

**Second opinion of the European Data Protection Supervisor 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**

(2007/C 91/02)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to 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 <sup>(1)</sup>,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data <sup>(2)</sup>, and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

1. On 19 December 2005, the EDPS issued an opinion <sup>(3)</sup> on the Proposal of the Commission for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. In this opinion, he underlined the importance of the proposal as an effective instrument for the protection of personal data in the area covered by Title VI of the EU-Treaty. Such an instrument should not only respect the principles of data protection as laid down in the Council of Europe Convention No 108 <sup>(4)</sup> and more specifically in directive 95/46/EC, but also provide for an additional set of rules taking into account the specific nature of the area of law enforcement. For the EDPS it is essential that the framework decision covers all processing of police and judicial data, even if they are not transmitted or made available by competent authorities of other Member States. Consistency of the protection of personal data is essential, regardless of where, by whom or for which purpose they are processed. The EDPS has made several proposals to improve the level of protection.
2. On 27 September 2006, the European Parliament adopted a legislative resolution on the Commission proposal. In general terms, the resolution has the same objectives as the opinion of the EDPS: support for the proposal in general and amendments aiming to enhance the level of protection afforded by the Framework Decision.
3. The Commission proposal is currently being discussed within Council. The Council is reportedly <sup>(5)</sup> making progress and is modifying essential elements of the text of the proposal. A serious effort is being made by the Council Presidency to make even more significant progress. It aims at reaching a common approach on the main elements by December 2006.
4. The EDPS welcomes that the Council is giving much attention to this important proposal. However, he is concerned about the direction of the developments. The texts currently being discussed within Council do not incorporate the amendments proposed by the European Parliament, nor the opinions of the EDPS and of the Conference of European Data Protection Authorities. On the contrary, in quite a few cases provisions in the Commission proposal, offering safeguards to the citizens, are deleted or substantially weakened. *As a result, there is a substantial risk that the level of protection will be lower than the level of protection afforded under Directive 95/46/EC or even under the more generally formulated Council of Europe Convention No 108 which is binding on the Member States.*

<sup>(1)</sup> OJ L 281, 23.11.1995, p. 31.

<sup>(2)</sup> OJ L 8, 12.1.2001, p. 1.

<sup>(3)</sup> OJ C 47, 25.2.2006, p. 27.

<sup>(4)</sup> Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981.

<sup>(5)</sup> Formally, there are no public documents available and the EDPS is not directly involved in the work of the Council Working Party. Documents, reflecting the state of play within Council, can be found on the website of Statewatch ([www.statewatch.org](http://www.statewatch.org)).

5. The EDPS notes that also the Libe-committee of the European Parliament has recently voiced its concerns regarding the choices of Council on this proposal for a framework decision.
6. It is for these reasons that the EDPS now issues a second opinion. This second opinion focuses on some essential concerns and does not repeat all the points made in the opinion of the EDPS in December 2005, which all remain valid.

#### *General concern*

7. In the developing area of freedom, security and justice, the exchange of police and judicial information between the Member States is becoming more and more important. Several legal instruments are proposed or have been adopted in order to facilitate this exchange of information. The EDPS underlines once more that in this context a solid legal framework which protects the data subject is needed to ensure that the fundamental rights of citizens are respected. The present (proposal for a) Framework Decision is directly linked to the proposals facilitating this exchange of information.
8. Although the EDPS recognises the importance of adopting the Framework Decision by Council as soon as possible, he warns that the rapidity of the decision making should not lead to a lowering of the standards of protection. The texts currently discussed within Council raise doubts as to whether the result will be solid enough, so as to give the citizen an effective level of protection. In the present situation, the consequence of the objective of rapidity would appear to be that possibly controversial provisions are deleted or weakened. The lack of time to reach consensus on possibly controversial provisions could result in the quality of the Framework Decision being compromised.
9. Under these circumstances, the EDPS recommends that Council allows more time for the negotiations in order to achieve a result that offers sufficient protection.

#### *Applicability to domestic processing*

10. This issue was an essential element of the opinion of December 2005 and was thoroughly discussed afterwards. Common rules on data protection should apply to all data in the area of police and judicial cooperation, and not be limited to cross-border exchanges between Member States. A more limited scope could not afford the appropriate protection, as required by Article 30(1)(b) of the EU-Treaty. This point was underlined on several occasions, also by other stakeholders besides the EDPS.
11. In his opinion of December 2005, the EDPS stated that a limitation to data that are exchanged with other Member States would make the field of application of the framework decision particularly unsure and uncertain, which would be contrary to its essential objective. At the time of collection or processing of personal data it is unknown as to whether those data will later be relevant for exchange with competent authorities in other Member States.
12. For this reason, *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.*
13. Two examples can be given to illustrate these consequences. In the first place, additional complexity and costs result from the fact that criminal files are in quite a number of cases composed of data originating from different authorities. The consequence of a limited scope would be that parts of such composed files — the parts containing data originating from authorities in other Member States — would be protected under the framework decision and that other parts would not be protected. In the second place, the legal certainty of individuals would be harmed since — in the case of a more limited scope — data originating from third countries, but not exchanged between Member States would not be covered by the Framework Decision. It goes without saying that the processing of those data entails specific risks to the data subject should there, for instance, be no legal obligation to examine the accuracy of those data. A good example would be the use of 'no-fly' lists of third countries for law enforcement purposes in a Member State.

14. The EDPS underlines once more that a high level of data protection is needed in the area of police and judicial cooperation, an area in which the processing of personal data poses, by its very nature, specific risks for the citizen as has *inter alia* been recognised by Article 30(1)(b) of the EU-Treaty. Moreover, 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.
15. The proposal serves both objectives. It should provide guarantees for the citizen against improper use of his or her personal data. To the affected citizen it is of no importance whether data concerning him or her are processed in the context of an exchange between the Member States or in a purely domestic context. Moreover, it should contribute to the mutual trust between the Member States, as a condition for a successful exchange of information. If common standards are applied to the processing of data this will result in an easier acceptance of data exchanged between the Member States.
16. The EDPS warns that a limitation of the scope of the Framework Decision to data in the context of an exchange would not fully ensure the building of trust between the authorities of the Member States. Moreover, a limited text does not protect the citizen in an appropriate way. Under those circumstances, the Framework Decision would no longer give an adequate guarantee for the citizen against possible misuse of his or her data by public authorities. In the opinion of the EDPS, this 'shield-function' of the legislation is essential, if only to ensure that the European Union respects fundamental rights, in accordance with Article 6 of the EU-Treaty.
17. Finally, there is a strategic argument in favour of a Framework Decision applicable to all processing. As the recent negotiations with the United States for a new agreement on the processing and transfer of airline passenger data <sup>(1)</sup> show, solid EU-legislation protecting the citizen in all EU-internal situations would also strengthen the position of the EU in negotiations with third countries. In the absence of such a solid law, it would be rather difficult to insist upon an adequate level of protection in third countries, as a precondition for the transfer of personal data.

#### Other concerns

18. *Emphasis on data quality.* Article 4 of the Commission proposal does not only include the main data quality principles of Directive 95/46/EC but also provides for some specific rules. It contains 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. It furthermore contains obligations for the Member States to distinguish data according to their degree of accuracy and reliability. This is an important provision since law enforcement authorities also use soft data based on presumptions, not necessarily on facts. The EDPS regards these provisions as essential safeguards, which should not be deleted from the proposal, nor be made optional.
19. *Data processing and purpose limitation.* In the opinion of December 2005, the EDPS analysed the need for better legal provisions on the further use of data that have been collected by an authority for a specific purpose. Presently, the concerns of the EDPS regarding Article 5 relate mainly to his view that, whilst on the one hand (further) processing of data for wider purposes needs to be allowed, on the other hand the law must provide for precise conditions for this processing, in order to protect the data subject. The EDPS warns against solutions that leave the matter fully to the discretion of national law or that do not limit the conditions for further processing in conformity with Directive 95/46/EC and Council of Europe Convention No 108 <sup>(2)</sup>. As to the processing of special categories of data: this is dealt with under Directive 95/46/EC and Convention No 108, in a general prohibition with exceptions <sup>(3)</sup>. The EDPS is concerned that in the Framework Decision the general prohibition will be deleted and that — by doing so — the exception becomes the rule. Such a solution would not only be inconsistent with Directive 95/46/EC, but would also not be in line with Convention 108.

<sup>(1)</sup> Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (OJ L 298, 27.10.2006, p. 29).

<sup>(2)</sup> See: Article 13, in connection with Article 6(1)(b) of Directive 95/46/EC, and Article 9, in connection with Article 5 sub (b) of Convention 108.

<sup>(3)</sup> See: Article 8 of Directive 95/46/EC and Article 6 of Convention 108.

20. *Exchange of data with other authorities and private parties.* The Commission proposal contains limitations and specific safeguards for the exchange of information with other authorities besides police and judicial authorities, private parties and authorities of third countries. The EDPS underlines the importance of such specific provisions for the following reasons. In the first place, exchange of information with those 'third parties' entails specific risks (security breaches, further processing for different purposes, etc.). In the second place, involvement of third parties in law enforcement and in the processing of law enforcement information is becoming more commonplace. Directive 2006/24/EC on data retention <sup>(1)</sup>, the agreement on PNR-data with the United States and the so called Swift-case <sup>(2)</sup> are good examples. In the third place, the PNR-judgement of the European Court of Justice of 30 May 2006 <sup>(3)</sup> raises serious doubts on the protection of personal data collected by private parties for commercial purposes and later on processed for law enforcement purposes.
21. As to the transfer to and from other — public or private — parties within the EU, it is important that the proposal deals with the matter in a precise way and offers solutions consistent with Directive 95/46/EC. Those solutions must ensure that the consequences of the pillar structure — in particular the uncertainty about the delimitation of both pillars as far as the exchange of personal data between law enforcement authorities and other parties is concerned — will not harm the effectiveness of the protection.
22. As to the transfer of data to and from third countries, the Commission proposal provides for an adequacy decision by the Commission. If this would not be acceptable in Council, the result would be that each Member State will decide about adequacy on its own or, even worse, transfer the data without examining the level of protection in the third country. The absence of a harmonised system for the exchange of personal data with third countries could also:
- harm the trust between the authorities of the Member States, since an authority might be less willing to share information with an authority in another Member State if this Member State could also share this information with authorities of third countries in the absence of clear safeguards.
  - provoke U-turns. If the authority of a Member State could not receive information directly from another Member State because of the protection given by the Framework Decision, it could ask for assistance from an authority of a third country.
  - enable forum shopping by authorities of third countries: those authorities could ask for information in the Member State with the lowest legal requirements for transfers.

The EDPS considers it essential that mechanisms ensuring common standards and coordinated decisions on adequacy be put in place, also in order to comply with Council of Europe Convention No 108 (in particular its Article 12) <sup>(4)</sup>. The text of the Framework Decision should provide for such mechanisms.

23. The EDPS understands that several Member States question the legal basis for the inclusion of a provision on the exchange of personal data with third countries, in cases whereby those data are not received from or made available by the competent authority of another Member State. According to the EDPS, there are no grounds for questioning this legal basis. The examples elaborated in the Opinion of December 2005 as well as the arguments mentioned in the previous paragraph demonstrate the direct link of this exchange with third countries with the police and judicial cooperation under Article 29 of the EU-Treaty. A provision on the exchange of personal data with third countries must be seen as an additional and necessary provision in order to achieve the objectives of Article 29 EU in conjunction with Article 6 EU, in particular a closer cooperation of police forces with respect for fundamental rights.

<sup>(1)</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).

<sup>(2)</sup> See Opinion 10/2006 of 22 November 2006 of the Article 29 Data Protection Working Party on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

<sup>(3)</sup> Judgement in cases C-317/04 and C-318/04.

<sup>(4)</sup> See also more precisely: Article 2 of Additional Protocol (ratified by several Member States), which is in line with Articles 25-26 of Directive 95/46/EC.

24. *Data subjects' rights.* The data subject has a right to be informed about the processing of personal data concerning him or her. This right is linked to the principle of fair and lawful processing of personal data which in itself is respected by the Framework Decision and is moreover protected under Council of Europe Convention No 108, in particular its Articles 5(a) and 8. An essential element of this right is that this information should be given by the data controller *ex officio*. 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. Of course this right to be informed is subject to exceptions and it is clear that these exceptions can play an important role in the area of law enforcement since information on criminal investigations could prejudice the investigation itself. However, any solution making the right to information dependent on a request by the data subject would not be acceptable and not be compatible with Council of Europe Convention No 108.
25. The EDPS underlines that *the position of the data protection authorities* should be consistent with the position afforded to them under Directive 95/46/EC. This position is all the more important in this area of police and judicial cooperation. The cooperation between law enforcement authorities in order to effectively combat terrorism and other serious crime requires processing of quite often sensitive personal data and requires exceptions to the rights of the data subjects (see, for instance the previous point, on the right to be informed).
26. The EDPS points in the first place to the need for an effective supervision and inspection by the authorities of the processing of personal data within the scope of this framework decision, especially when personal data are exchanged amongst the Member States in the area of police cooperation. In the second place, the advisory role of the authorities should be ensured, within the national jurisdiction as well as within the institutionalised network of data protection authorities, the Working Party of authorities (under the directive known as the 'Article 29-Working Party'). The input by data protection authorities is needed, in order to enhance the consistency of the protection under this instrument with the protection under Directive 95/46/EC, to ensure compliance with the legal obligations and to fully achieve harmonisation between the Member States, also on a practical level.
27. Article 24 of the Commission proposal contains detailed rules on *security*, comparable to the rules included in the Europol-convention. The EDPS warns against the deletion of these rules from the proposal. A harmonised level of security is an important tool to enhance trust, for the data subject as well as between the authorities of the Member States.
28. In his opinion of December 2005, the EDPS recommended that specific safeguards should be put in place with respect to the *processing of certain specific categories of data*, such as biometric data and DNA-profiles. In the area of law enforcement, the use of these categories of data is becoming more and more important, whereas this use can entail specific risks for the data subject. Common rules are needed. The EDPS regrets that this recommendation has not been taken into consideration by Council, at least not visibly. The EDPS urges the Commission and the Council to adopt a proposal on this matter, whether related to the principle of availability or not.

#### Conclusion

29. The EDPS recommends that the Council allows more time for the negotiations, so as to achieve a result that offers sufficient protection. Although the EDPS recognises the importance of adopting the Framework Decision by Council in the short term, he warns that the rapidity of the decision making should not lead to a lowering of the standards of protection.
30. Consistency of the protection is essential, independent of where, by whom or for which purpose personal data are processed. The EDPS urges the Council to respect a level of protection that is not lower than the level of protection afforded under Directive 95/46/EC or even under the more generally formulated Council of Europe Convention No 108 which is binding upon the Member States.
31. Common rules on data protection should apply to all data in the area of police and judicial cooperation, and not be limited to cross-border exchanges between Member States. This opinion contains arguments showing that a more limited scope is unworkable which would, if introduced, lead to additional complexity and costs for authorities and harm the legal certainty of individuals.

## 32. Other concerns of the EDPS are:

- The specific provisions on data quality in the Commission proposal should not be deleted from the proposal, nor be made optional.
- The provisions on the further use of data and on special categories of data should be consistent with Directive 95/46/EC and in line with Council of Europe Convention No 108.
- The specific provisions on exchange of data with other parties besides law enforcement authorities within the EU should not be deleted from the proposal, nor be limited in scope. As to the exchange of data with third countries, *at the very least* mechanisms ensuring common standards and coordinated decisions on adequacy should be put in place, also in order to comply with Council of Europe Convention No 108. The text of the Framework Decision should provide for such mechanisms.
- Solutions making the right to information dependent upon a request by the data subject are not acceptable and not compatible with Council of Europe Convention No 108.
- The position of the data protection authorities should be consistent with the position afforded to them under Directive 95/46/EC.
- The detailed rules on security, comparable to the rules included in the Europol-convention, should not be deleted from the proposal.
- The Commission and the Council should adopt a proposal on processing of specific categories of data, such as biometric data and DNA-profiles, whether related to the principle of availability or not.

Done at Brussels on 29 November 2006

Peter HUSTINX

*European Data Protection Supervisor*

---