EUROPEAN DATA PROTECTION SUPERVISOR

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 (COM (2005) 475 final)

(2006/C 47/12)

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**

Consultation of the EDPS

1. 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 has been sent by the Commission to the EDPS by letter of 4 October 2005.The EDPS understands this letter as a request to advise Community institutions and bodies, as foreseen in Article 28 (2) of Regulation nr. 45/2001/EC. According to the EDPS, the present opinion should be mentioned in the preamble of the Framework Decision.

The importance of the present proposal

2. The EDPS underlines the importance of the present proposal, from the perspective of the fundamental rights and freedoms of natural persons to have their personal data protected. The adoption of this proposal would mean a considerable step forwards for the protection of personal data, in an important area which in particular requires a consistent and effective mechanism for the protection of personal data on the level of the European Union.

3. In this context, the EDPS emphasises that police and judicial cooperation between the member states, as an element of the progressive establishment of an area of freedom, security and justice, is of growing significance. The Hague Programme has introduced the principle of availability in order to improve the cross-border exchange of law-enforcement information. According to the Hague Programme ([1]), the mere fact that information crosses borders should no longer be relevant. The introduction of the principle of availability reflects a more general trend to facilitate the exchange of law enforcement information (see for instance the so called Prüm Convention ([2]) as has been signed by seven Member States and the Swedish proposal for a Framework Decision on simplifying the exchange of information and intelligence between law enforcement agencies ([3])). The very recent approval by the European Parliament of a Directive of the European Parliament and of the Council on the retention of communication data ([4]) can be viewed in the same perspective. These developments require the adoption of a legal instrument to guarantee an effective protection of personal data within all the Member States of the European Union, based on common standards.

([1]) P. 18 of the programme.

([2]) Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. Prüm (Germany) 27 May 2005.

([3]) Initiative of the Kingdom of Sweden with a view to adopting a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts (OJ, C 281).

([4]) On the basis of 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

4. The EDPS points to the fact that the present general framework for data protection in this area is insufficient. In the first place, directive 95/46/EC does not apply to the processing of personal data in the course of activities which fall outside the scope of Community law, such as those provided for by Title VI of the Treaty on the European Union (Article 3 (2) of the directive). Although in most Member States the scope of the implementing legislation is wider than the directive itself requires and does not exclude data processing for the purpose of law enforcement, significant differences in national law exist. In the second place, the Council of Europe Convention No 108 ([1]) by which all the Member States are bound does not provide for the necessary preciseness in the protection as has been recognised already at the time of the adoption of Directive 95/46/EC. In the third place, neither of these two legal instruments takes into account the specific characteristics of the exchange of data by police and judicial authorities ([2]).

A contribution to the success of the cooperation itself

5. An effective protection of personal data is not only important for the data subjects but also contributes to the success of the police and judicial cooperation itself. In many aspects, both public interests go hand in hand.

6. One has to bear in mind that the personal data concerned are quite often of a sensitive nature and have been obtained by police and judicial authorities as a result of an investigation on persons. The willingness to exchange these data with authorities of other member states will increase if an authority is assured of the level of protection in that other member state. The EDPS mentions as relevant elements of data protection the confidentiality and security of data and the limitations on access and further use.

7. Moreover, a high level of data protection can assure the accuracy and reliability of personal data. Upon exchange of data between police and/or judicial authorities the accuracy and reliability of these data become even more important, especially since, further to consecutive exchanges and retransmission of data between law enforcement authorities, data are eventually processed far from their source and out of the context in which they were originally collected and used. Normally, the receiving authorities do not have any knowledge about additional circumstances and have to rely fully on the data themselves.

8. The harmonisation of the national rules on personal data in the area of police and justice — including adequate safeguards for the protection of these data — can thus stimulate the mutual trust as well as the effectiveness of the exchange itself.

Respect of the principles of data protection, combined with an additional set of rules

9. The need for and the importance of the present proposal have been emphasised on several occasions. During the Spring Conference in Krakow in April 2005, the European Data Protection Authorities adopted a declaration and a position paper in which they called for the adoption of a new legal framework on data protection applicable in third pillar-activities. This new framework should not only respect the principles of data protection as laid down in Directive 95/46/EC — it is important to guarantee the consistency of the data protection within the European Union — but also provide for an additional set of rules taking into account the specific nature of the area of law enforcement ([3]). The EDPS welcomes the fact that the present proposal takes into account these starting points: it respects the principles of data protection as laid down in Directive 95/46/EC and it provides for an additional set of rules.

10. This opinion will analyse to what extent the result is acceptable from the perspective of data protection, with due respect to the specific context of data protection in the area of law enforcement. On the one hand the data concerned are quite often of a very sensitive nature (see point 6 of this opinion) and, on the other hand, there is a strong pressure to access these data, in view of an effective performance by law enforcement, which can include the protection of the life and the physical security of persons. According to the EDPS, data protection rules should respond to justified needs of law enforcement, but should also protect the data subject against unjustified processing and access. To be in accordance with the principle of proportionality, the result of the considerations of the European legislator needs to reflect the respect of the two potentially opposite public interests. In this context, the EDPS mentions once more that quite often both interests go hand in hand.

The context of Title VI of the Treaty on the European Union

11. Finally, it is to be mentioned that the present proposal forms part of Title VI of the Treaty on the European Union, the so called third pillar. The intervention of the European legislator is bound by clear limitations: limitations of the legislative powers of the Union to the subjects mentioned in Articles 30 and 31, limitations as to the legislative procedure which does not include the full participation of the European Parliament, and limitations as to the judicial control since the competences of the European Court of Justice under Article 35 TEU are incomplete. These limitations require an even more careful analysis of the text of the proposal.

([1]) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981

([2]) In 1987, the Council of Europe issued a Recommendation No R (87) 15 regulating the use of personal data in the police sector, but this recommendation is by nature not binding to the Member States.

([3]) See in the same sense 'The EDPS as an advisor to the Community Institutions on proposals for legislation and related documents', 18 March 2005, published on www.edps.eu.int.

II. THE CONTEXT: EXCHANGE OF INFORMATION UNDER THE AVAILABILITY PRINCIPLE, DATA RETENTION AND THE SPECIFIC FRAMEWORKS OF SIS II AND VIS

II.1 The principle of availability

12. The proposal is closely linked to the proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final). The latter proposal aims to implement the principle of availability and by doing so ensure that information available to competent authorities of a Member State for the fight against crime shall be provided to equivalent authorities of other Member States. It should lead to the abolishment of the internal borders for the exchange of this information by subjecting the exchange of information to uniform conditions across the Union.

13. The close link between the two proposals results from the fact that law enforcement information involves to a large extent personal data. Legislation on the exchange of law enforcement information can not be adopted without safeguarding an adequate protection of personal data. When an intervention on the level of the European Union results in the abolishment of the internal borders for the exchange of this information, the protection of personal data can no longer be solely dealt with by national law. It has become a task of the European institutions to guarantee the protection of personal data across the territory of the Union without internal borders. This task has been explicitly stated in Article 30 (1)(b) TEU and is a consequence of the obligation for the Union to respect fundamental rights (Article 6 TEU). Moreover:

— Article 1 (2) of the present proposal explicitly states that Member States may no longer restrict or prohibit the cross-border flow of information for reasons of protection of personal data.

— The proposal for a Council Framework Decision on the exchange of information under the principle of availability contains several references to the present proposal.

14. The EDPS points out that a Council Framework Decision on the exchange of information under the principle of availability should only be adopted under the condition that a Framework Decision on the protection of personal data is adopted as well. However, the present proposal for a Council Framework Decision on data protection has its own merits and is needed even in the absence of a legal instrument on availability. This has been emphasised in section I of this opinion.

15. This being the case, the EDPS will analyse the two proposals in two separate opinions. This also has a practical reason. There is no guarantee that the proposals will be dealt with jointly and with the same promptness by Council and European Parliament.

II.2 Data retention

16. On 26 September 2005, the EDPS presented his opinion on the proposal for a Directive on the retention of communication data [1]. In this opinion he pointed out some important shortcomings of the proposal and suggested adding to the directive specific provisions on access to the traffic and location data by the competent authorities and on the further use of the data, as well as adding further additional safeguards for data protection. The text of the Directive as adopted by the European Parliament and the Council contains a limited — but by no means sufficient — provision on data protection and data security and contains an even more insufficient provision on access, referring the issuing of measures on the access to the retained data to national law, subject to relevant provisions of European Union law or public international law.

17. The approval of the Directive on the retention of communication data makes it even more urgent to establish a legal framework for data protection in the third pillar. By adopting the directive, the Community legislator obliges the providers of telecommunications and internet services to retain data for law enforcement purposes, without the necessary and appropriate safeguards for the protection of the data subject. A gap in the protection remains, since the directive does not (sufficiently) address the access to the data, nor their further use once the data have been accessed by competent authorities in the field of law enforcement.

18. The present proposal fills an important part of this gap since it applies to the further use of the data once they have been accessed by law enforcement authorities. The EDPS regrets however that the present proposal does not deal with access to these data either. Contrary to what is foreseen for the SIS II and the VIS-systems (see II.3 of this opinion), this subject-matter is left to the discretion of the national legislator.

II.3 Processing in the framework of SIS II and VIS

19. The European Union is currently using or developing several large scale information systems (Eurodac, SIS II, VIS) and striving towards synergies between these systems. There is also a growing tendency to granting a wider access for law enforcement purposes to these systems. These far reaching developments must take into account, according to the Hague Programme, the 'need to strike the right balance between law enforcement purposes and safeguarding fundamental rights of the individuals'.

[1] Opinion of the European Data Protection Supervisor 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), published on www.edps.eu.int

20. In his opinion of 19 October 2005 on the proposals for a Second Generation Schengen Information System (SIS-II) ([1]), the EDPS has underlined some elements regarding simultaneous application of general rules (*lex generalis* and more specific rules (*lex specialis)* on data protection. The present proposal can be seen as a *lex generalis*, replacing Convention 108 in the framework of the third pillar ([2]).

21. The EDPS underlines in this context that the proposal also provides for a general framework for data protection for specific instruments like the third pillar part of the SIS II and the access by law enforcement to the Visa Information System. ([3])

III. THE HEART OF THE PROPOSAL

III.1 Common standards applicable to all processing

The starting point

22. According to its Article 1 (1), the proposal intends to determine common standards to ensure the protection of personal data in the course of activities of police and judicial co-operation in criminal matters. Article 1 (1) should be read in conjunction with Article 3 (1) that states that the proposal shall apply to the processing of personal data (...) by a competent authority for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

23. It follows from these provisions that the proposed Framework Decision has two main characteristics: it sets common standards and it applies to all processing for the purpose of enforcement of criminal law, even if the data concerned have not been transmitted or made available by competent authorities of other Member States.

24. The EDPS underlines the importance of these two main characteristics. It should be the ambition of the present proposal to establish a framework for data protection that fully complements the already existing legal framework in the first pillar. Only if this condition is met, does the European Union fully comply with its obligation under Article 6 (2) TEU to respect the fundamental rights as guaranteed by the ECHR.

Common standards

25. As to the first characteristic: the present proposal aims to ensure that the existing principles of data protection will be applied within the area of the third pillar. Moreover, it provides for common standards specifying these principles, in view of their application in this area. The EDPS emphasises the importance of these aspects of the proposal. They reflect the specific and sensitive nature of the processing of personal data in this area. The EDPS values in particular the introduction of the principle of the distinction between personal data of categories of persons, as a specific principle of data protection for the area of police and judicial cooperation in criminal matters, in addition to existing principles of data protection (Article 4 (4)). According to the EDPS the principle itself and its legal consequences for the data subject should even be *more* specified (see points 88-92 of this opinion).

26. The rules have to apply to different situations, so they can not be too detailed. On the other hand, they need to give the citizen the necessary legal certainty, as well as an adequate protection of his personal data. According to the EDPS the balance between these two potentially conflicting legislative requirements has generally been met by the proposal. The provisions leave flexibility where needed, but are in most areas precise enough to protect the citizen.

27. On some points, however, the proposal is too flexible and does not provide for the needed safeguards. For example, in Article 7 (1) the proposal provides in a general exemption to the safeguards, under the sole condition 'otherwise provided by law'. Leaving such a broad discretionary power to keep the data for longer than necessary for the envisaged purpose would not only be incompatible with the fundamental right to data protection, but would also harm the basic need for harmonisation of the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.

28. Exemptions, where needed, should be limited to — national or European — legal provisions, issued to protect specific public interests. Article 7 (1) should mention these public interests.

29. This leads to another point. Whenever any other specific legal instrument under Title VI of the EU Treaty provides for more precise conditions or restrictions for the processing of or access to data, this more specific legislation should apply as a *lex specialis*. Article 17 of this proposal provides for derogations to Articles 12, 13, 14 and 15 when specific legislation under Title VI lays down specific conditions for the transmission of data. This is an illustration of the general nature of the proposal (as explained

([1]) Par. 2.2.4 of the opinion.

([2]) Council of Europe's Convention for the protection of individuals with regard to automatic processing of personal data, 28 January 1981.

([3]) Proposal for a Council Decision concerning the access for consultation to the Visa Information System to authorities in Member States responsible for internal security and to Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences (COM (2005) 600 final), issued on 24 November 2005. The EDPS intends to issue an opinion on this proposal in the beginning of 2006.

here above), but does not cover all the hypotheses. According to the EDPS, Article 17 should:

— be drafted in a more general way: if there is a more specific legislation governing whatever aspect of data processing (not only transmission of data), the specific legislation applies.

— contain the safeguard that derogations may not lower the level of protection.

Applicable to all processing

30. As to the second characteristic: the ideal result would be that all collection and processing of personal data within the framework of the third pillar should be covered.

31. It is essential for the achievement of its objective that the Framework Decision covers all police and judicial data, even if they are not transmitted or made available by competent authorities of other Member States.

32. This is all the more important since any limitation to data that are transmitted or made available to competent authorities in 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 ([1]). Harm would be done to the legal certainty of individuals. Under normal circumstances, one never knows in advance — at the time of collection or processing of personal data — if those data will be relevant for an exchange with competent authorities in other Member States. The EDPS refers in this context to the principle of availability and the abolishment of the internal borders for the exchange of law enforcement data.

33. Finally, the EDPS notes that the proposal does not apply to:

— processing in the framework of the second pillar of the EU-Treaty (common foreign and security policy).

— processing of data by intelligence services and the access by these services to these data when processed by competent authorities or other parties (this follows from Article 33 TEU).

In these areas, national law is to provide adequate protection of data subjects. This gap in the protection on EU level has to be taken into account in the appraisal of the proposal: ([2]) since not all processing in the field of law enforcement can be covered, the legislator has to ensure an even more effective protection in the areas that are indeed covered by the proposal.

([1]) The EDPS refers to the same reasoning by the Court in (*inter alia*) its judgement in Österreichischer Rundfunk and Others, Joined cases C-465/00, C-138/01 and C-139/01, ECR [2003], p. I-4989.

([2]) See in the same sense, the Opinion of the EDPS 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, point 33.

III.2 **The legal basis**

34. The recitals of the proposal for a Council Framework Decision on the exchange of information under the principle of availability mention a specific legal basis, namely Article 30 (1)(b). To the contrary, the present proposal does not specify which provisions under Article 30 or Article 31 form the legal basis.

35. Although it is not the task of the EDPS as an advisor on legislation of the European Union to choose the legal basis of a proposal, it is useful to suppose that also the present proposal could be based on Article 30 (1)(b). In addition, it could be based on Article 31 (1)(c) TEU and should also apply, in its entirety, to domestic situations, provided that this is necessary to improve the police and judicial cooperation between the Member States. In this context, the EDPS emphasises once more that all personal data that have been collected, stored, processed, or analysed for the purpose of law enforcement can, in particular under the principle of availability, be subject to an exchange with competent authorities of another Member State.

36. The EDPS shares the view that the Articles 30 (1)(b) and 31 (1)(c) TEU provide for a legal basis for rules on data protection not limited to the protection of personal data that are actually exchanged between the competent authorities of the Member States but also applicable to domestic situations. In particular:

— Article 30 (1)(b) that can serve as a legal basis for rules on the collection, storage, processing, analysis and exchange of relevant information is not limited to information that has been made available or transmitted to other Member States. The only limitation imposed by Article 30 (1)(b) lies in the relevance of the information to police cooperation.

— As far as judicial cooperation is concerned, Article 31 (1)(c) is even more explicit, since common action shall include 'ensuring compatibility in rules applicable in the Member States, as may be necessary to improve such cooperation'.

— It follows from the Pupino Case ([3]), that the Court of Justice applies principles of Community law on third pillar matters. This case law reflects the development from pure cooperation between authorities of Member States within the third pillar towards an area of freedom, security and justice, comparable to the internal market as established within the EC-Treaty.

([3]) Judgment of the Court of 16 June 2005, Pupino, Case C-105/03.

— According to the EDPS, the principle of effectiveness entails the Treaty not being interpreted in a way that hampers the institutions of the European Union to carry out their tasks effectively. This includes their task to protect fundamental rights.

— As has been said before, a limitation to cross-border situations would not respect the consequences of the principle of availability and would harm the legal certainty of individuals.

37. The EDPS draws separate attention to the *exchange of data with third countries*. The Member States use personal data collected and processed in third countries transferred to them for the purpose of law enforcement and they transfer personal data that they themselves have collected and/or processed to competent authorities in third countries and to international bodies.

38. Articles 30 and 31 TEU do not require a different treatment of personal data that have been gathered by authorities of third countries to those data that have originally been collected by competent authorities within the Member States. Data originating from third countries, once received, have to comply with the same standards as data collected within a Member State. However, the quality of the data can not always easily be secured (this will be discussed in the next chapter of this opinion).

39. Transmission of personal data by competent authorities of Member States to third countries falls strictly speaking outside of the scope of Title VI of the EU-Treaty. If, however, data could be transmitted to third countries without the protection of the data subject being assured, this would seriously damage the protection envisaged by the present proposal within the territory of the European Union for the reasons mentioned in Section III.4 of this opinion. In short:

— The data subjects' rights as assured by the present proposal are directly affected if the transmission to third countries was not subjected to rules of data protection.

— The risk would occur that competent authorities of Member States could circumvent the strict norms on data protection.

40. Summarized, the applicability of common rules on data protection on personal data exchanged by competent authorities of Member States with authorities of third countries and international organisations is necessary for the effectiveness of the common rules on the protection of personal data between the competent authorities of the Member States and is thus necessary to improve the cooperation between the Member States. The Articles 30 and 31 TEU provide for the necessary legal basis.

III.3 **Specific remarks on the scope of the proposal**

Personal data processed by judicial authorities

41. Personal data are processed and exchanged by police forces and also by judicial authorities. The proposal, based on the Articles 30 and 31 of the EU-Treaty applies to the cooperation between police forces and to the cooperation between judicial authorities. At this point, the proposal has a wider scope than the proposal for a Council Framework Decision on the exchange of information, that is limited to police cooperation and only applies to information prior to the commencement of a prosecution.

42. The EDPS welcomes the fact that the proposal extends to personal data processed by judicial authorities. There is a good reason for dealing with police data and data of judicial authorities, processed for the purposes of law enforcement, in the same proposal. In the first place, the organisation in the Member States of the chain of criminal investigation and prosecution diverges. The involvement of judicial authorities starts at different stages in the different Member States. In the second place, all personal data in this chain can end up in a judicial file. There is no logic in having different applicable regimes for data protection in the foregoing stages.

43. As to the supervision on the data processing however, a different approach is needed. Article 30 of the proposal enumerates the tasks of the supervisory authorities. Article 30 (9) states that the powers of the supervisory authority shall not affect the independence of the judiciary. The EDPS recommends clarifying in the proposal that the supervisory authorities do not monitor the data processing by judicial authorities as far as they are acting in their judicial capacities. ([1])

Processing by Europol and Eurojust (and the Customs Information System)

44. According to Article 3 (2) of the proposal, the Framework Decision shall not apply to the processing of personal data by Europol, Eurojust and the Customs Information System ([2]).

([1]) The provision could be similar to the provision in Article 46 of Regulation 45/2001/EC.

([2]) The Customs Information System is a small but rather complicated system consisting of national and supranational elements, comparable to the Schengen Information System. Given the relatively limited importance of the present proposal for the Customs Information System and the complexity of the system itself, it will be left aside in this opinion. The EDPS will deal with the Customs Information System in another context.

45. Strictly speaking this provision is superfluous, in any case in so far as it relates to Europol and Eurojust. A framework decision under Article 34 (b) TEU can only be adopted for the purpose of approximation of the laws and regulations of the Member States and can not be directed to Europol and Eurojust.

46. As to substance, the text of Article 3 (2) leads to the following observations:

— the present proposal provides for a general framework, that should in principle be applicable to all situations falling within the third pillar. Consistency of the legal framework for data protection is in itself an element that enhances the effectiveness of data protection.

— at this moment, Europol and Eurojust have well defined data protection systems at their disposal, including a system of supervision. For this reason, there is no immediate urgency to adapt the applicable rules to the text of this proposal.

— in the longer term, however, the rules on data protection applicable to Europol and Eurojust should be made fully consistent with the present framework decision.

— this is even more important since the present proposal for a framework decision -apart from its Chapter III — applies to the collection and processing of personal data that are transmitted to Europol and Eurojust by the Member States.

III.4 **Structure of the proposal**

47. The EDPS has analysed the proposal and concludes that generally speaking the proposal provides for a layered structure of protection. The common standards as laid down in Chapter II of the proposal (and on specific subject-matters, in Chapters IV-VII) contain two layers of protection:

— Transposition to the third pillar of general principles of data protection as laid down in Directive 95/46/EC, and other legal instruments of the European Communities, as well as Council of Europe Convention 108.

— Additional rules on data protection, applicable to all processing of personal data within the framework of the third pillar. Examples of these additional rules can be found in Article 4 (3) and (4) of the proposal.

48. Chapter III adds a third layer of protection for specific forms of processing. The titles of the two sections of chapter III and the wording of several provisions of the proposal seem to imply that this chapter only applies to data transmitted or made available by competent authorities in other Member States. As a result, some important provisions for the protection of personal data would not apply to personal data if they are not exchanged between Member States. Having said that, the text is ambiguous since the provisions themselves seem to go beyond activities directly related to exchanged data. In any case, this limitation of the scope is not explicitly explained nor justified in the explanatory memorandum, nor in the impact assessment.

49. The EDPS underlines the added value of such a layered structure which in itself can provide for an optimal protection of the data subject, taking into account the specific needs of law enforcement. It reflects the need for an adequate data protection as expressed during the Spring Conference in Krakow in April 2005 and is in principle in conformity with Article 8 of the Charter of Fundamental Rights of the European Union and the European Convention for the protection of Human Rights and Fundamental Freedoms, in particular its Article 8.

50. However, an analysis of the text of the proposal leads to the following observations.

51. In the first place: it should be ensured that the additional rules for data protection in Chapter II (the second layer, mentioned in point 47) do not derogate from the general principles of data protection. According to the EDPS, the additional rules in Chapter II should offer additional protection to the data subjects related to the specific context of the third pillar (police and judicial information). In other words: these additional rules may not lead to a lower level of protection.

52. Moreover, Chapter III on specific forms of processing (in which the third layer of protection is incorporated) should not derogate from Chapter II. According to the EDPS, the provisions of Chapter III should offer additional protection to the data subjects in situations where competent authorities of more than one Member State are involved, but those provisions may not lead to a lower level of protection.

53. In the second place: rules that are of a general nature should not be put in Chapter III. The EDPS recommends transferring those provisions to Chapter II. Only provisions that strictly relate to the protection of personal data in case of exchanging of data between Member States must be included in Chapter III. This is even more important since Chapter III contains important provisions in view of a high level of protection of the data subject in the context of law enforcement (see IV.1 of this opinion).

IV. **ANALYSIS OF THE ELEMENTS OF THE PROPOSAL**

IV.1 **Starting points of the analysis**

54. The EDPS, in analysing the different substantive elements of the proposal, will take into account its particular structure and content. The EDPS will not comment on each article of the proposal.

55. First of all, most of the provisions of the proposal mirror other EU legal instruments on the protection of personal data. Those provisions are consistent with the EU data protection legal framework and satisfactory to provide adequate data protection safeguards in the third pillar.

56. However, the EDPS notes that some provisions currently contained in Chapter III of the proposal — on specific points of processing and generally speaking (see point 48 of this opinion) applicable only to data exchanged with other Member states — integrate general and essential principles of EU data protection law. Therefore, those provisions in Chapter III should be moved to Chapter II and made applicable to all processing of data by law enforcement authorities. This is the case of the provisions concerning the verification of data quality (Article 9 (1) and (6)) and regulating further processing of personal data (Article 11(1)).

57. Some of the other articles of Chapter III of the proposal do not distinguish between additional conditions that are specifically related to the exchanges of data with other Member States — such as the consent of the competent authority of the transmitting Member State — and safeguards that are instead relevant and necessary also with regard to data processed within a Member state. In these cases, the EDPS recommends that the latter safeguards should be made generally applicable, even to those personal data that have not been transmitted or made available by another Member State. This recommendation concerns:

— transmission of data to private parties and to non law enforcement authorities (letters a) and b) of Articles 13 and 14), and

— transfers to third countries or international bodies (Article 15, except letter c)).

58. This part of the opinion will also draw the attention of the legislator to some additional safeguards that are not laid down by the current proposal. According to the EDPS, these additional safeguards should be provided in relation to automated individual decisions, personal data received from third countries, access to private parties' databases, processing of biometric data and DNA profiles.

59. In addition, the following analysis will provide recommendations to improve the current text, with a view to ensuring effectiveness of the provisions, coherence of the text and consistency with current data protection legal framework.

IV.2 **Purpose limitation and further processing**

60. Article 4 (1)(b) states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Normally, data will be collected in relation to a specified crime (or, under certain circumstances, to investigate a criminal group or network, etc). They can be used for that original purpose and might then be processed for another purpose provided it is compatible with the original one (data collected on an individual convicted of drug trafficking could be used in the framework of an investigation concerning a network of drug dealers, for instance). This approach reflects well the principle of purpose limitation, as it is also enshrined in Article 8 of the Charter of Human Rights for the European Union and is thus consistent with current data protection legislation.

Further processing for purposes within the scope of the Framework Decision

61. The EDPS notes that the proposal does not address completely satisfactorily one situation which may occur in police work: the need to further use the data for a purpose considered incompatible with the one they were collected for. Data, once collected by the police, might be needed to solve a completely different crime. To illustrate this, one can mention that data are collected for the prosecution of traffic offences and then used to locate and prosecute a car thief. The second purpose, however legitimate, cannot be considered as fully compatible with the purpose of the collection of data. If law enforcement authorities were not allowed to use the data for this second purpose, they could be inclined to collect data for broad or ill-defined purposes, in which case the principle of purpose limitation would loose its value as to collection. Moreover, the application of other principles, like proportionality, accuracy and reliability would be hampered (see Article 4 (1)(c) and (d)).

62. Under EU data protection law personal data must be collected for specified and explicit purposes and not further processed in a way incompatible with those purposes. However, the EDPS is of the opinion that some flexibility must be allowed as to further use. The limitation on collection is more likely to be well complied with if the authorities in charge of internal security know that they can rely, with appropriate safeguards, on a derogation to the limitation as to further use.

63. It should be clarified that this need for further processing is recognised in Article 11 of the proposal, but in a fairly insufficient way. Article 11 only applies to data received from or made available by the competent authority of another Member State and does not provide for sufficient safeguards.

64. The EDPS recommends applying Article 11 (1) to all data, regardless of whether or not they have been received from another Member State. Moreover, stricter safeguards should be added to what is stipulated in 11 (1)(b): the further use of data for a purpose considered incompatible with the initial one should be allowed only when it is strictly necessary, in a specific case, for the prevention, investigation, detection and prosecution of criminal offences or for the protection of the interests or fundamental rights of a person. Practically, the EDPS suggests laying down this provision in a new Article 4 bis (in any case, in Chapter II of the proposal).

65. Article 11 (2) and 11 (3) remain applicable as they are; they provide for supplementary safeguards for data received from other Member States. The EDPS points out that Article 11 (3) will apply to data exchange through the SIS II: the EDPS already mentioned in his opinion on SIS II that it should be ensured that indeed SIS data cannot be used for any other purpose than the purposes of the system itself.

Further processing for purposes outside the scope of police and judicial cooperation

66. In some cases, the data must be processed for the safeguard of other important interests. They could in these cases even be processed by other authorities than the competent authorities under this Framework Decision. These competences of the Member States could involve a privacy intrusive processing (for example, the screening of a person who is not a suspect) and should thus be accompanied by very strict conditions, like the obligation for Member States to adopt specific legislation if they want to make use of this derogation. Within the framework of the first pillar, this issue has been addressed in Article 13 of Directive 95/46/EC, stipulating that in specific cases restrictions to some provisions of the Directive are allowed. Member States applying such restrictions must do so in compliance with Article 8 ECHR.

67. Along the same line of reasoning, this Framework Decision should stipulate in Chapter II that Member States should be allowed to adopt legislative measures to allow further processing when such a measure is necessary to safeguard:

— the prevention of threats to public security, defence or national security;

— the protection of an important economic or financial interest of a Member State or of the European Union.

— the protection of the data subject.

IV.3 **Criteria for making data processing legitimate**

68. Article 5 of the proposal states that data may be processed by the competent authorities only if provided for by a law setting out that the processing is necessary for the fulfilment of the legitimate task of the authority concerned and for the purpose of the prevention, investigation, detection or prosecution of criminal offences. The EDPS supports the strict requirements of Article 5.

69. However, the text of Article 5 underestimates the need for making data processing legitimate on other legal grounds, in specific circumstances. It is an important provision that should, for instance, not make it impossible for the police to fulfil its legal obligations under national law to disclose information to immigration services or taxation authorities. Therefore, the EDPS suggests that Article 5 take into account other justified legal grounds for processing personal data, such as the necessity for compliance with a legal obligation to which the controller is subject, the unambiguous consent of the data subject, provided that the processing is carried out in the interest of the data subject, or the necessity to protect the vital interest of the data subject.

70. The EDPS remarks that respect of the criteria for making data processing legitimate has a special importance with regard to police and judicial cooperation, if one considers that an unlawful collection of personal data by police forces could entail that personal data not being able to be used as evidence in judicial proceedings.

IV.4 **Necessity and proportionality**

71. The Articles 4 and 5 of the proposal also aim to ensure — in a generally satisfactory manner — that limitations to the protection of personal data are necessary and proportional, as required under the law of the European Union and by the case law of the European Court of Human Rights on Article 8 ECHR:

— Article 4(1)(c) lays down the general rule that data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

— Article 5 specifies that the processing should be *necessary* for the fulfilment of the legitimate task of the authority concerned and for the purpose of the prevention, investigation, detection or prosecution of criminal offences.

— Article 4(4) states that processing of personal data is only necessary if certain specific conditions are fulfilled.

72. The EDPS notes that the proposed formulation of Article 4(4) does not meet the criteria laid down by the case law of the European Court of Human Rights relating to Article 8 ECHR, according to which a restriction to private life might be imposed only when it is necessary in a democratic society. According to the proposal, data processing would be considered as necessary not only when it would *make it possible* for law enforcement and judicial authorities to carry out their tasks, but also when there are *reasonable grounds* to *believe* that the personal data concerned would merely *facilitate or accelerate* the prevention, investigation, detection or prosecution of a criminal offence.

73. These criteria do not comply with the requirements of Article 8 ECHR, since almost any processing of personal data could be considered as facilitating the activities of police or of judicial authorities, even though the concerned data are not actually needed to carry out those activities.

74. The current text of Article 4 (4) would pave the way to unacceptably broad collection of personal data, merely based on the belief that personal data *may make it easier* to prevent, investigate, detect or prosecute a criminal offence. On the contrary, processing of personal data shall be considered necessary only where the competent authorities can clearly demonstrate a need for it, and provided that less privacy-intrusive measures are not available.

75. Therefore, the EDPS recommends redrafting the first indent of Article 4 (4) so as to ensure the respect of the case law on Article 8 ECHR. Furthermore, for systematic reasons, the EDPS suggests that Article 4 (4) is moved to the end of Article 5.

IV.5 **Processing of special categories of data**

76. Article 6 lays down an in-principle prohibition on the processing of sensitive data, i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life. This prohibition will not apply when the processing is provided for by a law and is absolutely necessary for the fulfilment of the legitimate task of the authority concerned for the purpose of the prevention, investigation, detection or prosecution of criminal offences. Sensitive data can also be processed if the data subject has given his explicit consent. In both cases, suitable specific safeguards shall be put in place.

77. The text of Article 6 leads to two remarks. In the first place, Article 6 relies too widely on the consent of the data subject. The EDPS stresses that processing of sensitive data on the basis of the explicit consent of the data subject should be allowed only insofar as the processing is carried out in the interest of the data subject, and the refusal to consent would not lead to negative consequences being imposed on the data subject. The EDPS recommends modifying Article 6 accordingly, also to make the article consistent with current EU data protection law

78. In the second place, the EDPS considers that also other legal grounds for processing, such as the necessity to protect the vital interests of the data subject or of another person (where the data subject is physically or legally incapable of giving his consent) could be taken into account.

79. In the field of police and judicial cooperation, the processing of other categories of possibly sensitive personal data, such as biometric data and DNA profiles, are of a growing importance. Those data are not explicitly covered by Article 6 of the proposal. The EDPS invites the EU legislator to pay special attention when implementing the general data protection principles laid down in this proposal into further legislation entailing the processing of these special categories of data. An example is the current proposal for a Council framework decision on the exchange of information under the availability principle (see above, points 12-15), which explicitly allows for processing and exchanges of biometric data and DNA profiles (see Annex II of the proposal), but does not address the sensitiveness and specificities of these data from a data protection point of view.

80. The EDPS recommends that specific safeguards should be provided, in particular with a view to guarantee that:

— biometric data and DNA profiles are used only on the basis of well established and interoperable technical standards,

— their level of accuracy is carefully taken into account and might be challenged by the data subject through readily available means, and

— that the respect of the dignity of persons is fully ensured.

It is for the legislator to decide whether to provide for these additional safeguards in this framework decision or in the specific legal instruments regulating the collection and exchange of these special categories of data.

IV.6 **Accuracy and reliability**

81. Article 4 (1) (d) lays down the general rules relating to data quality. According to this Article, the controller must ensure that data are accurate and, where necessary, up to date. He shall take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. This is in line with the general principles of EU data protection legislation.

82. Article 4 (1) (d), third sentence, establishes that Member States may provide for the processing of data to varying degrees of accuracy and reliability. The EDPS understands this provision as a derogation to the general principle of accuracy and recommends clarifying the derogatory nature of the provision, by adding 'however' or 'nevertheless' to the beginning of Article 4 (1)(d), third sentence. In these cases, where the accuracy of data cannot be fully ensured, the controller will have an obligation to distinguish data in accordance with their degree of accuracy and reliability, referring in particular to the fundamental distinction between data based on facts from data based on opinions and personal assessments. The EDPS underlines the importance of this obligation both for data subjects and law enforcement authorities, especially where data are processed far from their source (see point 7 of this opinion).

Verification of data quality

83. The general principle laid down in Article 4(1)(d) is supplemented by the more specific safeguards laid down in Article 9 on verification of data quality. In particular, Article 9 states that:

1. quality of personal data shall be verified at the latest before they are transmitted and made available. In addition, for data made available by direct automated access, the quality shall be regularly verified (Article 9 (1) and (2)).

2. in all transmissions of data, judicial decisions as well as decisions not to prosecute should be indicated, and data based on opinions checked at source before being transmitted, and their degree of accuracy or reliability indicated (Article 9 (1)).

3. personal data shall be marked on request of the data subject if their accuracy is denied by the data subject and if their accuracy or inaccuracy cannot be ascertained (Article 9 (6).

84. Therefore, Article 4(1) and Article 9 ensure, if jointly applied, that the quality of personal data is adequately verified, both by the data subject and by those authorities that are the closest to the sources of the data processed and thus in the best position to check them.

85. The EDPS welcomes these provisions, since, while focussing on the needs of law enforcement authorities, they ensure that each data is properly taken into account and used according to its accuracy and reliability, thus avoiding that a data subject is disproportionately affected by the possible lack of accuracy in some data concerning him or her.

86. Verification of data quality is an essential element of protection for the data subject, especially with regard to personal data processed by police and judicial authorities. Therefore, the EDPS regrets that the applicability of Article 9 on verification of quality of data is limited to data that are transmitted or made available to other Member states. This is unfortunate, since it entails that quality of personal data, which is essential also for law enforcement purposes, would be fully ensured only when these data are transmitted or made available to other Member States, but not when they are processed within a Member State [1]. Instead, it is essential — both in the interest of data subjects and of competent authorities — to ensure that proper verification of the quality concerns all personal data, including those not transmitted or made available by another Member state.

87. Therefore, the EDPS recommends removing in any case the limitations in the scope of application of Article 9 (1) and (6), by moving these provisions to Chapter II of the proposal.

The distinction between different categories of data

88. Article 4(2) lays down an obligation for the controller to make a clear distinction between personal data of different categories of persons (suspected, convicted, witnesses, victims, informers, contacts, others). The EDPS welcomes this approach. While it is true that law enforcement and judicial authorities might need to process data relating to very different categories of persons, it is essential that these data are distinguished according to the different degree of involvement in a crime. In particular, conditions for collecting data, time limits, conditions for refusing access or information to the data subject, modalities of access to data by competent authorities should reflect the particularities of the different categories of data processed and the different purposes for which these data are collected by law enforcement and judicial authorities.

89. In this context, the EDPS asks special attention for data relating to non-suspects. Specific conditions and safeguards are needed in order to ensure proportionality and to avoid prejudice for persons that are not actively involved in a crime. For this category of persons the proposal should contain additional provisions to restrict the purpose of the processing, to fix precise time limits and to limit the access to data. The EDPS recommends modifying the proposal accordingly.

[1] In addition, this would not be in line with Council of Europe's Recommendation No.R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector. In particular, Principle 7.2 provides that 'regular checks' on the quality of personal data should be established in agreement with the supervisory authority or in accordance with domestic law.

90. The current text of the proposal contains one specific safeguard relating to non suspects, namely Article 7 (1) of the proposal. According to the EDPS, this is an important safeguard, mainly since Member States are not allowed to provide for derogations. Unfortunately, Article 7 (1) lays down specific safeguards only with regard to time limits, and its applicability is limited to the category of persons mentioned in the last indent of Article 4 (3) of the proposal. Therefore, it does not provide for satisfactory guarantees and does not cover the whole group of non-suspects. ([1])

91. Also data relating to convicted persons deserve specific attention. Indeed, as far as these data are concerned, the recent and future initiatives on exchanges of criminal records should be duly taken into account and consistency should be ensured. ([2])

92. In the light of the foregoing observations, the EDPS recommends adding a new paragraph to Article 4 that contains the following elements:

— additional provisions to restrict the purpose of the processing, to fix precise time limits and to limit the access to data, as far as non suspects are concerned.

— the obligation for the Member States to lay down the legal consequences of the distinctions to be made between personal data of different categories of persons, reflecting the particularities of the different categories of data processed and the different purposes for which these data are collected by law enforcement and judicial authorities.

— the legal consequences should relate to conditions for collecting personal data, time limits, further transfer and use of data and conditions for refusing access or information to the data subject.

IV.7 **Time limits for the storage of personal data**

93. The general principles governing time limits for storage of personal data are laid down by Article 4(1)(e) and Article 7(1) of the proposal. As a general principle, personal data should be stored for no longer than necessary for the purpose for which they were collected. This is consistent with EU data protection legislation. ([3])

94. Nevertheless, the general provision of Article 7 (1) is only applicable 'unless otherwise provided by national law'. The EDPS notes that this exception is very general and goes beyond the derogations admissible according to Article 4(1)(e). The EDPS proposes that the general derogation of Article 7 (1) should be deleted or at least explicitly restrict the public interests justifying the use of this derogation by the Member States ([4]).

95. Article 7(2) states that the compliance with time limits shall be ensured by appropriate procedural and technical measures, and shall be regularly reviewed. The EDPS welcomes this provision, but recommends to state explicitly that the appropriate procedural and technical measures should provide for automatic and regular deletion of personal data after a certain period of time.

IV.8 **Exchanges of personal data with third countries**

96. Effective police and judicial cooperation within the EU borders increasingly depends on cooperation with third countries and international organisations. Many actions aimed at improving law enforcement and judicial cooperation with third countries or international organisations are currently discussed or envisaged both at national and EU level ([5]). The development of this international cooperation is likely to rely heavily on exchanges of personal data.

97. Therefore, it is essential that principles of fair and lawful processing — as well as principles of due process in general — also apply to the collection and the exchanges of personal data across Union borders, and that personal data are transferred to third countries or international organisations only if an adequate level of protection or appropriate safeguards are guaranteed by those third parties concerned.

([1]) See, more specific, point 94 of this opinion.

([2]) The decision of the Council 2005/876/JHA on the exchange of information extracted from the criminal record entered into force on 9 December. The decision adds to and facilitates existing mechanisms to transmit information referring to sentences based on existing conventions, such instruments as the European Convention on judicial assistance in criminal matters of 1959 and on the 2000 Convention on judicial assistance in criminal matters between the Member States. This text will later be replaced by a more precise Framework decision of the Council. The Commission envisages to propose a new Framework Decision in this area..

([3]) Besides the general provision on time limits for the storage of personal data, laid down by Article 7, the proposal lays down further specific provisions concerning personal data exchanged with other Member States. In particular, Article 9.7 establishes that personal data shall be deleted when:
1. they should not have been transmitted, made available or received
2. after a time limit communicated by the transmitting authority, unless the personal data are further needed for judicial proceedings
3. if data are not or no longer necessary for the purpose for which they were transmitted.

([4]) One could consider a limitation to the fight of terrorism and/or the specific public interests mentioned in Article 4 (1) (e): historical, statistical or scientific use.

([5]) For an example, see the recent Commission's Communication on 'A Strategy on the External Dimension of the Area of Freedom, Security and Justice' (COM(2005) 491 Final).

Transfers of personal data to third countries

98. In this perspective, the EDPS welcomes Article 15 of the proposal that provides for protection in case of transfer to competent authorities in third countries or to international bodies. However, this provision, included in Chapter III of the proposal, only applies to data received from or made available by competent authorities of other Member States. As a consequence of this limitation, a shortcoming in the system of data protection on the level of the European Union remains with regard to data that are not received from competent authorities from other Member States. According to the EDPS, this shortcoming can not be accepted for the following reasons.

99. Firstly, the level of protection offered by EU law in case of transfer to third country should not be determined by the source of the data — a police force within the Member State that transfers data to a third country, or a police force within another Member State.

100. Secondly, it should be noted that the rules regulating transfers of personal data to third countries represent a fundamental principle of data protection law. This principle does not only represent one of the fundamental provisions of Directive 95/46/EC, but it is also enshrined by the Additional Protocol to Convention 108 [1]. Common standards in protection of personal data, referred to by Article 1 of the proposal, could not be ensured if common rules for transfers of personal data to third countries do not embrace all processing operations. As a consequence, the data subjects' rights as ensured by the present proposal would be directly affected if personal data could be transmitted to third countries that do not offer an adequate level of protection.

101. Thirdly, limitation of the scope of these rules to 'exchanged data' would entail that — with regard to data processed only within one country — there would be no safeguards: paradoxically personal data could be transferred to third countries — disregarding any adequate protection of personal data — more 'easily' than to other Member States. This would give rise to possibilities of 'information laundering'. Competent authorities of Member States could circumvent the strict norms on data protection by transmitting data to third countries or international organisations, where they could be accessed by a competent authority of another Member State or even sent back to such an authority.

102. Therefore, the EDPS recommends amending the present proposal so as to ensure that Article 15 applies to the exchange of *all* personal data with third countries. This recommendation does not relate to Article 15 (1)(c) that by its nature can only be relevant to personal data exchanged with other Member States.

Exceptional transfers to non adequate countries

103. Article 15 lays down a series of conditions for transfers to competent authorities in third countries or to international organisations comparable to the conditions of Article 25 of Directive 95/46/EC. Nonetheless, Article 15(6) lays down the possibility to transfer data to third countries or international organisations in which an adequate level of data protection is not ensured, provided that the transfer is absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.

104. The applicability of the exception laid down by paragraph 6 should be clarified. Therefore, the EDPS recommends:

— making clear that this exception merely establishes a derogation to the condition of 'adequate protection' but does not impinge on the other conditions laid down by the first paragraph of Article 15.

— adding that transfers of data carried out according to this exception should be subject to appropriate conditions (such as an explicit condition that data shall be processed only temporarily and for specific purposes) and shall be communicated to the competent Supervisory Authority.

Processing of personal data received from third countries

105. In the context of the increasing exchange of personal data with police and judicial authorities of third countries, special attention should also be paid to the personal data 'imported' from those third countries where adequate standards of respect for human rights — and in particular for protection of personal data — are not ensured.

[1] The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, was signed on 8/11/2001 and entered into force on 1/7/2004. This binding international law instrument has been signed so far by 11 States (9 of which are EU Members). Article 2.1 of the Protocol lays down the general principle that 'Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer'.

106. From a broader perspective, the EDPS considers that the legislator should ensure that personal data received from third countries comply at least with international standards regarding the respect of human rights. For example, data collected under torture or through violations of human rights, blacklists based merely on political convictions or sexual preferences should not be processed and relied upon by law enforcement and judicial authorities, unless this is done in the interest of the data subject. Therefore, the EDPS recommends that this is clarified at least in a recital of the proposal, possibly by reference to relevant international instruments ([1]).

107. With regard more specifically to protection of personal data, the EDPS remarks that, when personal data are transmitted from countries where there are no adequate standards and guarantees for the protection of personal data, the possible lack of data quality shall be duly assessed with a view to avoiding erroneous reliance on such information by EU law enforcement authorities and preventing prejudice for data subjects.

108. Therefore, the EDPS recommends adding a provision to Article 9 of the proposal stating that the quality of personal data transmitted from third countries should be specifically assessed as soon as they are received and the degree of accuracy and reliability of those data should be indicated.

IV.9 **Exchanges of personal data with private parties and non law enforcement authorities**

109. Articles 13 and 14 of the proposal lay down a series of requirements to be fulfilled in cases where personal data are further transmitted to private parties and non law enforcement authorities. As mentioned before, these articles supplement the more general rules laid down in Chapter II, which should in any case be complied with.

110. The EDPS is of the opinion that, while transfer to private parties and other public bodies can be necessary in particular cases for the purpose of preventing and combating crime, specific and strict conditions should apply. This is line with the point of view expressed by the European Data Protection Commissioners in the Krakow position paper ([2]).

111. In this perspective, the EDPS considers that additional conditions laid down by Articles 13 and 14 could be considered satisfactory, if applied jointly with general rules laid down in Chapter II, including a comprehensive application of the rules on further processing (see above, IV.2). However, the current proposal limits the applicability of Articles 13 and 14 to personal data received from or made available by the competent authorities of another Member State.

112. The general applicability of the latter conditions is even more important if one considers the growing exchange of data between law enforcement authorities and other authorities or private parties also within Member States. An example can be found in the public/private partnership in law enforcement activities ([3]).

113. Therefore, the EDPS recommends amending the present proposal so as to ensure that Article 13 and 14 apply to the exchange of *all* personal data, including those not transmitted or made available by another Member State. This recommendation does not relate to Articles 13 (c) and 14 (c).

Access and further use of personal data controlled by private parties

114. The exchange of personal data with private parties is bidirectional: it entails personal data also being transmitted or made available by private parties to law enforcement and judicial authorities.

115. In this case, personal data collected for commercial purposes (commercial transactions, marketing, provision of services, etc.) and managed by private controllers are then accessed and further used by public authorities for the very different purpose of prevention, investigation, detection or prosecution of criminal offences. In addition, the accuracy and reliability of data processed for commercial purposes shall be carefully assessed when these data are used for law enforcement purposes ([4]).

([1]) UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, signed by all EU Member States and entered into force on 26 June 1987. In particular, Article 15 states that 'Each State Party shall ensure that any statement which is established to have been made as a result of torture shall not be invoked as evidence in any proceedings, except against a person accused of torture as evidence that the statement was made'.

([2]) *Position paper on Law Enforcement & Information Exchange in the EU*, adopted at the Spring Conference of European Data Protection Authorities, Krakow, 25-26 April 2005

([3]) See Commission Legislative and Work Programme 2006 COM(2005) 531 final

([4]) For example, a phone bill will be reliable for commercial purposes as long as it correctly states which phone calls have been made; anyway, the same phone bill might not be fully relied upon by law enforcement authorities as conclusive evidence about who made a specific phone call.

116. A very recent and important example of access to private databases for law enforcement purposes is provided by the approved text of the Directive on the retention of communication data (see above, points 16-18), according to which providers of publicly available electronic communications services or of public communications networks will have to store for up to two years certain data concerning communications, in order to ensure that these data are available for the purpose of the investigation, detection and prosecution of serious crime. According to the approved text, issues concerning access to these data go beyond Community law and might not be regulated by the Directive itself. Instead, these important issues may be the subject of national law or action pursuant to Title VI of the TUE ([1]).

117. In his opinion on the proposal for this directive, the EDPS has defended a wider interpretation of the EC-Treaty, because limitation on access is necessary to assure an adequate protection of the data subject whose communications data have to be retained. Unfortunately, the European legislator did not include rules on access in the abovementioned directive.

118. In the present opinion, the EDPS expresses again his strong preference that EU law should provide common standards on access and further use by law enforcement authorities. As long as this is not dealt with under the first pillar, a third pillar instrument could provide for the necessary protection. This position of the EDPS is further supported by the general increase of exchanges of data between Member States and the recent proposal on availability principle. Different national rules on access and further use would not be compatible with the proposed EU-wide 'free circulation' of law enforcement information, which also includes data from private databases.

119. Therefore, the EDPS considers that common standards should apply on access by law enforcement authorities to personal data held by private parties, so as to ensure that access is permitted only on the basis of well defined conditions and limitations. In particular, access by competent authorities should be allowed only on a case-by-case basis, under specified circumstances, for specified purposes, and be under judicial control in the Member States.

([1]) According to the recitals of the Directive 'Issues of access to data retained pursuant to this Directive by national public authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be the subject of national law, or action pursuant to Title VI of the Treaty on European Union, always noting that such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as they are guaranteed by the ECHR. Article 8 ECHR, as interpreted by the European Court of Human Rights...'

IV.10 **Rights of the data subject**

120. Chapter IV deals with the rights of the data subject, in a way which is in general consistent with current data protection legislation and with Article 8 of the EU Charter of Fundamental Rights.

121. The EDPS welcomes these provisions, since they provide for a harmonised set of rights for data subjects, while taking into account the particularities of processing by law enforcement and judicial authorities. This is a significant improvement, since the current situation is characterized by a wide variety of rules and practices especially concerning the right of access. Some Member States do not allow for access of the data subject to his data but have a system of 'indirect access' (to be exercised by the national data protection authority in the name of the data subject).

122. Under the proposal, the possible derogations to the direct right of access are harmonized. This is all the more important to allow citizens, whose data are increasingly processed and exchanged by competent authorities of different EU Member States, to avail themselves of a harmonised set of rights as data subjects, disregarding the Member State in which data are collected or processed ([2]).

123. The EDPS recognizes the opportunity to restrict data subjects' rights in those cases when this is necessary for the purpose of the prevention, investigation, detection or prosecution of criminal offences. Anyway, since these limitations must be considered as exceptions to basic rights of the data subjects, a strict proportionality test should apply. This means that exceptions should be limited and well defined, and that restrictions should be, where possible, partial and limited in time.

124. In this perspective, the EDPS would like to draw the attention of the legislator especially to letter (a) of paragraph 2 of Articles 19, 20, 21, which lay down a very broad and undefined exception to the rights of data subjects, by stating that these rights may be restricted if necessary to 'enable the controller to fulfil its lawful duties properly'. Furthermore, this exception overlaps with the provision of letter (b), which allows restrictions of data subject's rights when it is necessary 'to avoid

([2]) In particular, Chapter IV deals with the right of information (Articles 19 and 20) and the right of access, rectification, erasure or blocking (Article 21). In general, these articles provide data subjects with all the rights that are usually guaranteed by EU data protection law, while laying down a series of exceptions aimed at taking into account the peculiarities of the third pillar. In particular, restrictions to data subjects' rights are allowed by almost identical provisions laid down with regard to both right to information (Articles 19.2 and 20.2) and right to access (Article 21.2).

prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities'. While the latter exception can be deemed to be justified, the former appears to impose a disproportionate restriction on data subject's rights. Therefore, the EDPS recommends deleting letter (a) of paragraph 2 of Articles 19, 20, 21.

125. In addition, the EDPS recommends improving Articles 19, 20, 21 as follows:

— specify that the restrictions on the rights of the data subject are not compulsory, do not apply for an indefinite period of time and are permitted 'only' in the specific cases listed in the articles,

— take into account that information should be provided by the controller autonomously and not on the basis of a request by the data subject,

— add to Article 19(1)(c) that information should also be provided on 'the time-limits for storing the data',

— ensure (by amending Article 20 (1) in line with other EU data protection instruments) that information — where data have not been obtained from the data subject or have been obtained from him without his knowledge — shall be provided to him 'no later than the time when data are first disclosed'

— ensure that the mechanism to appeal against refusal or restriction of the data subjects' rights is applicable to cases of restriction of the right to be informed and amend the last sentence of Article 19(4) accordingly.

Automated individual decisions

126. The EDPS regrets that the proposal does not address the important issue of automated individual decisions at all. In fact, practical experience shows that law enforcement authorities make increasing use of automated processing of data intended to evaluate certain personal aspects of persons, in particular in order to assess their reliability and conduct.

127. The EDPS — while recognising that these systems may be necessary in certain cases in order to increase the effectiveness of law enforcement activities — notes that decisions based solely on automated processing of data should be subject to very strict conditions and safeguards when they produce legal effects concerning a person or significantly affect a person. This is even more important in the third pillar context, since in this case competent authorities are endowed with public coercive power and thus their decisions or actions are likely to affect a person or to be more intrusive than would normally happen where such decisions/actions are taken by private parties.

128. In particular, and consistently with general data protection principles, such decisions or actions should be allowed only if expressly authorized by law or by the competent supervisory authority, and should be subject to appropriate measures aimed at safeguarding the data subject's legitimate interests. Moreover, the data subject should have readily available means allowing him/her to put forward his or her point of view and be able to know the logic of the decision, unless this is incompatible with the purpose for which data are processed.

129. Therefore, the EDPS recommends introducing a specific provision on automated individual decisions, in line with current EU data protection legislation.

IV.11 **Security of processing**

130. As far as security of processing is concerned, Article 24 lays down an obligation for the controller to implement appropriate technical and organisational measures, which are in line with the provisions of other EU data protection instruments. Furthermore, paragraph 2 gives a detailed and comprehensive list of measures that shall be implemented with regard to automated data processing.

131. The EDPS welcomes this provision, but suggests, with a view to facilitating an effective control by supervisory authorities, to add to the list of measures laid down by paragraph 2 the following supplementary measure: *'k) implement measures to systematically monitor and report on the effectiveness of these security measures (systematic self-auditing of security measures)*'. ([1])

Logging of data

132. Article 10 states that each automated transmission or reception of personal data shall be logged in (in case of automated transmission) or documented (in case of non automated transmission), in order to ensure the subsequent verification of the lawfulness of transmission and data processing. Such information shall be available on request to the competent supervisory authority.

([1]) See, in the same sense, the opinion of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM(2004) 835 final, published on www.edps.eu.int

133. The EDPS welcomes this provision. Nonetheless, the EDPS notes that, in order to ensure a comprehensive supervision and check proper use of personal data, also 'access' to data shall be logged in or documented. This information is essential, since an effective monitoring of a proper processing of personal data must focus not only on the lawfulness of the transmission of personal data between authorities, but also on the lawfulness of the access by those authorities [1]. Therefore, the EDPS recommends modifying Article 10 so as to provide that also access to data is logged or documented.

IV.12 **Judicial remedies, liability and sanctions**

134. Chapter VI of the proposal deals with judicial remedies (Article 27), liability (Article 28) and sanctions (Article 29). The provisions are in general consistent with current EU data protection legislation.

135. In particular, as far as sanctions are concerned, the EDPS welcomes the specification that sanctions, in case of infringement of the provisions laid down pursuant to the framework decision, will have to be effective, appropriate and dissuasive. Furthermore, criminal sanctions in case of intentionally committed offences implying serious infringements — especially with regard to confidentiality and security of processing — will ensure a higher deterrent effect for more serious breaches of data protection law.

IV.13 **Control, supervision and advisory tasks**

136. The provisions in the proposal that deal with the control and the supervision of data processing, as well as on the consultation on matters related to data processing resemble to a large extent the provisions of Directive 95/46/EC. The EDPS welcomes that the Commission has opted in its proposal for already tested and well functioning mechanisms and underlines in particular the introduction of a (compulsory) system of prior checking. Such a system is not only foreseen in Directive 95/46/EC, but is moreover included in Regulation 45/2001/EC and has proved to be an effective instrument at the disposal of the EDPS in the supervision of data processing by institutions and bodies of the European Communities.

137. Another instrument for the control and supervising of data processing that has proved to be effective is the appointment of Data Protection Officers by a controller. This instrument functions in several Member States. It is laid down in Regulation 45/2001/EC as a compulsory instrument and plays a key role on the level of the European Communities. Data Protection Officers are administrators within an organisation that shall ensure in an independent manner the internal application of provisions on data protection.

138. The EDPS recommends adding provisions on Data Protection Officers to the proposal. These provisions could be modelled analogous to the Articles 24-26 of Regulation 45/2001/EC.

139. The proposal for a framework decision is directed to the Member States. It is therefore logical that Article 30 of the proposal foresees supervision by independent supervisory authorities. This article is drafted in a similar way as Article 28 of Directive 95/46/EC. These national authorities should cooperate with each other, with the joint supervisory bodies set up under Title VI of the EU Treaty and with the EDPS. Moreover, Article 31 of the proposal envisages the establishment of a Working Party which must play a similar role as the Article 29 Working Party plays in first pillar matters. All the relevant players in the area of data protection are mentioned in Article 31 of the proposal.

140. It goes without saying that, in a proposal that envisages improving the police and judicial cooperation between the Member States, cooperation between all the relevant players in the area of data protection plays an important role. The EDPS therefore welcomes the emphasis in the proposal on cooperation between the supervisory bodies.

141. Moreover, the EDPS emphasises the importance of a consistent approach on matters of data protection that could be enhanced by promoting the communication between the existing Article 29 Working Party and the Working Party established by the present proposal for a Framework Decision. The EDPS recommends an amendment of Article 31 (2) of the proposal so as to also entitle the chairperson of the Article 29-Working Party to participate or be represented in meetings of the new Working Party.

142. The text of Article 31 of the present proposal contains one remarkable difference with Article 29 of Directive 95/46/EC. The EDPS is a full member of the Article 29 Working Party. This membership includes the right to vote. The present proposal also designates the EDPS as a member of the Working Party (based on Article 31), but does not foresee a right to vote for the EDPS. It is not clear for what reasons the present proposal deviates from Article 29 of Directive 95/46/EC. According to the EDPS, the proposed text is ambiguous about the role of the EDPS which could hamper the effectiveness of his involvement in the work of the Working Party. The EDPS therefore recommends retaining consistency with the text of the directive.

[1] This is in line with the provisions laid down by Article 18 of the proposal, according to which the transmitting authority will be informed on request about the further processing of the personal data transmitted or made available, and by Article 24, implementing the security measures, also in the light of the proposed systematic self-auditing of these measures.

IV.14 **Other provisions**

143. Chapter VIII of the proposal contains some final provisions amending the Schengen Convention and other instruments concerning the processing and protection of personal data.

Schengen Convention

144. Article 33 of the proposal stipulates that Articles 126 to 130 of the Schengen Convention will be replaced by this Decision for the matters falling within the scope of the EU Treaty. Articles 126 to 130 of the Schengen Convention contain the general data protection rules for processing of data communicated pursuant to the Convention (but outside of the Schengen Information System).

145. The EDPS welcomes this replacement as it improves consistency of the data protection regime in the third pillar and represents in some respects a significant improvement for the protection of personal data, for instance by increasing the powers of the supervisory authorities. However, it has on some points, the unintended — and unfortunate — result of lowering the level of data protection. Some provisions of the Schengen Convention are indeed stricter than those of the Framework Decision.

146. The EDPS especially mentions Article 126 (3) (b) of the Schengen Convention that states that data can be used only by judicial authorities and departments and authorities carrying out tasks or performing duties in relation with the purposes stipulated by the Convention. This provision seems to exclude the transmission to private parties, while it would be allowed under the proposed Framework Decision. Another point is that the data protection provisions in the Schengen Convention apply also to *all* data communicated from or included in *non-automated* files (Article 127), while non structured files are excluded from the scope of the proposed Framework Decision.

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union

147. Article 34 states that Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union is replaced by the framework decision. The EDPS notes that while this replacement would in general provide for a better protection of personal data exchanged in the framework of the Convention, it could also give rise to some problems of compatibility between the two instruments.

148. In particular, the Convention deals also with mutual assistance in interceptions of telecommunications. In this case, the requested Member State may give its consent — to the interception or transmission of the recording of telecommunications — subject to any conditions which would have to be observed in a similar national case. According to Article 23(4) of the Convention, when these additional conditions relate to the use of personal data, they will prevail on the data protection rules laid down by Article 23. Analogously, Article 23(5) determines the precedence of the additional rules safeguarding information collected by joint investigation teams. The EDPS notes that if Article 23 is replaced by the current proposal, it would be unclear whether the aforementioned additional rules would be still applicable. Therefore, the EDPS recommends clarifying this point, with a view to thoroughly assessing the consequences of a full replacement of Article 23 of the Convention by this framework decision.

Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data

149. Article 34(2) states that any reference to the Convention 108 shall be construed as a reference to this Framework Decision. The interpretation and the concrete applicability of this provision are far from being clear. In any case, the EDPS assumes that this provision only applies within the scope *ratione materiae* of this Framework Decision.

Final issues

150. As far as the systematic coherence of the text is concerned, the EDPS notes that some articles could find a better location in the text of the proposal.

Therefore, the EDPS suggests:

1. Moving Article 16 ('Committee') from Chapter III ('Specific forms of processing') to a new chapter

2. Moving Article 25 ('Register') and 26 ('Prior checking') from Chapter V ('Confidentiality and security of processing') to a new chapter

V. **CONCLUSIONS**

A considerable step forwards

a) The adoption of this proposal would mean a considerable step forwards for the protection of personal data, in an important area which in particular requires a consistent and effective mechanism for the protection of personal data on the level of the European Union.

b) An effective protection of personal data is not only important for the data subjects but also contributes to the success of the police and judicial cooperation itself. In many aspects, both public interests go hand in hand.

Common standards

c) According to the EDPS, a new framework for data protection should not only respect the principles of data protection — it is important to guarantee the consistency of the data protection within the European Union — but also provide for an additional set of rules taking into account the specific nature of the area of law enforcement.

d) The present proposal fulfils these conditions: it ensures that the existing principles of data protection as laid down in Directive 95/46/EC will be applied within the area of the third pillar, since most of the provisions of the proposal mirror other EU legal instruments on the protection of personal data and are consistent with those legal instruments. Moreover, it provides for common standards specifying these principles, in view of their application in this area, that are generally speaking satisfactory to provide adequate data protection safeguards in the third pillar.

Applicable to all processing

e) It is essential for the achievement of its objective that the Framework Decision covers all police and judicial data, even if they are not transmitted or made available by competent authorities of other Member States.

f) Articles 30 (1)(b) and 31 (1)(c) TEU provide for a legal basis for rules on data protection not limited to the protection of personal data that are actually exchanged between the competent authorities of the Member States but also applicable to domestic situations.

g) The proposal does not apply to processing in the framework of the second pillar of the EU-Treaty (common foreign and security policy), nor to processing of data by intelligence services and the access by these services to these data when processed by competent authorities or other parties (this follows from Article 33 TEU). In these areas, national law is to provide adequate protection of data subjects. This gap in the protection on EU level requires an even more effective protection in the areas that indeed are covered by the proposal.

h) The EDPS welcomes the fact that the proposal extends to personal data processed by judicial authorities.

In relation to other legal instruments

i) Whenever any other specific legal instrument under Title VI of the EU Treaty provides for more precise conditions or restrictions for the processing of or access to data, the specific legal instrument should apply as a *lex specialis*.

j) The present proposal for a Council Framework Decision on data protection has its own merits and is needed even in the absence of the adoption of a legal instrument on availability (as proposed by the Commission on 12 October 2005).

k) The approval by the European Parliament of the Directive on the retention of communication data makes it even more urgent to establish a legal framework for data protection in the third pillar.

Structure of the proposal

l) The additional rules in Chapter II (in addition to the general principles of Directive 95/46/EC) should offer additional protection to the data subjects related to the specific context of the third pillar, but may not lead to a lower level of protection.

m) Chapter III on specific forms of processing (in which the third layer of protection is incorporated) may not derogate from Chapter II: the provisions of Chapter III should offer additional protection to the data subjects in situations where competent authorities of more than one Member State are involved, but those provisions may not lead to a lower level of protection

n) The provisions concerning the verification of data quality (Article 9 (1) and (6)) and regulating further processing of personal data (Article 11(1)) should be moved to Chapter II and made applicable to all processing of data by law enforcement authorities, even if personal data have not been transmitted or made available by another Member State. It is, in particular, essential — both in the interest of data subjects and of competent authorities — to ensure that proper verification of the quality concerns all personal data.

Purpose limitation

o) The proposal does not address completely satisfactorily one situation which may occur in police work: the need to further use the data for a purpose considered incompatible with the one they were collected for.

p) Under EU data protection law personal data must be collected for specified and explicit purposes and not further processed in a way incompatible with those purposes. Some flexibility must be allowed as to further use. The limitation on collection is more likely to be well complied with if the authorities in charge of internal security know that they can rely, with appropriate safeguards, on a derogation to the limitation as to further use.

q) The Framework Decision should stipulate in Chapter II that Member States should be allowed to adopt legislative measures to allow further processing when such a measure is necessary to safeguard:

— the prevention of threats to public security, defence or national security;

— the protection of an important economic or financial interest of a Member State.

— the protection of the data subject.

These competences of the Member States could involve a privacy intrusive processing and should thus be accompanied by very strict conditions

Necessity and proportionality

r) The principles of necessity and proportionality of the proposal should fully reflect the case law of the European Court on Human Rights, by ensuring that processing of personal data is considered necessary only where the competent authorities can demonstrate a clear need for it, and provided that less privacy-intrusive measures are not available.

Exchanges of personal data with third countries

s) If data could be transmitted to third countries without the protection of the data subject being assured, this would seriously damage the protection envisaged by the present proposal within the territory of the European Union. The EDPS recommends amending the present proposal so as to ensure that Article 15 applies to the exchange of *all* personal data with third countries. This recommendation does not relate to Article 15 (1)(c)

t) When personal data are transmitted from third countries, their quality should be carefully assessed in the light of the respect of human rights and data protection standards before they are used.

Exchanges of personal data with private parties and non law enforcement authorities.

u) Transfer to private parties and other public bodies can be necessary in specific cases for the purpose of preventing and combating crime, but specific and strict conditions should apply. The EDPS recommends amending the present proposal so as to ensure that Articles 13 and 14 apply to the exchange of *all* personal data, including those not received or made available by another Member State. This recommendation does not relate to Articles 13 (c) and 14 (c).

v) Common standards should apply to access by law enforcement authorities to personal data held by private parties, so as to ensure that access is permitted only on the basis of well defined conditions and limitations.

Special categories of data

w) Specific safeguards should be provided, in particular with a view to guarantee that:

— biometric data and DNA profiles are used only on the basis of well established and interoperable technical standards,

— their level of accuracy is carefully taken into account and might be challenged by the data subject through readily available means, and

— that the respect of the dignity of persons is fully ensured.

The distinction between different categories of data

x) Personal data concerning different categories of people (suspects, convicted persons, victims, witnesses, etc) should be processed according to different, appropriate conditions and safeguards. Therefore, the EDPS proposes adding a new paragraph to Article 4 that contains the following elements:

— the obligation for the Member States to lay down the legal consequences of the distinctions to be made between personal data of different categories of persons.

— additional provisions to restrict the purpose of the processing, to fix precise time limits and to limit the access to data, as far as non suspects are concerned.

Automated individual decisions

y) Decisions based solely on automated processing of data should be subject to very strict conditions when they produce effects concerning a person or significantly affect a person. in this case. Therefore, the EDPS recommends introducing specific provisions on automated individual decisions, similar to those in Directive 95/46/EC.

Selection of other recommendations

z) The EDPS recommends:

— redrafting the first indent of Article 4 (4) so as to ensure the respect of the case law on Article 8 ECHR, since the proposed formulation of Article 4(4) does not meet the criteria laid down by the case law of the European Court of Human Rights relating to Article 8 ECHR.

— deleting the broad derogation of Article 7 (1) or at least explicitly restricting the public interests justifying its use by the Member States.

— modifying Article 10 so as to provide that also access to data is logged or documented.

— deleting letter (a) of paragraph 2 of Articles 19, 20 and 21.

— adding provisions on Data Protection Officers to the proposal. These provisions could be modelled analogous to the Articles 24-26 of Regulation 45/2001/EC.

— amending Article 31 (2) of the proposal so as to also entitle the chairperson of the Article 29-Working Party to participate or be represented in meetings of the new Working Party.

Done at Brussels on 19 December 2005,

Peter HUSTINX

European Data Protection Supervisor