

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

(2007/C 169/02)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ⁽¹⁾,

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

HAS ADOPTED THE FOLLOWING OPINION

I Preliminary remarks

The initiative and the opinion of the EDPS

1. In February 2007, 15 Member States have taken the initiative with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime ⁽³⁾. This initiative deals with matters concerning the processing of personal data. The European Data Protection Supervisor is responsible for advising on this initiative since this falls within the limits of the task entrusted to him, in particular in Article 41 of Regulation (EC) No 45/2001. The EDPS issues this opinion *ex officio*, since no request for advice has been sent to the EDPS ⁽⁴⁾. According to the EDPS, the present opinion should be mentioned in the preamble of the Council Decision ⁽⁵⁾.

⁽¹⁾ OJ L 281, 23.11.1995, p. 31.

⁽²⁾ OJ L 8, 12.1.2001, p. 1.

⁽³⁾ The Member States are mentioned in the title of this opinion. The initiative was published on 28 March 2007 in OJ C 71, p. 35.

⁽⁴⁾ The Commission is under Article 28 (2) of Regulation (EC) No 45/2001 obliged to consult the EDPS when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. In case of an initiative of one or more Member States this obligation does not apply; consultation of the EDPS by these Member States is optional.

⁽⁵⁾ In accordance with the practice of the Commission in other (recent) cases. See, most recently, the Opinion of the EDPS of 12 December 2006 on proposals for amending the Financial Regulation applicable to the general budget of the European Communities and its Implementing Rules (COM(2006) 213 final and SEC(2006) 866 final), published on www.edps.europa.eu.

The background and the content of the present initiative

2. The background of this initiative is unique within the third pillar cooperation. The initiative aims to make the essential parts of the Prüm Treaty, signed on 27 May 2005 by seven Member States ⁽⁶⁾, applicable to all Member States. These essential parts have already been ratified by some of these seven Member States, whilst others of these Member States are in the process of ratification. The substance of these essential parts is therefore clearly not intended to be changed. ⁽⁷⁾
3. According to its recitals, the initiative must be seen as an implementation of the principle of availability that has been presented in the Hague Programme of 2004 as an innovative approach to the cross-border exchange of law enforcement information ⁽⁸⁾. The initiative is presented as an alternative to the proposal for a Council Framework Decision on the exchange of information under the principle of availability on which the EDPS presented his opinion on 28 February 2006 ⁽⁹⁾, which was not debated in Council with the view to its adoption.
4. The initiative takes a fundamentally different approach than the above mentioned proposal for a Council Framework Decision. Where this proposal foresees direct access to available information, the initiative aims at indirect access through reference data. The initiative moreover requires from the Member States to collect and store certain information, even if it is not yet available in the national jurisdiction.
5. An important focus in the initiative is on the exchange of biometric information between police and judicial authorities of the Member States, in particular data from DNA analysis files and automated dactyloscopic information systems (systems containing fingerprints ⁽¹⁰⁾).
6. The initiative incorporates a chapter 6 entitled 'General provisions on data protection'. This chapter contains a number of data protection arrangements, which are tailored to the specific nature of the data exchange it regulates ⁽¹¹⁾. Chapter 6 also refers to the Council of Europe Convention No 108 ⁽¹²⁾ and related documents of the Council of Europe as a general framework for data protection, in the absence of the adoption of a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. ⁽¹³⁾

II Focus of the opinion of the EDPS

7. This opinion will take into account the unique nature of the initiative, more specifically the fact that major amendments in the substance of the provisions are not foreseen. The EDPS will therefore focus on a number of more general issues related to the initiative and its context. The amendments the EDPS proposes mainly serve to improve the text without modifying the system of information exchange itself.
8. The first issue is of a procedural nature. The initiative implies that a small number of Member States fix the policy choices of all the Member States, in an area which is covered by provisions of the EU-Treaty, particularly Title VI of the EU-Treaty (the third pillar). The procedures of Title VI for enhanced cooperation have not been followed.
9. The second issue relates to the principle of availability. Although the initiative must be seen as an implementation of this principle, it does not lead to availability as such but it is only one further step towards availability of law enforcement information across the borders of the Member States. It is part of a piecemeal approach aiming to facilitate the exchange of law enforcement information.

⁽⁶⁾ Treaty of 27 May 2005 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 immigration.

⁽⁷⁾ See point 15 below.

⁽⁸⁾ The Hague Programme for strengthening freedom, security and justice in the European Union, approved by the European Council on 5 November 2004.

⁽⁹⁾ COM (2005) 490 final. EDPS opinion is published in OJ [2006], C 116, p. 8.

⁽¹⁰⁾ This opinion will use the more common term 'fingerprints' instead of 'dactyloscopic data', the term used in the initiative.

⁽¹¹⁾ See recital 17 of the initiative.

⁽¹²⁾ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981.

⁽¹³⁾ See further Par. VII of this opinion.

10. The third issue can be circumscribed as the issue of proportionality. It is difficult to assess whether the provisions of the initiative for a Council Decision are justified by the need to combat terrorism and cross-border crime. The EDPS recalls that the Prüm Convention has been set up as a 'laboratory' for cross border exchange of information, in particular DNA analysis files and fingerprints. However, the present initiative is presented before the experiments with the exchange have been effectively put in practice ⁽¹⁴⁾.
11. The fourth issue has to do with the use of biometric data. The initiative requires collection, storage and (limited) exchange of DNA analysis files and fingerprints. The use of these biometric data in law enforcement presents specific risks for the data subjects and requires extra safeguards, in order to protect their rights.
12. The fifth issue follows from the fact that the Council Decision should build on an appropriate general framework for data protection in the third pillar, which is not yet in place on EU-level. In this opinion, the EDPS will illustrate the importance of such a general framework as a *condicio sine qua non* for the exchange of personal data by law enforcement authorities based on the present initiative.

III The procedure and the legal basis

13. The Prüm-Treaty is often compared with the 1985 Schengen Agreement and the 1990 Schengen Convention, for obvious reasons. Much the same countries are involved, the subject-matter is similar, and there is a close link with cooperation within the EU ⁽¹⁵⁾. However, there is a fundamental difference with Schengen. Presently, there is a European legal framework which enables the European Union to regulate the matters concerned and there were actual plans to make use of it for the (main) matters covered by the Prüm-Treaty. More in particular, at the time of concluding the Prüm Treaty, the Commission was preparing a proposal for a Council Framework Decision. ⁽¹⁶⁾
14. The Member States concerned opted nevertheless for a multilateral treaty enabling them to sidestep the thorny path of third pillar legislation by unanimous agreement. They also evaded the substantive and procedural requirements of enhanced cooperation, included in Articles 40, 40A, 43 and 43A of the EU-Treaty ⁽¹⁷⁾. This is all the more important since the procedure on enhanced cooperation was compulsory, if at least eight Member States were participating. However, only seven Member States signed the Prüm-Treaty, but they subsequently encouraged other Member States to join. One could argue that the Prüm Convention breaches the law of the European Union, for the reasons mentioned above. However, this argument is mainly of a theoretical nature, in the framework of the third pillar with limited powers of the Commission to ensure compliance with the law of the European Union by the Member States and limited competences of the European Court of Justice, as well as of other Courts.
15. In the present situation, 15 Member States took the initiative aiming to replace the Prüm Treaty by a Council Decision. Although the possibility of a change in substance of the provisions is not formally excluded and can not be formally excluded, it is clearly the goal of the Members States that presented the initiative not to allow any substantial changes. This goal follows from the fact that the seven 'Prüm-countries' just implemented the Prüm Treaty in national law (or are in advanced stage of its implementation) and do not wish to change their national provisions again. The goal is illustrated by the way the German Presidency of the Council proceeds. For instance, the time schedule for adoption is very tight and the initiative will not be examined in a Council Working Group, but only in the Article 36-Committee (the Coordinating Committee of senior officials based on Article 36 TEU).
16. As a result, the other Member States are denied a real say in the choice of rules. They can only choose between participating and not participating. Since the third pillar requires unanimity, if one Member State disapproves of the text, the result may be that the other Member States proceed on the basis of the procedure of enhanced cooperation.

⁽¹⁴⁾ Apart from a first experience with exchange of information between Germany and Austria, mentioned under point 33.

⁽¹⁵⁾ In the times of Schengen, the cooperation within the European Economic Community. The Prüm-Treaty is often referred to as Schengen III.

⁽¹⁶⁾ The proposal (mentioned in point 3) was adopted by the Commission after the Prüm Treaty was adopted.

⁽¹⁷⁾ These articles *inter alia* require involvement of the Commission and the European Parliament and must guarantee that enhanced cooperation is only used as a last resort.

17. This background also affects the democratic legitimacy of the initiative, since the opinion of the European Parliament under Article 39 TEU can hardly have any consequence for the choices of rules. Equally, this opinion can have only limited effect.
18. According to the EDPS, it is unfortunate that this procedure has been followed. It denies all need for a democratic and transparent legislative process since it does not even respect the already very limited prerogatives under the third pillar. At this stage, the EDPS recognises the fact that this procedure has been chosen and this opinion will therefore further concentrate mainly on the substance of the initiative.
19. Finally, the EDPS has noted the fact that the initiative foresees the instrument of a Council Decision and not a Council Framework Decision, although the initiative relates to the purpose of approximation of the laws and regulations of the Member States. This choice of instrument could be related to the possibility of taking implementing measures by qualified majority, in case of Council Decisions under Article 34 (2) (c) TEU. Article 34 of the initiative deals with these implementing measures.
20. The EDPS recommends adding a sentence to Article 34 of the initiative for a Council Decision, which reads as follows: 'The Council shall consult the EDPS before the adoption of such an implementing measure.' The reason for this amendment is obvious. Implementing measures will most often affect the processing of personal data. Moreover, if the Commission does not take the initiative for such measures, Article 28 (2) of Regulation (EC) No 45/2001 does not apply.
21. In this context, it should be noted that the seven Member States that signed the Prüm Treaty also concluded on 5 December 2006 an Implementing agreement containing the necessary provisions for the administrative and technical implementation and application of the Treaty. ⁽¹⁸⁾ One can assume that this implementing agreement will be the model for the implementing measures under Article 34 of the initiative for a Council Decision. This opinion will refer to this implementing agreement in so far as this could contribute to a better understanding of the initiative itself.

IV The initiative and the principle of availability

22. The principle of availability can be seen as an important means for the realisation of an area of freedom, security and justice without internal borders. Free sharing of information between law enforcement authorities is an important step in tackling territorial restrictions in combating crime, as a result of internal borders remaining in place for investigations.
23. According to the Hague Programme, the principle means 'that, throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, (...)'. The Programme furthermore emphasises that the 'methods of exchange of information should make full use of new technology and must be adapted to each type of information, where appropriate, through reciprocal access to or interoperability of national databases, or direct (on-line) access'.
24. Against this background, the initiative only takes a small step. Its ambitions are much smaller than those of the Commission Proposal for a Council Framework Decision on the exchange of information under the principle of availability. The initiative can be qualified as a step towards availability, but does not *stricto sensu* implement the principle of availability. It complements other measures aiming to facilitate the exchange of law enforcement information, such as the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union ⁽¹⁹⁾ that must ensure that information and intelligence will be provided to authorities of other Member States, on request.

⁽¹⁸⁾ This agreement can be found in Council document 5437/07 of 22 January 2007. See: <http://www.statewatch.org/news/2007/jan/prum-implementing-agreement.pdf>

⁽¹⁹⁾ OJ L 386, p. 89. This Framework Decision is adopted on Swedish initiative.

25. In his opinion on this Commission Proposal, the EDPS advocated that the principle of availability should be implemented by way of a more cautious, gradual approach. In such an approach the types of data exchanged under the principle of availability should be limited and only indirect access, via index data, should be allowed. ⁽²⁰⁾ Such a gradual approach enables stakeholders to monitor the effectiveness of the exchange of information for law enforcement, as well as the consequences for the protection of the personal data of the citizen.
26. These observations remain valid in the present situation. The EDPS welcomes that the present initiative takes this more cautious, gradual approach as a way of implementing the principle of availability.
27. The Articles 5 and Article 10 of the initiative can be seen as an illustration of this approach. They deal with the supply of further personal data (and other information) following a match between DNA-profiles, respectively fingerprints. Both cases shall be governed by the national law of the requested Member State, including the legal assistance rules. The legal effect of those two articles is limited. They are a rule of conflict of law (of a declaratory nature; not changing the present situation), but they do not implement the principle of availability. ⁽²¹⁾

V Necessity and proportionality

28. An effective exchange of law enforcement information is a key issue in police and judicial cooperation. It is essential to the development of an area of freedom, security and justice without internal borders that information is available across the national borders. An appropriate legal framework is needed to facilitate the exchange.
29. It is a different issue to determine whether the provisions of the present initiative are justified by the need to combat terrorism and cross-border crime or, in other words, whether they are necessary and proportionate.
30. Firstly, on the level of the European Union, a number of measures have been adopted in order to facilitate the exchange of law enforcement information. In some cases, these measures include the establishment of a centralised organisation, like Europol or Eurojust, or a centralised information system, like the Schengen Information System. Other measures deal with the direct exchange between the Member States, like the present initiative. Only recently, Council Framework Decision 2006/960/JHA has been adopted as an instrument aiming to simplify the exchange of law enforcement information.
31. In general, new legal instruments on police and judicial cooperation should only be adopted after an evaluation of the already existing legislative measures, leading to the conclusion that those existing measures are not sufficient. The recitals of the present initiative do not give evidence of a full evaluation of the existing measures. They mention Council Framework Decision 2006/960/JHA and indicate that full use should be made of new technology and that reciprocal access to national data bases should be facilitated. Precise information should be exchanged swiftly and efficiently. This is all. There is for instance no reference to the information exchange between the Member States via the Schengen Information System, which is an essential instrument for the exchange of information between the Member States.
32. The EDPS regrets the fact that the present initiative is issued without a proper evaluation of the existing measures on the exchange of law enforcement information and calls on the Council to include such an evaluation in the procedure of adoption.
33. Secondly, as said before the Prüm Convention has been set up as a 'laboratory' for cross border exchange of information, in particular DNA and fingerprints. It enabled the Member States concerned to experiment with this exchange. At the date of issuing the presented initiative for a Council Decision the experiments have not effectively been put in practice on a wider scale, apart from a first exchange between Germany and Austria ⁽²²⁾.

⁽²⁰⁾ Opinion of the EDPS of 28 February 2006 OJ C 116, 17.5.2006, p. 8, point 69.

⁽²¹⁾ The EDPS welcomes the gradual approach in general (point 26). However, as will be shown in point 37, in this specific case a minimum harmonisation of essential elements of collection and exchange of different kinds of data would be preferable.

⁽²²⁾ The results of the automated comparison of DNA profiles in the German and Austrian DNA databases have been presented to the Informal Meeting of JHA Ministers in Dresden (14-16 January 2007) and are published on the website of the German Presidency (www.bmi.bund.de). They roughly cover November and December 2006. The results of this first exchange mention an impressive number of more than 2000 hits in two months, in some cases clearly related to serious crime.

34. The EDPS is not convinced that the first results of this limited exchange — for a short period and only with two Member States involved, however interesting they may be — can be used as giving sufficient empirical basis for making the system applicable to all the Member States.
35. It makes a difference of scale whether one establishes a system of information exchange between a few Member States, that already have experience with DNA-databases, or if one establishes an EU-wide system, including Member States that have no experience at all. Moreover, the small scale allows close contacts between the Member States involved; those contacts could also be used to monitor the risks for the protection of the personal data of the persons concerned. Furthermore, the small scale is much easier to supervise. So, even if the Prüm Convention itself would be necessary and proportionate, this does by itself not mean that the present initiative should be evaluated in the same sense.
36. Thirdly, as will be demonstrated further on in this opinion, there are big differences in the national laws of the Member States, relating to the collection and use of biometric data for law enforcement purposes. Also, national practices are not harmonised. In this context, it also should be noted that a harmonised legal framework for data protection in the third pillar has not yet been adopted.
37. The initiative does not harmonise essential elements of the collection and exchange of the different kinds of data included in the initiative. For instance, the initiative is not precise on the purposes of collection and exchange. Do the provisions on DNA profiles apply to all crimes or can a Member State limit their application to more serious crime? The initiative is not clear either on the circle of data subjects affected by the collection and exchange. Do the databases only contain (biometric) material of suspects and/or convicted persons, or also material of other data subjects, such as witnesses or other persons that happened to be in the neighbourhood of a crime? According to the EDPS, a minimum harmonisation of these essential elements would have been preferable, also to ensure compliance with the principles of necessity and proportionality.
38. The EDPS concludes as follows. There are clear indications that the present initiative is likely to be a useful instrument for police cooperation. This indication is even stronger in the light of the first experiences with the Prüm Treaty in Germany and Austria. However, an examination of the necessity and the proportionality of the present initiative is not easily done. The EDPS regrets the fact that the present initiative is taken without a proper impact assessment taking into account the observations made in this part of the opinion. He calls on the Council to include such an assessment in the procedure of adoption and to examine as part of this assessment other — possibly less privacy-intrusive — policy options ⁽²³⁾.
39. The EDPS equally proposes to include an evaluation clause in Chapter 7 of the initiative ('Implementing and final provisions'). Such an evaluation clause could read as follows: 'The Commission shall submit to the European Parliament and the Council an evaluation of the application of this Council Decision with a view to determining whether it is necessary to amend the provisions of this Council Decision, no longer than three years after the Council Decision has taken effect'.
40. Such an evaluation clause is a specially useful instrument in the present context where the necessity and the proportionality of the present initiative are not (yet) clearly established and where an EU-wide system for information exchange is introduced, based on limited experiences.

VI Different kinds of data: DNA profiles, fingerprints and vehicle registration data

General observations

41. Chapter 2, on line access and follow up requests, distinguishes three types of data: DNA profiles, fingerprints and vehicle registration data. This distinction leads to two general observations.
42. In the first place, it has to be noted that all data processed within the framework of the Council Decision, except the data meant in Article 13 ⁽²⁴⁾, are personal data in the sense of Directive 95/46/EC ⁽²⁵⁾ and other instruments of community law. According to Article 2 (a) of the directive 'personal data' shall mean any information relating to an identified or identifiable natural person; an identifiable

⁽²³⁾ A 'privacy impact assessment'.

⁽²⁴⁾ And perhaps also the unidentified DNA-profiles mentioned in Article 2 (2) of the initiative.

⁽²⁵⁾ 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, OJ L 281, p. 31.

person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. 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, that — once adopted — would be applicable to the exchange of information under the present initiative, uses the same definition. The EDPS regrets the fact that the initiative does not give a definition of personal data and suggests, for reasons of legal clarity, including such a definition in Article 24.

43. In any event, under the definition mentioned in the preceding point, it is beyond doubt that also databases containing only DNA profiles and reference data from DNA analysis files and from fingerprint identification systems are wholly or predominantly considered to be collections with personal data.
44. In the second place, the purpose of the data exchange is different for the three types of personal data: DNA profiles, fingerprints and vehicle registration data. As to DNA, Member States shall open and keep national DNA analysis files for the investigation of criminal offences (Article 2 (1)), as to fingerprints they shall ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offences (Article 8) and in the case of vehicle registration data, the exchange encompasses not only the prevention and investigation of criminal offences, but also certain other — not criminal — offences, as well as the purpose of maintaining public order and security (Article 12 (1)).
45. Equally, the exchange of and access to DNA and fingerprint data is subject to more stringent guarantees than the exchange of and access to vehicle registration data. As to DNA and fingerprint data, the access is initially limited to reference data from which the data subject can not be directly identified. The initiative states the principle of the separation in two different databases between the biometric data on one side and the textual identification data on the other side. The access to the second database is only possible if a 'hit' happened in the first one. Such separation between databases does not exist for vehicle registration data, where an automatic and direct access is provided, and no double database is required.
46. The EDPS supports this gradation and considers it to be a useful instrument for the protection of the data subject: the more sensitive the data, the more limited the purposes for which they can be used and the more limited the access. In the specific case of DNA, potentially the most sensitive of the personal data covered by the initiative, the data can only be exchanged for reasons of criminal prosecution and not for pre-emptive policing. Moreover, profiles can only be taken from the non-coding part of the DNA.

Specific observations on DNA data

47. As to DNA data, reference can be made to earlier EDPS-opinions ⁽²⁶⁾. It is essential that the concept of DNA data is clearly defined and that a difference is made between DNA profiles and DNA data that can provide information on genetic characteristics and/or the health status of a person. Also progress in science has to be taken into account: what is considered as an innocent DNA profile at a certain moment in time, may at a later stage reveal much more information than expected and needed.
48. The initiative limits the availability to DNA profiles established from the non-coding part of DNA. However, precise definitions of DNA-profiles, as well as a procedure to establish such common definitions, pursuant to the state of the art in science, are missing in the text of the initiative. The implementing agreement of the Prüm-Treaty ⁽²⁷⁾ defines the non-coding part as follows: chromosome zones containing no genetic expression, i.e. not known to provide information about specific hereditary characteristics. The EDPS suggests including a definition of non-coding part in the initiative itself, as well as providing for a procedure ensuring that indeed — both now and later — no more information can be revealed from the non-coding part.

⁽²⁶⁾ See for instance the EDPS-Opinion on the principle of availability cited in footnote 9, points 59-60.

⁽²⁷⁾ See footnote 18.

49. The initiative relies on the presupposition that matching DNA profiles is the key instrument in police cooperation. For this reason, all Member States have to establish DNA databases for the purposes of criminal justice. Taking into account the costs of these databases and the risks from the perspective of data protection, a thorough *ex ante* assessment is needed of the effectiveness of this instrument. The limited experience in the exchange of DNA data between Germany and Austria does not suffice.
50. The EDPS notes in this perspective that the initiative obliges all Member States to establish national DNA analysis files. It is important to underline that several Member States already have well established national DNA databases, whilst other Member States have less or no experience in this area. The most developed database in Europe (and in the world) is the DNA database in the United Kingdom. It amounts to more than 3 millions entries, making it the most extensive collection of DNA profiles. The database extends to those persons who have been convicted of offences, as well as to those who have been arrested and to those who have volunteered samples for elimination purposes ⁽²⁸⁾. The situation is different in other countries. For instance, in Germany profiles are only held for those who have been convicted of serious offences. One could even assume that in Germany the collection of DNA for wider purposes would not be compatible with the case law of the Constitutional Court. ⁽²⁹⁾
51. The EDPS regrets the fact that the initiative does not specify the categories of persons that will be included in the DNA databases. Such a specification would not only harmonise the national provisions in this area — which could contribute to the effectiveness of the cross-border cooperation — but could also enhance the proportionality of the collection and exchange of these personal data, provided that the categories of persons would be limited.
52. A related issue that is left to the national law of the Member States is the period of retention of data in the DNA analysis files. National law can provide that the profiles which are created in those files are retained for the lifetime of the data subject, whatever is the outcome of a judicial procedure, whereas it could also provide that the profiles are kept, unless the person has not been charged and is therefore not condemned by a court, or that the need for continued storage is reviewed on a regular basis. ⁽³⁰⁾
53. Finally, the EDPS points at Article 7, on the collection of cellular matters and supply of DNA profiles. A similar provision is not foreseen for fingerprints. The provision obliges a Member State, on the request of another Member State and in the context of ongoing investigations or criminal proceedings, to collect and examine cellular material of an individual and subsequently supplying the DNA profile to that other Member State, under conditions. This article is quite far going. It obliges a Member State to actively collect (and examine) biometric material of an individual, provided that such collection and examination would be allowed in the requesting Member State (condition b).
54. The provision is not only far going, but also undetermined. On the one hand there is no limitation to more serious crime and not even to suspects of a crime, on the other hand the requirements of the law of the requested Member State must be fulfilled (condition c) without an indication of what these requirements can be about. According to the EDPS, a further clarification of this article is needed, preferable by specifying the text of the article. In any event, the principle of proportionality requires a more limited interpretation of this article.

VII The data protection framework

55. This part of the opinion will discuss the following issues, relating to data protection:
- The need for a general framework for data protection in the third pillar.
 - Illustrations why the general framework is needed, despite the provisions of chapter 6 of the initiative.
 - A short examination of Chapter 6 itself.

⁽²⁸⁾ See the evidence submitted by the UK Information Commissioner to the House of Lords Select Committee on the European Union Sub Committee F (Home Affairs) Inquiry into the Prüm Convention (pt. 10 of the Evidence). With elimination purposes is meant the elimination of persons from groups of suspects of crimes.

⁽²⁹⁾ See, for instance, Judgment of 14 December 2000, BvR 1741/99, in which the use of DNA samples for less serious offences was not considered to be compatible with the principle of proportionality.

⁽³⁰⁾ See, on this alternative, Article 20 (1) of the proposal for a Council Decision establishing the European Police Office (EUROPOL), (COM(2006) 817 final) and the EDPS Opinion of 16 February 2007 (point 26).

56. As a preliminary point, the EDPS notes that Article 1 of the initiative that describes the aim and scope does not contain a reference to Chapter 6, although the Council Decisions contains a chapter on data protection. The EDPS therefore recommends adding such a reference to the text.

The need for a general framework

57. As stated on several other occasions ⁽³¹⁾, it is essential to the EDPS that specific legal instruments facilitating the exchange of law enforcement information — like the present initiative for a Council Decision — are not adopted before the adoption by Council of a framework on data protection, guaranteeing an appropriate level of data protection in conformity with the conclusions of the EDPS in his two opinions on the Commission proposal for a Council Framework Decision on data protection in the third pillar. ⁽³²⁾
58. A legal framework for data protection is a *condicio sine qua non* for the exchange of personal data by law enforcement authorities, as is required by Article 30 (1) (b) of the EU Treaty, and recognised in several EU policy documents. However, in practice legislation facilitating exchange of data is adopted before an adequate level of data protection is guaranteed. This order should be reversed.
59. Reversal of the order is also important because the more detailed rules on data protection in the present initiative may conflict with the future common framework decision for data protection in the third pillar which is still under discussion. It is also not efficient to start the implementation of the data protection provisions of this initiative — which includes the adoption of standards for data protection and administrative procedures, as well as the designation of competent authorities — before the adoption of a Framework Decision on data protection that might contain different requirements and would thus require changes of the just adopted national provisions.
60. Article 25 (1) of the present initiative now refers to Council of Europe Convention 108, its Additional Protocol of 8 November 2001 and Recommendation No R (87) 15 on the use of personal data in the police sector. Those instruments adopted by the Council of Europe should provide for a minimum level of protection of personal data. However, as the EDPS stated before ⁽³³⁾, the Convention by which all the Member States are bound does not provide for the necessary preciseness as has been recognised already at the time of the adoption of Directive 95/46/EC. The Recommendation is by its nature not binding.

Illustrations of the need for a general framework, in spite of Chapter 6

61. Firstly, the provisions of Chapter 6 of the initiative are intended to build on a general framework for data protection (see Article 25 of the initiative). The provisions must be seen as a *lex specialis* applicable to the data supplied pursuant to this Council Decision. Unfortunately, the present general framework of Council of Europe Convention 108 and related documents is unsatisfactory. However, the intention in itself illustrates that an appropriate general framework laid down in a Council Framework Decision is needed. But this is not the only illustration of the need for such a framework.
62. Secondly, the initiative covers only a part of the processing of personal data for law enforcement purposes and of the exchange of such data between the Member States. Chapter 6 of the initiative is by its nature limited to processing related to the exchange of information foreseen by the initiative. All other exchange of other police and judicial information within the scope of the initiative, notably information not related to DNA profiles, fingerprints and vehicle registration data, is thus excluded. Another example of the partial coverage of Chapter 6 of the initiative relates to access for law enforcement purposes to data collected by private companies, since the initiative aims at the exchange of information between agencies responsible for the prevention and investigation of criminal offences (Article 1 of the initiative).

⁽³¹⁾ See most recently, the EDPS-Opinion of 16 February 2007 on the proposal for a Council Decision establishing the European Police Office (EUROPOL).

⁽³²⁾ Opinions of the EDPS of 19 December 2005 (OJ [2006] C 47, p. 27) and of 29 November 2006, published on the EDPS-website.

⁽³³⁾ See, for instance, the (first) opinion on the Commission proposal for a Council Framework Decision on data protection in the third pillar, point 4.

63. Thirdly, as to the field of application of the provisions of Chapter 6, the text of the initiative is ambiguous and therefore lacks legal clarity. According to Article 24 (2) of the initiative, these provisions apply to data that are or have been supplied pursuant to this Council Decision. According to the EDPS, this wording ensures that the direct access to DNA profiles, fingerprints and vehicle registration data is covered, as well as the specific situation under Article 7 of the initiative ⁽³⁴⁾. Furthermore, it is beyond doubt that also the supply of personal data under Article 14 (major events) and Article 16 (to prevent terrorist offences) is covered.
64. However, it is not clear whether Chapter 6 only applies to personal data that are or have been exchanged between the Member States or that it also applies to the collection and processing of DNA material and fingerprints in a Member State pursuant to Articles 2 and 8 of the initiative. In other words, does Chapter 6 apply to personal data that have been collected under the Council Decision, but not (yet) supplied to authorities in other Member States? It is moreover unclear whether the supply of further personal data following a match between DNA-profiles or fingerprints is covered since on the one hand Recital 11 implies that the supply of further information (through mutual assistance procedures) falls within the scope of the Council Decision, whereas on the other hand the Articles 5 and 10 emphasise that such supply is governed by national law. Finally, it has to be noted that Article 24 (2) contains an exception to the applicability of Chapter 6. The provisions shall apply 'save as otherwise provided in the preceding Chapters'. According on the EDPS, this proviso is without substantial value — the EDPS did not notice any contradictory provisions in the preceding chapters —, but the proviso might nevertheless enhance the ambiguity of the text as to the applicability of Chapter 6.
65. The EDPS recommends that Article 24 (2) specifies that Chapter 6 applies to the collection and processing of DNA material and fingerprints in a Member State and that also the supply of further personal data within the scope of this decision is covered. Moreover, the proviso 'save as otherwise provided in the preceding Chapters' should be deleted. Those clarifications would ensure that the provisions of Chapter 6 have substantial consequences.
66. Fourthly, the nature of the provisions on data protection in Chapter 6 themselves, as far as they build on the traditional notion of mutual legal assistance in criminal matters, are an illustration of the need for a general framework. Information sharing presupposes a minimum-harmonisation of basic rules on data protection or at least the mutual recognition of national law, so as to avoid that the effectiveness of cooperation is harmed by differences between the laws of the Member States.
67. Although the initiative provides for harmonisation on some important matters of data protection law, on other important matters, the provisions on data protection in Chapter 6 do not harmonise national law nor do they prescribe mutual recognition. Instead, they build on the simultaneous applicability of two (or more) legal systems: supply of data is quite often only allowed if the laws of both the supplying Member State and the receiving Member State are observed. In other words, on those matters the initiative does not contribute to an area of freedom, security and justice without internal borders, but they give substance to the traditional system of mutual legal assistance in criminal matters, based on national sovereignty. ⁽³⁵⁾
68. According to the EDPS, this nature of Chapter 6 does not facilitate the exchange of personal data but enhances the complexity, taking into account that the initiative aims to make the system of the Prüm Treaty applicable to all 27 Member States and since a general common framework for data protection has not been adopted. For example, Article 26 (1) allows processing for other purposes only if this is permitted under the national law of both the supplying and the receiving Member State. Another example is Article 28 (3) that states that personal data that should not have been supplied (or received) shall be deleted. But how does the receiving Member State know that these data had not been lawfully supplied under the law of the supplying Member State? This could lead to difficult questions when these issues arise in cases before national courts.

⁽³⁴⁾ See point 53 of this opinion.

⁽³⁵⁾ See also Recital 11 of the initiative that stipulates that Member States 'request further information through mutual assistance procedures'.

69. Fifthly, this common framework for data protection is all the more important since there are big differences between the laws of the Member States, both in substantive criminal law as in law on judicial procedure in criminal matters. Apart from the consequences for the cooperation between the authorities of the Member States, these differences also directly affect the data subjects in cases where data concerning them are exchanged between authorities in two or more Member States. For instance, their effective means of redress before a court may not be the same in all Member States.
70. To conclude, the proposal harmonizes some elements of the exchange of data between competent authorities and includes for this reason a chapter on data protection, but it is far from harmonizing all data protection guarantees. The provisions are neither comprehensive (like a general framework, *lex generalis*, should be) nor complete (since important elements are missing, as will be demonstrated in point 75).
71. It is obvious that outside the scope of the initiative, a general common framework for data protection is needed. The citizen is entitled to rely on a minimum harmonised level of data protection, no matter where in the European Union data concerning him are being processed for law enforcement purposes.
72. But also within the scope of the initiative, such a common framework is needed. The initiative deals *inter alia* with collection, processing and exchange of potentially sensitive biometric data like DNA material. Moreover, the circle of data subjects that can be included in this system is not limited to data of persons suspected (or convicted) of specific crimes. Under those circumstances, one should even more rely on a clear and adequate system of data protection.
73. In this context, it has to be repeated that the scope of the initiative and of its Chapter 6 is not clearly defined. This makes it important for reasons of legal security that personal data are well protected, irrespective of the question whether or not and in what situations they fall within the scope. For the same reasons, consistency between the applicable rules within and outside the scope of the initiative should be guaranteed.

The provisions of Chapter 6

74. The provisions on data protection in Chapter 6 of the present initiative apply to data which are or have been supplied pursuant to the decision. They deal with a number of important issues and have been carefully drafted, as specific provisions on top of a general framework for data protection. The EDPS concludes that in general terms the provisions offer in substance an appropriate protection.
75. However, in addition to what has been said before on the nature of the provisions of Chapter 6, the EDPS has identified some other shortcomings in the provisions of Chapter 6 ⁽³⁶⁾:
- Article 30 on logging is only applicable to the exchange of personal data, not to the access to those data for law enforcement purposes. It would have been better to draft the article in such a way that it ensures that all activities in respect of those data must be logged.
 - Article 31 limits the right to information of the data subject to a right to be informed upon request. This requirement is contrary to an essential element of data protection, namely that the data controller provides a data subject from whom data relating to himself are collected with some basic information on this collection, without being requested to do so by that data subject ⁽³⁷⁾. Indeed, the data subject will in many cases not know about the collection of his data. Of course the exercise of the right to information may be subject to exceptions, conditions or limitations, for instance to protect the interest of an ongoing criminal investigation, but that may not result in the right itself being deprived of its substantive content, by requiring as a general rule a request from the data subject. ⁽³⁸⁾

⁽³⁶⁾ This point does not contain a limitative list of shortcomings; it only mentions most important ones from the perspective of data protection.

⁽³⁷⁾ See for instance Article 10 of Directive 95/46/EC (reference in footnote 25).

⁽³⁸⁾ The EDPS notes that Article 31 refers to Directive 95/46/EC, whereas in a third pillar instrument a reference to a legal instrument applicable in this area would have been more logical, in casu the Protocol to Council of Europe Convention 108.

- Chapter 6 does not foresee a separation of data relating to different categories of people (victims, suspects, other people whose data are included in a data base). Such a separation of categories of people according to their degree of involvement in a crime was included in the Commission proposal for a Council Framework Decision on data protection in the third pillar and is even more important in the context of the present initiative, since this allows the processing of — in some cases sensitive — personal data of persons who are not directly involved in a crime.
 - One comment has already been made: a definition of personal data is missing ⁽³⁹⁾.
76. The EDPS recommends the Council to deal with these shortcomings, either by amending the text of the initiative and/or by including these elements in a Council Framework Decision on data protection in the third pillar. In the view of the EDPS, the first option does not necessarily lead to a modification of the system of information exchange itself and does not contradict the intention of the 15 Member States that took the initiative not to change the essential parts of the Prüm Treaty.

VIII Conclusions

77. This opinion takes into account the unique nature of the initiative, more specifically the fact that major amendments in the substance of the provisions are not foreseen. The amendments the EDPS proposes mainly serve to improve the text without modifying the system of information exchange itself.
78. The EDPS welcomes that the present initiative takes a more cautious, gradual approach as a way of implementing the principle of availability. However, he regrets that the initiative does not harmonise essential elements of the collection and exchange of the different kinds of data, also to ensure compliance with the principles of necessity and proportionality.
79. The EDPS regrets the fact that the present initiative is taken without a proper impact assessment and calls on the Council to include such an assessment in the procedure of adoption and to examine as part of this assessment other — possibly less privacy-intrusive — policy options.
80. The EDPS supports the approach of the initiative relating to the different kinds of personal data: the more sensitive the data, the more limited the purposes for which they can be used and the more limited the access.
81. The EDPS regrets the fact that the initiative does not specify the categories of persons that will be included in the DNA data bases and that it does not limit the retention period.
82. The Council Decision should not be adopted by Council before the adoption of a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, offering an appropriate level of protection.
83. The provisions on data protection in Chapter 6 of the initiative do not facilitate the exchange of personal data but enhance the complexity of this exchange, as far as they build on the traditional notion of mutual legal assistance in criminal matters.
84. The EDPS recommends the following amendments of the text of the initiative:
- including in Article 1 a reference to Chapter 6 on data protection.
 - including a definition of non-coding part of DNA, as well as providing for a procedure ensuring that — both now and later — no more information can be revealed from the non-coding part.
 - specifying the text of article 7, taking into account that the principle of proportionality requires a more limited interpretation of this article.

⁽³⁹⁾ See point 42 above.

- including a definition of personal data in Article 24.
 - specifying in Article 24 (2) that Chapter 6 applies to the collection and processing of DNA material and fingerprints in a Member State and that also the supply of further personal data within the scope of this decision is covered.
 - deleting in Article 24 (2) the proviso ‘save as otherwise provided in the preceding Chapters’.
 - modifying Article 30 on logging in a way that it ensures that all activities in respect of those data must be logged.
 - modifying Article 31 so as to guarantee the right to information of the data subject, without requiring a request.
 - including in Chapter 6 a separation of data relating to different categories of people (victims, suspects, other people whose data are included in a data base).
 - adding a sentence to Article 34 of the initiative for a Council Decision, which reads as follows: ‘The Council shall consult the EDPS before the adoption of such an implementing measure.’.
 - including an evaluation clause in Chapter 7 of the initiative.
85. More in general, the EDPS recommends the Council to deal with the shortcomings of the initiative, either by amending the text of the initiative and/or by including these elements in a Council Framework Decision on data protection in the third pillar. In the view of the EDPS, the first option (relating to the elements mentioned in the preceding point) does not necessarily lead to a modification of the system of information exchange itself and does not contradict the intention of the 15 Member States that took the initiative not to change the essential parts of the Prüm Treaty.
86. Finally, the present opinion should be mentioned in the preamble of the Council Decision.

Done in Brussels, 4 April 2007.

Peter HUSTINX
European Data Protection Supervisor
