort of Chinese wall from other areas of protection. Personal data are exchanged between the pillars. In many cases, it is not easy at all to determine to what pillar an activity belongs. Processing for SIS is a good example, since SIS functions under the first pillar (immigration) and under the third pillar (combat of crime). Another example is the cooperation between private companies and law enforcement. One can just think of the Data retention Directive that was heavily discussed in Parliament.
16. A consistent system with the first pillar is all the more important, as the Data retention Directive shows, since data collected by private companies are later on used for law enforcement purposes.

V. Other essential elements

17. The fourth point to be made has to do with other essential elements of data protection in the third pillar.
18. In my recent opinion, concerns were raised, mainly because of the developments in Council. In order to proceed, basically all controversial provisions were deleted or weakened. We are concerned about several issues.
19. The Commission proposal makes a distinction between different kinds of data subjects (suspects, convicted people, victims, witnesses, etc.). Data related to them should be treated differently, with specific safeguards, especially with regard to non-suspects of crimes. This distinction is important and should not be deleted.
20. The proposal should include rules on the transfer of data to and from third countries. The Commission proposal provides for an adequacy decision by the Commission, in case of transfer to a third country. It must be ensured that such transfer takes place only after examination of the level of protection in the third country. Otherwise, the EU would not protect its citizens in a satisfactory way.
21. An essential element of the right to information of the data subject is that this information is given to him spontaneously. Since the data subject normally does not know and can not know that information concerning him or her is being processed, it would be contrary to the nature of this right to require a request from the data subject. The Council seemed to require such a request.

22. Finally, the risks of the use of biometric data, such as DNA, need to be mentioned. A framework decision should address these risks, but unfortunately this issue is not dealt with.
23. These issues are relevant for police cooperation and data exchange in general. But they become more acute where police information is exchanged at a large scale (SIS I and SIS II), or when concrete ideas are developed about the principle of availability or the interoperability of data bases.
24. The development of adequate standards for data protection should thus be considered and dealt with as a pre-condition for a better cooperation. Not as a source of problems, but as a condition for legitimacy and strength.