EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final)

(2006/C 116/04)

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,

Having regard to the request for an opinion in accordance with Article 28(2) of 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,

HAS ADOPTED THE FOLLOWING OPINION:

I. PRELIMINARY REMARKS

1. The Proposal for a Council Framework Decision on the exchange of information under the principle of availability has been sent by the Commission to the EDPS by letter of 12 October 2005. The EDPS understands this letter as a request to advise Community institutions and bodies, as foreseen in Article 28(2) of Regulation (EC) No 45/2001. According to the EDPS, the present opinion should be mentioned in the preamble of the Framework Decision.

2. The nature of this opinion has to be seen in the context described under II. As indicated under II, it is far from obvious that the present proposal — or the approach to availability taken by the proposal — will eventually lead to the adoption of a legal instrument. Other approaches are advocated by a considerable number of Member States.

3. However, it is obvious that the subject of the availability of law enforcement information across the internal borders — or, more widely, the exchange of this information — is high on the agenda of the Member States, inside as well as outside the Council, and within the European Parliament.

4. It is equally obvious that this subject is highly relevant from the perspective of the protection of personal data, as the present opinion itself will illustrate. The EDPS recalls that the present proposal was presented by the Commission with a close link to the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, object of an opinion of the EDPS, presented on 19 December 2005.

5. The EDPS will use this occasion to present in this opinion some general and more fundamental points of view on the subject of exchange of law enforcement information and on the approaches for regulating this subject. By presenting this opinion, the EDPS envisages ensuring that the perspective of data protection will be duly taken into account in future discussions on the subject.

6. The EDPS will be available for further consultation at a later stage, following relevant developments in the legislative process on this proposal as well as on other related proposals.

II. THE PROPOSAL IN ITS CONTEXT

7. The principle of availability has been introduced as an important new principle of law in the Hague Programme. It entails that information needed for the fight against crime should cross the internal borders of the EU without obstacles. The objective of the present proposal is to implement this principle in a binding legal instrument.

8. The exchange of police information between different countries is a popular subject for legislators, within and outside the framework of the EU. Recently, the following initiatives drew the attention of the EDPS.

9. In the first place, on 4 June 2004 Sweden proposed a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. On this proposal, the Council has reached an agreement on a general approach in its meeting of 1 December 2005.

10. In the second place, on 27 May 2005, seven Member States signed a Convention in Prüm (Germany) on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. It introduces *inter alia* measures to improve information exchange for DNA and fingerprints. The Convention is open for any Member State of the European Union to join. The Contracting Parties aim to incorporate the provisions of the Convention into the legal framework of the European Union.

11. In the third place, the availability of law enforcement information across the internal borders of the European Union will also be further facilitated by other legal instruments, such as the proposals regarding a Second Generation Schengen Information System (SIS II), the proposal for access for consultation to the Visa Information System (VIS) and the proposal for a Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States. In this respect, it is also useful to mention the Communication on improved effectiveness, enhanced operability and synergies among European databases in the area of Justice and Home Affairs, issued by the Commission on 25 November 2005.

12. Because all of these initiatives have been issued, it follows that the present proposal for a Framework Decision on availability should not be examined by itself, but other approaches to the exchange of law enforcement information should also be taken into account. This is even more important since it is the current tendency within the Council to give preference to other approaches to information exchange and to the concept of availability than the general approach proposed by the Commission in the present proposal. The present text of the proposal might even not be the object of discussion in the Council.

13. Furthermore, this proposal is closely linked to the Proposal for a Framework Decision on the protection of personal data. The present opinion must be understood in connection with the more profound opinion on the latter Framework Decision.

14. In his opinion on the Proposal for a Framework Decision on the protection of personal data, the EDPS underlined the importance of adequate data protection as a necessary consequence of a legal instrument on availability. According to the EDPS, such a legal instrument should not be adopted without essential guarantees on data protection.

15. The EDPS takes the same position in respect of the adoption of other legal instruments that facilitate the flow of law enforcement information across the internal borders of the EU. The EDPS therefore welcomes that the Council as well as the European Parliament have dedicated priority to the aforementioned proposal for a Framework Decision on the protection of personal data.

III. THE AVAILABILITY PRINCIPLE AS SUCH

16. The availability principle is in itself a simple principle. The information that is available to certain authorities in a Member State must also be provided to equivalent authorities in other Member States. The information must be exchanged as swiftly and easily as possible between the authorities of the Member States and preferably by allowing direct online access.

17. The difficulties arise because of the environment in which the principle of availability has to be made effective:

— A heterogeneous organisation of the police and the judiciary in the Member States, with different checks and balances.

— Different types of (sensitive) information are included (such as DNA or fingerprints).

— Different ways of access to relevant information for competent authorities even within Member States.

— It is difficult to ensure that information originating from another Member State will be properly interpreted due to differences in languages, in technological systems (interoperability) and in legal systems.

— It has to be included in the existing and extensive patchwork of legal provisions that deal with the exchange of law enforcement information between countries.

18. Irrespective of this complex environment, it is common understanding that the principle can not work by itself. Additional measures are needed to ensure that information can effectively be found and accessed. In any case, those measures must make it easier for law enforcement authorities to find out whether law enforcement authorities in other Member States have relevant information at their disposal and where this relevant information can be found. Such additional measures could consist of interfaces that deliver direct access to all or specific data held by other Member States. The proposal for a Framework Decision on availability introduces for this reason 'index data', specific data that can be accessed directly across the borders.

19. In general terms, the availability principle should facilitate the flow of information between the Member States. The internal borders will be abolished and the Member States have to allow that information available to their police authorities will increasingly become accessible for other authorities. The Member States lose competence to control the flow of information, which also results in the fact that they no longer can rely on their national legislation as a sufficient instrument for an adequate protection of the information.

20. It is for this reason that the proposal needs specific attention from the perspective of the protection of personal data. In the first place, information that is normally confidential and well secured must be provided to authorities in other Member States. In the second place, to make the system work index data must be established and made available to authorities in other Member States. The implementation of this principle will, as a consequence, generate more data than currently available.

IV. **MAIN ELEMENTS**

Scope of the principle of availability

21. First of all, it is essential to define to which kind of information the principle of availability will apply. The field of application of this principle is defined in general terms in Article 2 of the proposal, in combination with Article 1(1) and Article 3(a). The principle shall apply to information that is:

— existing information;

— listed in Annex II which defines six types of information;

— available to competent authorities.

These are the three essential elements of the scope of the principle in the proposal by the Commission. The scope is further refined in Article 2. Article 2(1) limits the application of the principle of availability to the stage prior to the commencement of a prosecution, whereas Article 2(2), (3) and (4) provide some more specific restrictions.

22. To understand the consequences of the proposal, a more profound analysis of the three essential elements mentioned above is needed. The first two elements of the scope are by themselves reasonably clear. The definition of 'existing information' is elaborated in Article 2(2) stating that the Framework Decision does not entail any obligation to collect and store information for the sole purpose of making it available, whereas the list in Annex II can not be interpreted in different ways. It is the third essential element, by itself and in combination with the first two elements that needs further clarification.

23. The proposal does not specify whether 'available information' consists merely of information already controlled by competent authorities or also includes information that can be potentially obtained by these authorities. However, according to the EDPS, the proposal could be interpreted as comprising both.

24. Indeed, while Article 2(2) seems to suggest a narrower scope, by specifying that the Framework Decision 'does not entail any obligation to collect and store information […] for the sole purpose of making it available', Article 3(a) allows a broader interpretation, by stating that 'information' shall mean 'existing information, listed in Annex II'.

25. Annex II mentions at least two categories of data that are commonly controlled by others than the police. The first category is vehicle registration information. In many Member States, the databases containing this information are not controlled by law enforcement authorities, even though they are regularly accessed by these authorities. Should this kind of information fall within the scope of the 'available information' which, according to Article 1, shall be provided to equivalent competent authorities of other Member States? The second category of data listed in Annex II to be mentioned are telephone numbers and other communications data: should these data be considered to be 'available' even when these data are not controlled by competent authorities, but by private companies?

26. Moreover, other provisions of the proposal, and more particular Articles 3(d) and 4(1)(c) of the proposal, support the view that 'designated authorities' and even 'designated parties' may control information that is 'available' for 'competent authorities'. It also follows from the text of the proposal that a 'competent authority' of a Member State is an authority covered by Article 29, first hyphen, of the EU-Treaty whereas any national authority can qualify as a 'designated authority'.

27. According to the EDPS, application of the availability principle to information that is controlled by designated authorities and designated parties, entails the following questions:

— Does Article 30(1)(b) provide for a sufficient legal basis, since information has to be made available by designated authorities and designated parties and from databases that do not fall within the framework of the third pillar?

— Will the Framework Decision on the protection of personal data apply, as is assumed e.g. in Article 8 of the proposal?

— If not, is the processing in accordance with the obligations under Directive 95/46/EC?

28. The implementation of such a broad principle as the 'principle of availability' requires a clear and precise definition of the data that shall be considered available. Therefore, the EDPS recommends:

— Clarifying the scope.

— As a first option, limiting the scope of the principle of availability to information controlled by competent authorities.

— As a second option, in case of a broader scope, ensuring sufficient safeguards for the protection of personal data. The questions raised in point 27 hereinabove have to be taken into consideration.

Other issues related to the scope

29. According to Article 2(1) of the proposal, the Framework Decision shall apply to the processing of information prior to the commencement of a prosecution. Its scope is more limited than the proposal for a Framework Decision on the protection of personal data that fully applies to judicial cooperation in criminal matters.

30. However, according to the EDPS this limitation does not by itself limit the scope of the proposal to police cooperation. It could also include judicial cooperation in criminal matters since in a number of Member States judicial authorities also have competences on criminal investigations, before the commencement of a prosecution. However, the fact that the proposal is solely based on Article 30(1)(b) TEU seems to indicate that it only applies to police cooperation. A clarification on this aspect would be welcomed.

31. The present proposal applies to providing information to Europol whereas the proposal for a Framework Decision on the protection of personal data excludes the processing of personal data by Europol. The EDPS advises limiting the information exchange with Europol to the purposes of Europol itself, as mentioned in Article 2 of the Europol Convention and the Annex thereof. Moreover, account should be taken of the detailed rules for exchange of data with Europol, which are already laid down in several Council Acts.

No new databases containing personal data

32. The starting point of the proposal is that it will not lead to the construction of new databases containing personal data. To that effect, Article 2(2) is clear: it does not entail any obligation to collect and store information for the sole purpose of making it available. From the perspective of data protection, this is an important and positive element of the proposal. The EDPS recalls his opinion on the proposal for a directive on the retention of data processed in connection with the provision of public electronic communication ([1]) in which he emphasised that legal obligations that lead to substantial databases run particular risks for the data subject, *inter alia* because of risks of illegitimate use.

33. However:

— It is important to ensure that the proposal will not promote an unconditional interconnection of databases and thus a network of databases which will be hard to supervise.

— There is an exception to the starting point mentioned above: Article 10 of the proposal which ensures that index data are available on line. Index data may contain personal data or in any case reveal their existence.

Direct and indirect access to information

34. The proposal provides for direct and indirect access to information. Article 9 of the proposal foresees direct on line access to information contained in databases to which corresponding national authorities have direct on line access. Article 10 entails an indirect access. Index data of information that is not accessible online shall be available for online consultation by equivalent competent authorities of other Member States and Europol. When consultation of index data results in a match, this authority may issue an information demand and send it to the designated authority in order to obtain the information identified by the index data.

35. Direct access does not lead to new databases, but it requires the interoperability of the databases of the equivalent competent systems within the Member States. Moreover, it will necessarily introduce a new usage of already existing databases by providing a facility to all competent authorities of the Member States which until now had only been open to national competent authorities. Direct access will automatically mean that an increased number of persons will have access to a database and therefore encompasses a growing risk of misuse.

([1]) Opinion of 26 September 2005 on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM (2005) 438 final).

36. In case of direct access by a competent authority of another Member State, the designated authorities of the originating Member State have no control over the access and the further use of the data. This consequence of direct access as foreseen by the proposal has to be properly addressed, since:

— It seems to invalidate the powers of the designated authorities to refuse the provision of information (under Article 14).

— It raises questions as to responsibilities for the accuracy and the keeping up to date of data, once they have been accessed. How can a designated authority of the originating Member State ensure that data are kept up to date?

— It is not only the designated authority that is no longer capable of fulfilling all its obligations under data protection law, but also the national data protection authority of the originating Member State can no longer supervise the application of the obligations since it lacks any competence *vis-a-vis* law enforcement authorities of other Member States.

— These problems are even more predominant in case of access to databases of designated authorities and designated parties, not being law enforcement authorities (see points 25-28 of this opinion).

This consequence of direct access is an important reason why the adoption of the present proposal should depend on the adoption of a Framework Decision on the protection of personal data. One problem remains: it is difficult to see how designated authorities could refuse the provision of information under Article 14.

37. As concerns indirect access through index data that give information on a hit/no hit system: this is not a new phenomenon. It is the basis of the functioning of European large scale information systems, such as the Schengen Information System. The establishment of a system of index data has the advantage that it allows the originating Member States to control the exchange of information from their police files. If consultation of index data results in a match, the requesting authority may issue an information demand concerning the data subject involved. This demand can be properly assessed by the requested authority.

38. Nevertheless, a proper analysis is needed since the establishment of a system of index data — in areas where those systems until now did not exist, other than the European large scale information systems — can create new risks for the data subject. The EDPS emphasises that although index data do not contain much information about the data subject, consultation of index data can lead to a highly sensitive result. It may reveal that a person is included in a police file in relation to criminal offences.

39. Therefore, it is of the utmost importance that the European legislator provides for adequate rules, at least on the creation of index data, on the management of the filing systems of index data and on the adequate organisation of the access to the index data. According to the EDPS, the proposal is not satisfactory on these points. At this stage, the EDPS makes three observations:

— The definition of index data is unclear. It is not clear whether index data are seen as meta-data, primary keys or even both? The notion of index data needs to be clarified, as it has a direct impact on the level of data protection and the required safeguards.

— The proposal should clarify the role of national contact points as regards index data. Involvement of national contact points could be necessary, in particular in cases when the interpretation of the index data requires specialised knowledge for instance in case of the possible matching of fingerprints.

— The proposal leaves the adoption of rules necessary for the creation of index data to implementing legislation in accordance with the comitology-procedure foreseen in Article 19. Although implementing rules might be needed, the basic rules for the creation of index data should be included in the Framework Decision itself.

Prior authorisation by judicial authorities

40. The information exchange shall not prevent Member States requiring prior authorisation by judicial authorities to transmit the information to the requesting authority when this information is under judicial control in the requested country. This is important since, according to a survey on police powers to exchange personal data [1], not in all Member States police can autonomously access these data. According to the EDPS, the availability principle should not undermine the obligation under national law to obtain a prior authorisation for the information, or at least establish specific rules concerning the categories of data for which prior authorisation has to be obtained, that will be applicable in all Member States.

[1] Replies to questionnaire on Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, in particular as regards serious offences including terrorist acts (Council Doc No 5815/1/05).

41. This obligation should be interpreted in connection with Article 11(2) of the Proposal for a Framework Decision on the protection of personal data that also envisages that the transmitting Member State has a say in the further use of the data in the Member State to which the data have been transmitted. The EDPS notes the importance of this principle, which is needed to ensure that availability will not lead to circumventing restrictive national legislation on the further use of personal data.

Final remark

42. These elements require high standards of data protection. Special attention should be given to ensure the principles of purpose limitation and further processing as well as to the accuracy and the reliability of the information that is accessed (see the opinion of the EDPS on the Framework Decision on the protection of personal data, IV.2 and IV.6).

V. OTHER APPROACHES

Swedish proposal

43. The Swedish proposal is not limited to specific types of information but covers all information *and intelligence*, even information and intelligence that is kept by others than competent law enforcement authorities. The proposal advances cooperation by setting time limits to answer requests for information and by abolishing discrimination between the exchange within one Member State and cross border exchange of information. It does not provide for additional measures ensuring that the information can effectively be accessed. It is for this reason understandable that the Commission was not satisfied by the Swedish proposal in itself, as an adequate instrument for availability ([1]).

44. The approach in the Swedish proposal has the following general implications, from the perspective of data protection:

— It is welcomed that the proposal is strictly limited to the processing of existing data and does not lead to any new databases, not even to 'index data'.

— However, the absence of 'index data' is not by definition a positive element. Index data, if adequately secured, can facilitate a targeted and therefore less intrusive research of data with a sensitive nature. It can also allow for better filtering of requests and for better supervision.

— In any case, the proposal leads to an increase of the cross border exchange of personal data, with risks for the protection of personal data, *inter alia* because the competence of the Member States to fully control the exchanger of data is affected. It should not be adopted independently of the adoption of the Framework Decision on the protection of personal data.

([1]) See Commission Staff Working Document Annex to the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, SEC 2005 (1207) of 12.10.2005.

Prüm Convention

45. The Prüm Convention takes another approach to implementing the principle of availability. Whereas the present proposal for a Framework Decision has a general approach — not providing for specific rules for the exchange of specific types of information but applicable to all types of information, in so far as they are listed in Annex II (see points 21-28 of this opinion) -, the approach of the Prüm Convention is gradual.

46. This approach it is sometimes called a 'data field-by-data field approach'. It applies to specific types of information (DNA, fingerprinting data and vehicle registration data) and it lays down the obligation to take into account the specific nature of the data. The Convention lays down the obligation to open and keep DNA analysis files for the investigation of criminal offences. A similar obligation applies to fingerprinting data. As to vehicle registration data, direct access has to be given to national contact points of other Member States.

47. The approach of the Prüm Convention gives rise to three types of observations.

48. In the first place, it goes without saying that the EDPS does not endorse the process leading up to this Convention, outside the institutional framework of the European Union, and therefore without substantive involvement of the Commission. Moreover, this means no democratic control by the European Parliament and no judicial control by the Court of Justice and as a result there are less guarantees that all the (public) interests are equally balanced. This includes the perspective of data protection. In other words, the institutions of the European Union do not have the opportunity to assess — before the system is established — the impact of the policy choices on the protection of personal data.

49. In the second place, it is obvious that some elements of the Prüm Convention are clearly more intrusive to the data subject than the proposal for a Framework Decision on availability. The Convention necessarily leads to the establishment of new databases which in itself presents risks to the protection of personal data. The necessity and proportionality of the establishment of these new databases should be demonstrated. Adequate safeguards for the protection of personal data should be provided.

A 'data field-by-data field approach'

50. In the third place, as said before, the Convention takes a 'data field-by-data field approach'. Hereinabove, the EDPS mentioned the difficulties and uncertainties related to the environment in which the principle of availability has to be made effective. Under those circumstances, it is according to the EDPS preferable not to set up a system for a range of data, but to start with a more cautious approach which involves one type of data and to monitor to what extent the principle of availability can effectively support law enforcement, as well as the specific risks for the protection of personal data. Based on these experiences, the system could possibly be extended to other types of data and/or modified in order to be more effective.

51. This 'data field-by-data field approach' would also better fulfil the requirements of the principle of proportionality. According to the EDPS, the needs for a better cross border exchange of data for the purpose of law enforcement could justify the adoption of a legal instrument on EU level, but to be proportional the instrument should be appropriate to achieve its goal which can be more properly established after a period of practical experiences. Furthermore, the instrument should not disproportionately harm the data subject. The exchange should not relate to more types of data than strictly necessary, with a possibility of an anonymous exchange of data, and should take place under strict conditions of data protection.

52. Moreover, a more cautious approach as advocated by the EDPS could — possibly in addition to the 'data field-by-data field approach' — include starting the implementation of the availability principle only by way of indirect access, via index data. The EDPS mentions this as a point for consideration in the further legislative process.

VI. **WHICH DATA?**

53. Annex II enumerates the types of information that may be obtained under the proposed Framework Decision. All of the six types of information listed there are personal data under most circumstances because they all involve a relation to an identified or identifiable person.

54. Under Article 3(g) of the Proposal, index data shall mean 'data the purpose of which is to distinctively identify information and that can be queried by means of a search routine to ascertain whether or not information is available'. In the 'Approach for the implementation of the principle of availability' [1] the following data are qualified as index data:

— the identification of the persons concerned;

— an identifying number for the objects concerned (vehicles/documents);

— fingerprints/digital photos.

Another type of data that could qualify as index data would be DNA-profiles. This list of index data reveals that index data may contain personal data and thus, an adequate protection is required.

55. The EDPS specifically addresses the issue of DNA-profiles. DNA analysis has proved to be of significant value for the investigation of crime and efficient exchange of DNA data can be essential to the fight against crime. However, it is essential that the concept of DNA data is clearly defined and that the specific characteristics of these data are properly taken into account. Indeed, from a data protection point of view, there is a big difference between DNA samples and DNA profiles.

56. DNA samples (often collected and stored by law enforcement authorities) should be considered as particularly sensitive, since they are more likely to contain the whole DNA 'picture'. They can provide information on genetic characteristics and the health status of a person, as may be required for totally different purposes such as giving medical advices to individuals or young couples.

57. On the contrary, DNA profiles only contain some partial DNA information extracted from the DNA sample: they can be used to verify the identity of a person, but in principle they do not reveal genetic characteristics of a person. Nonetheless, progress in science may increase the information that can be revealed by DNA profiles: what is considered as an 'innocent' DNA profile at a certain moment in time, may at a later stage reveal much more information than expected and needed, and in particular information concerning genetic characteristics of a person. The information that can be revealed by DNA profiles should thus be considered as dynamic.

58. In this perspective, the EDPS notes that both the Prüm Convention and the Commission proposal promote the exchange of DNA data between law enforcement, but there are substantial differences in the way they do so.

[1] Document from the Presidency to the Council of 5 April 2005 (Doc. No.: 7641/05).

59. The EDPS welcomes that the Commission proposal does not establish any obligation to collect DNA data and that it clearly limits the exchange of DNA data to DNA profiles. Annex II defines DNA profiles through an initial common list of DNA markers used in forensic DNA analysis in Member States. This list — based on the seven DNA markers of the European Standard Set as defined Annex I of the Council Resolution of 25 June 2001 on the exchange of DNA analysis results [1] — guarantees that DNA profiles will not contain, when they are extracted, any information about specific hereditary characteristics.

60. The EDPS highlights that this Council Resolution lays down some very important safeguards which are specifically related to the dynamic nature of DNA profiles. Indeed, section III of the Resolution, after limiting the exchanges of DNA analysis results to 'chromosome zones […] not known to provide information about specific hereditary characteristics', further recommends Member States to no longer use those DNA markers which, due to science developments, may provide information on specific hereditary characteristics.

61. The Prüm Convention provides for a different approach, since it obliges the Contracting Parties to open and keep DNA analysis files for the investigation of criminal offences. It therefore entails the creation of new DNA databases and an increased collection of DNA data. Furthermore, it is unclear which kind of data are included in the 'DNA analysis files' and the Convention does not take into account the dynamic evolution of DNA profiles.

62. The EDPS points out that any legal instrument laying down exchanges of DNA data should:

— Clearly limit and define the type of DNA information which may be exchanged (also with regard to the fundamental difference between DNA samples and DNA profiles).

— Set up common technical standards aimed at avoiding that variations in practices on forensic DNA databases in Member States could lead to difficulties and inaccurate results when data are exchanged.

— Provide for appropriate legally binding safeguards aimed at preventing that the developments of science would result in obtaining from DNA profiles personal data which are not only sensitive, but also unnecessary for the purpose for which they were collected.

63. In this perspective, the EDPS hereby confirms and integrates the remarks already made in his opinion on the Framework Decision on the protection of personal data (point 80). In that Opinion, the EDPS pointed out, with regard to DNA data, that specific safeguards should be provided, so as to guarantee that: the available information may only be used to identify individuals for the prevention, detection, or investigation of criminal offences; the level of accuracy of DNA profiles is carefully taken into account and might be challenged by the data subject through readily available means; the respect of the dignity of persons must be fully ensured [2].

64. These considerations lead furthermore to the conclusion that legislation on the establishment of DNA-files and the exchange of data from these files should only be adopted after an impact assessment in which the benefits and the risks could have been properly assessed. The EDPS recommends that this legislation contains obligations for a regular evaluation after its entry into force.

65. Finally, Annex II includes other types of information that may be exchanged. It includes information that originates from private parties since telephone numbers and other communication data, as well as traffic data do normally originate from telephone operators. The explanatory memorandum confirms that Member States are obliged to ensure that law enforcement relevant information controlled by authorities or by private parties designated for this purpose, is shared with equivalent competent authorities of other Member States and Europol. Whereas the proposal applies to personal data originating from private parties, the applicable legal framework should — according to the EDPS — contain additional safeguards to protect the data subject so as to ensure the accuracy of the data.

VII. **PRINCIPLES OF DATA PROTECTION**

66. The rules on the protection of personal data are not specifically laid down in the proposed Council Framework Decision, while in other instruments, like the Prüm Convention or the Swedish proposal, there are some specific provisions on the protection of personal data. The lack of specific rules on the protection of personal data in the availability proposal is acceptable only insofar as the general rules contained in the proposal for a Framework Decision on data protection in third pillar are fully applicable and provide for a sufficient protection. Moreover, rules on personal data protection laid down by specific instruments — such as the Swedish proposal and the Prüm Convention — should not lower the level of protection ensured by the general framework. The EDPS recommends adding a specific clause on possible conflicts between the different rules on data protection.

[1] OJ C 187, p. 1.

[2] In the same line, see also the Council of Europe's 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of personal biometric data', February 2005.

67. At this point, the EDPS would like to highlight again, by recalling his opinion with regard to the Framework Decision on the protection of personal data, the importance of having consistent and comprehensive data protection rules in place with regard to law enforcement cooperation that apply to all processing. Subsequently, the EDPS reiterates the other points made in that opinion. In this paragraph, the following data protection issues are emphasised:

— Lawful processing of personal data. The EDPS supports the approach that information can be available only if it has been collected lawfully (as mentioned by Article 2.2 with regard to information collected through coercive measures). Lawful processing of personal data would also ensure that information made available and exchanged can be properly used also in a judicial proceeding. Indeed, although information processed after the commencement of a prosecution falls outside the scope of the proposed instrument, it is still likely that information exchanged before by law enforcement authorities ends up in judicial proceedings.

— Quality of personal data is of specific importance since the availability principle favours that information will be used by law enforcement authorities operating outside the context in which the data were collected. Those authorities even have direct access to databases of other Member States. The quality of the personal data can only be ensured if its accuracy is regularly and properly checked, if information is distinguished according to the different categories of persons concerned (victims, suspects, witnesses, etc), and if, when necessary, the decree of accuracy is indicated (see EDPS Opinion on the protection of personal data, IV.6).

These points make once more clear why data protection rules, and especially rules on accuracy, should be applicable to all kinds of processing, also to domestic ones. Otherwise, personal data which are directly accessed could be incorrect, out of date and thus impinge both on the data subjects' rights and on the efficiency of investigations.

— Purpose limitation. According to the principle of availability, personal data may be accessed by equivalent competent authorities of other Member States. However, the competences of law enforcement authorities may substantially differ from country to country. It is therefore essential to ensure that the basic principle of purpose limitation is respected in spite of the different scope of competences of the various competent authorities exchanging the data. Information which is collected and processed by a certain authority with a specific purpose can not then be used for a different purpose just by virtue of the different, maybe broader, competences of the receiving authority.

Therefore, the EDPS welcomes Article 7 of the proposed Framework Decision, which should be read as a specification of the general rules laid down in the proposed Framework Decision on the protection of personal data. Furthermore, the EDPS notes that the assessment of the equivalence between different authorities (which in the current proposal is left to a comitology procedure) should be carried out carefully and with due respect to the purpose limitation principle.

— Time limits for storing exchanged information shall also be seen in the light of the purpose limitation principle: information accessed or exchanged for one purpose should be deleted as soon as it is no longer necessary for that purpose. This would avoid unnecessary duplication of databases, while still allowing competent authorities to access (updated) available information again, in case it is necessary for another legitimate purpose.

— Logging of information transmitted according to the principle of availability. Logging should take place on both sides: in the requested as well as in the requesting Member State. Access logs, not only exchange logs, should be kept (see EDPS Opinion on the protection of personal data, point 133), also with a view to ensuring that national competent authorities trust each other and do not completely loose control over the information available. The need for traceability of information also implies a possibility to update and/or correct information.

— Rights of data subjects. Systems for exchange of information between EU law enforcement authorities increase situations whereby personal data are (temporarily) processed at the same time by competent authorities in different Member States. This means on one hand that common EU-standards on data subjects' rights should be established, and on the other hand that data subjects should be able to exercise their rights, to the extent allowed by rules on data protection in third pillar, with regard to both authorities that make data available and authorities that access and process these data.

— Supervision. The EDPS points out that, depending on the case, more than one national supervisory authority may be competent to monitor the processing of personal data carried out on the basis of the current proposals. In this regard, direct online access to law enforcement information calls for an enhanced supervision and coordination by relevant national data protection authorities.

VIII. CONCLUSIONS

General conclusions relating to the principle of availability

68. The EDPS uses the occasion to present in this opinion some general and more fundamental points of view on the subject of exchange of law enforcement information and on the approaches for regulating this subject. The EDPS will be available for further consultation at a later stage, following relevant developments in the legislative process on this proposal or on other related proposals.

69. According to the EDPS, the principle of availability should be implemented into a binding legal instrument by way of a more cautious, gradual approach which involves one type of data and to monitor to what extent the principle of availability can effectively support law enforcement, as well as the specific risks for the protection of personal data. This more cautious approach could include starting with the implementation of the availability principle only by way of indirect access, via index data. Based on these experiences, the system could possibly be extended to other types of data and/or modified in order to be more effective.

70. Any legal instrument implementing the principle of availability should not be adopted without the prior adoption of essential guarantees on data protection as included in the Proposal for a Framework Decision on the protection of personal data.

Recommendations aiming to modify the present proposal

71. The EDPS recommends clarifying the scope of the principle of availability as follows:

— Adding a clear and precise definition of the data that will be considered available.

— As a first option, limiting the scope of the principle of availability to information controlled by competent authorities.

— As a second option, in case of a broader scope, ensuring sufficient safeguards for the protection of personal data. The questions raised in point 27 of this opinion have to be taken into consideration.

72. The EDPS makes the following observations on direct access to databases by a competent authority of another Member State:

— The issue has to be properly addressed since, in case of direct access, the designated authorities of the originating Member State have no control over the access and the further use of the data.

— The proposal may not promote an unconditional interconnection of databases and thus a network of databases which will be hard to supervise

73. The Framework Decision should be more precise on the establishment of a system of index data. More in particular:

— The proposal should provide for adequate rules, at least on the creation of index data, on the management of the filing systems of index data and on the adequate organisation of the access to the index data.

— The definition of index data needs to be clarified.

— The proposal should clarify the role of national contact points as regards index data.

— The basic rules for the creation of index data should be included in the Framework Decision itself and not left to implementing legislation in accordance with the comitology-procedure.

74. The EDPS points out that the proposal -in so far as it lays down exchanges of DNA data — should:

— Clearly limit and define the type of DNA information which may be exchanged (also with regard to the fundamental difference between DNA samples and DNA profiles).

— Set up common technical standards aimed at avoiding that variations in practices on forensic DNA databases in Member States could lead to difficulties and inaccurate results when data are exchanged

— Provide for appropriate legally binding safeguards aimed at preventing that the developments of science would result in obtaining from DNA profiles personal data which are not only sensitive, but also unnecessary for the purpose for which they were collected.

— Only be adopted after an impact assessment.

75. The EDPS advises limiting the information exchange with Europol to the purposes of Europol itself, as mentioned in Article 2 of the Europol Convention and the Annex thereof.

Done at Brussels on 28 February 2006.

Peter HUSTINX

European Data protection Supervisor