I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes

(2010/C 92/01)

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,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 15 September 2009 from the European Commission,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 10 September 2009, the Commission adopted two proposals, namely the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) [3], and the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes [4]. The proposals were sent by the Commission to the EDPS for consultation and received on 15 September 2009, in accordance with Article 28(2) of Regulation (EC) No 45/2001 (hereinafter 'the proposals' or 'the proposed Regulation' and 'the proposed Decision'). The EDPS has also received the Impact Assessment.

2. The EDPS welcomes that he is consulted and recommends that reference to this consultation be made in the recitals of the proposal, in a similar way as in a number of other legislative texts on which the EDPS has been consulted, in accordance with Regulation (EC) No 45/2001.

3. The EDPS has a specific interest in these proposals also in view of the supervisory powers he exercises over the Central Unit of the Eurodac database, and the coordinated supervision he must ensure on the Eurodac system as a whole together with the national data protection authorities.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2009) 342 final.
[4] COM(2009) 344 final.

4. The question of giving access to large-scale IT systems for law enforcement has already been addressed by the EDPS in the context of the access to the Visa Information System by law enforcement authorities and Europol ([5]). The subject matter of the proposals is also closely related to the general recast of the Eurodac and Dublin Regulations on which the EDPS has issued two opinions on 18 February 2009 ([6]).

II. CONTENT AND BACKGROUND OF THE PROPOSALS

5. The proposals establish the basis for the right of designated authorities of Member States as well as Europol to request a comparison of fingerprint data or a latent copy with the Eurodac data. A successful comparison which results in a 'hit' reply from Eurodac will be accompanied by all data that is held in Eurodac regarding the fingerprint. Requests for supplementary information following a hit are not regulated in the proposals but are covered by existing instruments on the exchange of law enforcement information. The scope of the proposals covers the fight against terrorist offences and serious criminal offences, such as trafficking in human beings and drugs ([7]).

6. Article 7 of the proposed Decision determines the conditions for access to Eurodac by designated authorities. Access is allowed only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Council Decision 2008/615/JHA ([8]) on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime return negative results and where the comparison is necessary for the combat of terrorist offences or other serious criminal offences, this comparison is necessary in a specific case and that there are reasonable grounds to consider that the comparison will substantially contribute to the combat of any of the criminal offences in question. The EDPS notes that Article 7 does not require that the data subject whose fingerprints the request concerns is a suspect of any of those criminal offences.

7. It should be reminded that the objective of the creation of the Eurodac system was to facilitate the application of the Dublin Regulation, which makes it possible to determine the Member State responsible for examining an asylum application, by comparing the fingerprints of asylum seekers and illegal immigrants. The Eurodac system enables Member States to identify asylum applicants and persons who have been apprehended while unlawfully crossing an external frontier of the Community. By comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State, or whether an asylum applicant entered the Union territory unlawfully. When adopted, the Regulation establishing Eurodac did not contemplate police access to Eurodac; the fingerprints were collected for the very specific purpose prescribed in Article 1(1) of the Eurodac Regulation.

8. Article 1(2) of the proposed Regulation now extends the purpose of the Eurodac system and adds the purpose of the prevention, detection and investigation of terrorist offences and other serious criminal offences, under the conditions set out in the proposals. This change of purpose is explained in recital 6 of the proposed Decision which stipulates that 'since Eurodac has been established to facilitate the application of the Dublin Regulation, access to Eurodac for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences constitute a change of the original purpose of Eurodac, which interferes with the fundamental right to the private life of individuals whose personal data are processed in Eurodac.'

9. Access by law enforcement authorities to Eurodac has already been announced in the past, some years after adoption of the Eurodac Regulation. It is mentioned in documents such as the Hague Programme, the conclusions of the Mixed Committee of the JHA Council of 12-13 June 2007 and the Commission Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 24 November 2005 ([9]): 'In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as a shortcoming. The same could also be said for SIS II immigration and Eurodac data'.

10. As recognized both in the Impact Assessment and the Explanatory Memorandum, the proposals to make Eurodac accessible to law enforcement authorities have provoked considerable criticisms by several stakeholders.

([5]) Opinion of 20 January 2006 on the proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005) 600 final) (OJ C 97, 25.4.2006, p. 6).

([6]) Opinion of 18 February 2009 on the proposal for a Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) (COM(2008) 825) and Opinion of 18 February 2009 on the proposal for a Regulation establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (COM(2008) 820 final).

([7]) See in particular Article 1 of the proposed Decision.

([8]) OJ L 210, 6.8.2008, p. 1, hereinafter: Prüm Decision.

([9]) COM(2005) 597 final, paragraph 4.6.

III. FOCUS OF THE OPINION

11. In this opinion, the EDPS will analyse the legitimacy of the proposals. This analysis will lead to the conclusion that the EDPS has serious doubts whether these proposals are legitimate and whether legislative instruments should be adopted on the basis of these proposals.

12. The analysis will be made on the basis of the following steps:

(a) the point of departure: how to strike the right balance between the need for public security and the right to data protection.

(b) the proposals as continuation of two more general tendencies:

(i) law enforcement authorities are increasingly facilitated to use personal data of individuals that are not directly related to a specific crime and which had been collected for other purposes;

(ii) new legal instruments were proposed as an addition to existing legal instruments, which have not yet been fully implemented. This raises questions relating to the necessity of such new instruments;

(c) the specific circumstances of the present case. A lot of information is already available for law enforcement authorities in this field;

(d) the proposal will have impact mainly on a particular vulnerable group in society, namely the applicants for asylum, with the risk of further stigmatisation of this group;

(e) the timing of the proposals. The proposals are adopted, not awaiting two important changes of context which might have an important impact on the proposals, namely the Stockholm programme and the (possible) entry into force of the Lisbon Treaty. Moreover, the proposal is made independently from the general recast of the Eurodac and Dublin Regulations, which are still discussed within the Council and the European Parliament;

(f) the compatibility with Article 8 of the European Convention on Human Rights.

13. The opinion will not analyse the substantive provisions of the proposals in detail. In general, the provisions are of a good legislative quality. They are well drafted and ensure strict conditions under which Member States' designated authorities and Europol may request the comparison of fingerprint data with those stored in the Eurodac central database. Nevertheless in paragraphs 49-50, a few comments will be made on the substance.

IV. THE POINT OF DEPARTURE

14. The EDPS wishes to emphasize that a better exchange of information is an essential policy goal for the European Union. This emphasis on information exchange is even more logical in the absence of a European police force, a European criminal justice system and a totally harmonised European border control. Measures relating to information are therefore an essential contribution of the European Union allowing the national authorities of the Member States to address cross border crime in an effective way and to effectively protect the external borders. However, they should not only contribute to the security of the citizens but also to their fundamental freedoms.

15. In other words, governments need appropriate instruments to guarantee the security of the citizen, but within our European society they have to fully respect the citizen's fundamental rights. It is the task of the EU-legislator to ensure this balance. The need for such balance is explicitly underlined by the Commission in its Communication of 10 June 2009 on an Area of freedom, security and justice serving the citizen ([10]). It also plays a significant role in the discussions towards a new multi-annual programme in the area of freedom, security and justice (the 'Stockholm programme').

16. It is in this context good to emphasize that data protection law does by no means prejudice the legitimate interests of governments to protect public security. If data are needed for a specific and legitimate purpose they can be used, where necessary with additional measures providing adequate safeguards. It is also essential that information is gathered, shared and processed only on the basis of concrete needs for security and taking into account data protection principles.

17. The fight against terrorist offences and other serious offences ([11]) can certainly be a legitimate ground to allow processing of personal data, in compliance with the fundamental rights to privacy and data protection. However, to be valid, the necessity of the intrusion must be supported by clear and undeniable elements, and the proportionality of the processing must be demonstrated. This is all the more required in case of an extensive intrusion in the rights of individuals constituting a vulnerable group in need of protection, as foreseen in the proposals.

([10]) COM(2009) 262 final. See also the EDPS Opinion of 10 July 2009 on this Communication, paragraph 22.

([11]) The purposes for which comparison of fingerprint data is allowed under Article 1 of the proposed Decision.

V. THE CONTINUATION OF MORE GENERAL TENDENCIES

The tendency to give law enforcement a wide access to data

18. It should be underlined that the proposals not only fit in the general trend to grant law enforcement authorities access to several large-scale information and identification systems, but also constitute a further step in a tendency towards giving law enforcement authorities access to data of individuals who in principle are not suspected of committing any crime. It moreover concerns data that have been collected for purposes that are not related to the combat of crime. Recent examples are:

— Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ([12]),

— Council Decision 2008/633/JHA of 23 June 2008 concerning the consultation (access) of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences ([13]),

— the proposal for a Council Framework Decision on the use of Personal Name Record (PNR) for law enforcement purposes ([14]).

19. In his opinions relating to these initiatives, the EDPS has taken a critical approach towards granting law enforcement access to personal data of individuals that are not suspected of any crime and that have been collected for other purposes. The EDPS emphasized the need to give a proper justification and to fulfil the necessity and proportionality tests. In his opinion on PNR, he even warned for a move towards a total surveillance society.

20. This approach was specified in the EDPS Opinion on the Commission's Communication of 10 June 2009 on an Area of freedom, security and justice serving the citizen ([15]). The opinion asks to specifically address in the Stockholm programme the tendency to use information collected for other purposes. Strict conditions are needed, such as the condition that requests for data should be proportionate, narrowly targeted and in principle based on suspicions on specific persons.

The need for a general debate on law enforcement access

21. This opinion must also be seen in the context of a wider debate on the future of the EU information exchange and the increased tendency of law enforcement access to huge databases. The EDPS takes this opportunity to emphasize the need for a case-by-case assessment of every proposal of this kind and for a coherent, comprehensive and future-oriented vision on this matter, preferably related to the Stockholm programme.

22. Nowadays, more than ever before, there is a clear need for in-depth reflection on how the EU information exchange and IT large-scale systems should look like. This reflection should duly take into account both the costs for privacy and the effectiveness for law enforcement, in the first place when new instruments are proposed and discussed, but also after those instruments have been implemented, by means of periodic reviews. This is also a matter which requires tailor-made safeguards and more focus on the purpose limitation principle. This vision should include a reflection on the (possible) entry into force of the Lisbon Treaty and its implications on the systems based on a First and Third Pillar legal basis.

Evaluation of existing instruments

23. The present proposals were adopted in addition to existing legal instruments used for consultation of fingerprints, which have not yet been fully implemented. The EDPS points in this context in particular to the Prüm Decision, ([16]), which shall be implemented by the Member States by June 2011. On the basis of this Decision the Member States grant each other an automated access inter alia to national Automated Fingerprint Identification Systems (AFIS) on the basis of a hit/no hit request. If a query on the basis of the Prüm Decision produces a hit, supplementary information, including personal data, can be obtained in the Member State that recorded the fingerprint in its national AFIS using national law, including through mutual legal assistance.

([12]) OJ L 105, 13.4.2006, p. 54. EDPS Opinion of 26 September 2005 (OJ C 298, 29.11.2005, p. 1).
([13]) OJ L 218, 13.8.2008, p. 129.
([14]) Not yet adopted by Council; last available text on the Register of the Council from 29 June 2009, 5618/2/09. EDPS Opinion of 20 December 2007 (OJ C 110, 1.5.2008, p. 1).
([15]) See footnote 8.
([16]) See also paragraph 6 and footnote 6.

24. Another instrument which might be of use in this context is Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union ([17]). This instrument facilitates the exchange of information (i.e. the fingerprints as well as the supplementary information) which is held by or is available to law enforcement authorities in the Member States. This instrument has been operational since 18 December 2008.

25. The only longer existing tool at the disposal of the Member States is the traditional instrument of mutual legal assistance under which the judicial authorities of the Member States can seek access to criminal and non-criminal fingerprint collections, including concerning asylum seekers on the basis of the Convention on Mutual Assistance in Criminal Matters.

26. The EDPS believes that it is essential to first implement and evaluate the application of the new EU instruments that permit consultation by one Member State of fingerprints and other law enforcement data held by another Member State as part of the assessment of the necessity of the access to Eurodac.

27. Compliance with the proportionality principle does not only imply that the proposed measure is effective, but also that the purpose envisaged by the proposal cannot be reached using the existing tools. Those tools must be carefully assessed before additional/new measures are put in place to process personal information. According to the EDPS, such comprehensive assessment has not taken place.

VI. THE SPECIFIC CIRCUMSTANCES OF THE PRESENT CASE

28. As a starting point, the EDPS notes that in its Communication of 24 November 2005 the Commission reminded that 'neither claiming asylum nor a visa application indicates in any way that a hitherto innocent individual will commit a crime or a terrorist act' ([18]).

29. The proposals concern the access to personal data of individuals who not only in principle are not suspected of any crime, but are also in need of higher protection because they flee from persecution. These persons represent an especially vulnerable population, and their precarious position has to be taken into account in the assessment of the necessity and proportionality of the proposed action.

30. The Explanatory Memorandum of the proposed Decision states that there is a structural information and verification gap since there is currently no single system that is accessible to law enforcement authorities which enables to determine the Member State that has information on an asylum seeker.

31. This may be the case, but this does not answer the question why this information is needed on asylum seekers who are as said a vulnerable group and in principle not suspected, whereas similar fingerprinting information is not available on any other group in society either. There may be good reasons, but they are not given by the Commission.

32. The EDPS also draws attention to a further justification of the proposals. The Explanatory Memorandum to the proposed Decision mentions that in case a query on the basis of the Prüm Decision produces a hit, the supplementary information, including personal data, can be obtained in the Member State which recorded the fingerprint in its national AFIS using national law, including mutual legal assistance. Having said this, the Commission seems to use as one argument in the justification of the proposal the fact that 'while this procedure might be successful for those Member States that store fingerprints of asylum seekers together with other fingerprints collected by law enforcement authorities in a national AFIS, it will be unsuccessful for those Member States that do not store fingerprints of asylum seekers in their national AFIS unless they are related to crime'. This argument is also put forward in the Impact Assessment accompanying the proposals.

33. In the EDPS' view, such argument does not have any merit. The systematic storage of the fingerprints of asylum seekers who have not been related to any crime in the same database with other fingerprints collected by law enforcement authorities — of asylum seekers and/or other persons suspected of crime or convicted — raises in itself serious concerns as to the purpose limitation principle and the legitimacy of data processing. Instead of using this argument, the Commission should consider whether this systematic storage is in compliance with EU law on data protection.

VII. THE TIMING OF THE PROPOSAL

34. The proposals are adopted by the Commission at a moment where the context is changing.

([17]) OJ L 386, 29.12.2006, p. 89.
([18]) Communication mentioned in paragraph 9 of this opinion.

35. In the first place, the adoption of the Stockholm programme is expected in December 2009. Intensive discussions on the drafting of this multi-annual programme in the area of freedom, security and justice are taking place these months. The use and exchange of information will be an important issue in the Stockholm programme, including the development of a European Information Model ([19]) or a European Information Management Strategy for security ([20]). In this context, the EDPS advocates a balanced approach whereby privacy and data protection guarantees are embedded in information systems already at the earliest possible stage. Closely related to the Stockholm programme are the activities of the Ad hoc Group on Information Exchange in Council. The subject matter of the present proposals will most probably be covered by those activities.

36. In the second place, the EDPS draws attention to the need for reflection on the consequences of the entry into force of the Lisbon Treaty on the future legislation relating to the activities of law enforcement. The first consequence would be that any proposal of this kind would in the future be subject to an ordinary legislative procedure, thus implying equal involvement of the Council and the European Parliament. The second consequence is related to the abolition of the pillar structure of the EU-Treaty. The Lisbon Treaty might require that the Commission will have to present a new proposal based on the new legal basis, possibly even merging the proposed Regulation and the proposed Decision into one legal instrument, which would in any event contribute to legal clarity.

37. In the third place, the EDPS also questions the need for the adoption of this proposal in a procedure distinct from the general recast of the Eurodac and Dublin Regulations, which are still discussed in Parliament and in Council. The consequence of the present proposals is that while fundamental discussions on the modification of the Eurodac system are not finalised, the purpose of the system will be changed, which also means another fundamental modification of the system. Consistency would have been better ensured if these proposals had been joined to the general recast ([21]) or postponed until after the first modification would have been adopted.

38. Under these circumstances, it is better now to postpone the adoption of the proposal, to avoid legal uncertainty. The Commission does not claim that the proposals have to be adopted with urgency and the urgency is certainly not demonstrated by any other circumstances.

VIII. **COMPATIBILITY WITH ARTICLE 8 ECHR**

39. The Explanatory Memorandum of the proposed Regulation explicitly deals with the compliance with fundamental rights, inter alia with Article 8 of the EU Charter of Fundamental Rights on the protection of personal data. It explains that, according to the Commission, in order to ensure that the processing of personal data for law enforcement purposes does not contravene the fundamental right to the protection of personal data, in particular the necessity and the proportionality, the proposal sets out strict conditions.

40. The EDPS is not convinced by this statement of the Commission. He notes that it is crucial to assess whether the proposals stand the test of legitimacy under Article 8 of the European Convention on Human Rights, as interpreted by the Court of Justice and the European Court of Human Rights. The proposals should comply with the necessity and proportionality principles, taking into account the context of instruments already available. The Commission should make a credible demonstration of this in the proposal or in the Explanatory Memorandum. The leading case in this respect is *S.* and Marper v. the United Kingdom ([22]).

41. In recital 6 of the proposed Decision, it is stated that '(a)ny such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to attain a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve'. However, the recitals do not substantiate why *this proposed instrument* is necessary.

42. It is derived from a well-established case-law of the European Court of Human Rights that an interference shall be considered necessary in a democratic society for a legitimate aim as required by Article 8(2) ECHR if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient' ([23]). The national authorities also enjoy a margin of appreciation, 'the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved' ([24]). The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights ([25]).

([19]) Terminology used by the Commission in its Communication of 10 June 2009, referred to in footnote 8.

([20]) Terminology used by the Swedish Presidency.

([21]) See paragraph 4.

([22]) Joined applications 30562/04 and 30566/04, *S. and Marper* v. *United Kingdom*, judgment of 4 December 2008, ECHR not yet released.

([23]) See, inter alia, the Gillow v. the United Kingdom judgment of 24 November 1986, Series A No 109, paragraph 55.

([24]) See the Leander v. Sweden judgment of 26 March 1987, Series A No 116, paragraph 59. See also Judgment of the ECJ of 20 May 2003, Österreichischer Rundfunk and Others. Joined Cases C-465/2000, C-138/01 and C-139/01, ECR [2003], p. I-4989. paragraph 83.

([25]) Connors v. the United Kingdom, judgement of 27 May 2004, No 66746/01, paragraph 82.

43. In this context, it is primarily needed to assess the purpose of the intended processing of personal data: has the purpose been clearly identified, and does it provide evidence for its necessity and proportionality? It should also be proven that no other means which would be less invasive are available to achieve the envisaged purpose.

44. The proposal claims that the purpose of the Eurodac system has been changed in comparison with the initial one, as is explained in recital 6 of the proposed decision ([26]). However, a simple change of a legislative text will not result in a measure that is compatible with Article 8 ECHR. One can even argue that the legislative change does not result in a change of purpose at all. The data will also in the future be stored in the Eurodac system for the sole purpose of facilitating the application of the Dublin regulation. Only in exceptional situations, as discussed before in this opinion, will law enforcement authorities of the Member States have access. The proposals do therefore not change the purpose, but must be perceived as exceptions to the purpose limitation principle, which may be allowed under Article 13 of Directive 95/46/EC, under certain conditions. The EDPS is however not convinced that these conditions are met in the present case.

45. The EDPS underlines in this context that just stating a change of purpose in the legislative proposal does not make it acceptable. A legislative change does not in itself lead to a different assessment of whether the proposals are necessary in a democratic society, proportionate and otherwise acceptable under the provisions mentioned in the previous paragraph.

46. The intrusive character of the instruments proposed by the Commission is evident. However, their utility and necessity are far from being demonstrated in the proposals. The necessity should be proven by the demonstration of substantial evidence of a link between asylum applicants and terrorism and/or serious crime. This is not done in the proposals. It is true that suspects may have entered the EU territory by putting in a bogus asylum claim. However, the fact that this is a possible scenario does not make it a general pattern which would justify the adoption of the instruments.

47. Also, of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as *a priori* suspects ([27]). In this respect, the European Court of Human Rights bears in mind that the right of every person under the Convention to be presumed innocent includes the general rule that no suspicion regarding person's innocence may be voiced after his or her acquittal ([28]).

48. Moreover, the EDPS believes that a possible argument that direct access by law enforcement to Eurodac is convenient, easy and quick should not be enough for the proposal to pass the test of necessity. The demonstration of necessity cannot be based on mere usefulness of access even under strict data protection safeguards. In short, the EDPS has considerable doubts whether the proposals are legitimate under Article 8 ECHR.

IX. **A FEW COMMENTS ON THE SUBSTANCE**

49. Only by way of 'obiter dictum', the EDPS recommends a specification to be made in the text of Article 2 *bis* of the proposed Regulation or, as an alternative to the latter, adding in the proposed Decision that access to Eurodac can be granted to law enforcement authorities when *they have a specific reason to believe that a suspect has applied for asylum* previously. It is suggested in the Explanatory Memorandum, but not included in the text of the proposal itself. The EDPS believes that such a safeguard would have important added value. However, this suggestion does not in itself mean that the EDPS accepts the principle of the access of law enforcement to Eurodac. It should be understood as a subsidiary recommendation.

50. The EDPS also notes that the stringent criteria for access to Eurodac by designated authorities ([29]) do not apply to the access to Eurodac data by Europol. Requests for comparison by Europol are allowed for the purposes of a specific analysis or an analysis of a general nature and of a strategic type. The EDPS questions how the wider facilities for Europol might comply with the reasoning provided by the Commission, namely that the access is necessary only for specific cases, under specific circumstances and under strict conditions.

X. **CONCLUSION**

51. The EDPS has serious doubts whether these proposals are legitimate and whether legislative instruments should be adopted on the basis of these proposals. These doubts are based on the considerations in this opinion which can be summarized as follows.

52. The EDPS wishes to emphasize that a better exchange of information is an essential policy goal for the European Union. Governments need appropriate instruments to guarantee the security of the citizen, but within our European society they have to fully respect the citizen's fundamental rights. It is the task of the EU-legislator to ensure this balance.

([26]) See paragraph 8 of this opinion.
([27]) S and Marper.
([28]) Asan Rushiti v. Austria, No 28389/95, paragraph 31, 21 March 2000, with further references, 33 EHRR 56.
([29]) Article 7 of the proposed Decision; see paragraph 6 of this opinion.

53. Measures to combat terrorist offences and other serious offences can be a legitimate ground to allow processing of personal data, provided that the necessity of the intrusion is supported by clear and undeniable elements, and the proportionality of the processing is demonstrated. This is all the more required since the proposals concern a vulnerable group in need of higher protection because they flee from persecution. Their precarious position has to be taken into account in the assessment of the necessity and proportionality of the proposed action. The EDPS also points at the risk of stigmatisation.

54. The EDPS recommends to assess the legitimacy of the proposals in a wider context, notably:

(a) the tendency of granting law enforcement access to personal data of individuals that are not suspected of any crime and that have been collected for other purposes;

(b) the need for a case-by-case assessment of every proposal of this kind and for a coherent, comprehensive and future-oriented vision, preferably related to the Stockholm-programme;

(c) the need to first implement and evaluate the application of other new EU instruments that permit consultation by one Member State of fingerprints and other law enforcement data held by another Member State;

(d) the urgency of the proposal, in relation to the changing legal and policy environment.

55. In relation to the compatibility of the proposals with Article 8 ECHR, the EDPS questions the change of purpose of the system and underlines that just stating the change of purpose in a legislative proposal does not constitute such a change. Moreover, a legislative change does not in itself lead to a different assessment of whether the proposals are necessary in a democratic society, proportionate and otherwise acceptable, notably in view of the rules on purpose limitation in Directive 95/46/EC.

56. The EDPS emphasises that the necessity should be proven by the demonstration of substantial evidence of a link between asylum applicants and terrorism and/or serious crime. This is not done in the proposals.

57. Finally, the EDPS welcomes that he is consulted and recommends that reference to this consultation be made in the recitals of the proposal, in a similar way as in a number of other legislative texts on which the EDPS has been consulted, in accordance with Regulation (EC) No 45/2001. He also makes a few comments on the substantive texts of the proposals.

Done at Brussels, 7 October 2009.

Peter HUSTINX

European Data Protection Supervisor