Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] [.....] (Recast version)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

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]

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008[3] on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 30 May 2012, the Commission adopted a proposal concerning a recast for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of

[1] OJ L281, 23.11.1995, p. 31.
[2] OJ L8, 12.1.2001, p. 1.
[3] OJ L350, 30.12.2008, p. 60.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

Regulation (EU) 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 to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice (hereinafter: 'the Proposal').[4]

2. The Proposal was sent by the Commission to the EDPS for consultation on 5 June 2012, pursuant to Article 28(2) of Regulation (EC) No 45/2001. The EDPS recommends that reference to the present consultation be made in the preamble of the Proposal.

3. The EDPS regrets that the Commission services did not ask the EDPS to provide informal comments to the Commission before the adoption of the Proposal, according to the agreed procedure in relation to Commission documents relating to the processing of personal data.[5]

4. The Proposal was presented to the Home Affairs Ministers at the Justice and Home Affairs Council on 7-8 June 2012 and is currently under discussion within Council and the European Parliament with a view to adopt a regulation under the ordinary legislative procedure by the end of 2012. The present opinion of the EDPS intends to give input to this procedure.

1.2. Background

5. EURODAC was established in 2000 by Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of the Dublin Convention.[6] The Commission presented proposals for amendment of this Regulation in 2008[7] and in 2009.[8] The 2008 Commission Proposal aimed at ensuring a higher degree of harmonisation and better standards of protection for the Common European Asylum System (CEAS), while the 2009 Commission Proposal sought to use asylum seekers' fingerprints for law enforcement purposes.

6. The EDPS delivered Opinions on both the 2008 Commission Proposal[9] and the 2009 Commission Proposal.[10] Especially in the second Opinion, the EDPS was very critical.

---

[4] COM(2012)254 final.
[5] The last time, the EDPS was informally consulted by the Commission on an amendment of the EURODAC Regulation was in 2008.
[6] OJ L316, 15.12.2000, p. 1.
[7] COM(2008)825 final.
[8] COM(2009)342 final and COM(2009)344 final.
[9] 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), OJ C229, 23.9.2009, p. 6.

7. Following the entry into force of the Treaty on the Functioning of the European Union (TFEU) and the abolition of the pillar structure, the Commission adopted a new proposal in 2010, replacing the earlier proposals.[11] With a view to progressing in the negotiations on the asylum package and facilitating the conclusion of an agreement on EURODAC, the 2010 Commission Proposal did no longer include provisions on access to EURODAC for law enforcement purposes.

8. The current Proposal withdraws and replaces the 2010 Commission Proposal using the recast procedure in order to:
    - take into account a resolution of the European Parliament and the results of negotiations in the Council;[12]
    - introduce the possibility for Member States' law enforcement authorities and Europol to access the EURODAC central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences;
    - introduce the necessary amendments to Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice.[13]

9. According to the Explanatory Memorandum of the Proposal, it has become clear that including law enforcement access for EURODAC 'is needed as part of a balanced deal on the negotiations of the Common European Asylum System package'.[14] No new consultation and impact assessment were conducted for the current Proposal since, according to the Explanatory Memorandum, the Impact Assessments of 2008 and 2009[15] were still valid. Apparently, for the same reasons, the EDPS was not given the possibility to provide informal comments, as mentioned in point 3 above.

1.3. Reasons for and structure of this EDPS Opinion

10. In the present Opinion, the EDPS wishes to highlight the following main concerns:
    - the procedure followed does not do justice to the fundamental nature of the Proposal; a new impact assessment should have been performed;
    - the necessity and proportionality of access to EURODAC data for law enforcement purposes are not sufficiently demonstrated;
    - the Proposal does not consider sufficiently the implications of the use of EURODAC data for law enforcement purposes with regard to applicable data protection law aspects, nor does it consider the new legal

[10] Opinion of 7 October 2009 on the proposals regarding law enforcement access to EURODAC, OJ C92, 10.4.2010, p. 1.
[11] COM(2010)555 final.
[12] See the Explanatory Memorandum p. 3.
[13] OJ L 286, 1.11.2011, p. 1.
[14] See the Explanatory Memorandum p. 3.
[15] SEC(2008)2981 and SEC(2009)936.

basis for data protection since the entry into force of the Lisbon Treaty, and the ongoing data protection reform.

11. The Opinion is structured as follows:
    - Section 2 provides critical remarks on the procedure followed by the Commission;
    - Section 3 focuses on the general concerns with regard to the access to EURODAC data for law enforcement purposes;
    - Section 4 contains comments on the applicable data protection law in the collection and processing of EURODAC data in a law enforcement perspective;
    - Section 5 contains comments on more specific provisions in the proposal relating to EURODAC access for law enforcement purposes;
    - Section 6 provides some comments on other provisions of the proposal;
    - Section 7 lists the conclusions.

12. The Opinion builds on points of view expressed in earlier opinions relating to the EURODAC review (see point 5), as well as on other opinions in relevant areas. It also takes into account the experiences of the EURODAC Supervision Coordination Group, established to facilitate the supervision foreseen under Article 20 of the current EURODAC Regulation.[16]

2. THE PROCEDURE FOLLOWED BY THE COMMISSION

13. It appears that the Commission understands this Proposal as a technical exercise. From the Explanatory Memorandum it can be deduced that it mainly aims at reviving its older proposal, issued in 2009. However, in the last three years important institutional and substantive changes have taken place, for instance as a consequence of the entry into force of the Treaty of Lisbon. Moreover, the fact that in 2010 it was decided to take out provisions on law enforcement access in order to facilitate negotiations in Council and Parliament is a clear indication that the present proposal - including as a main objective law enforcement access - is not of a predominantly technical nature.

14. According to the Commission, the Proposal reinstates the provisions proposed in the lapsed proposal for a Council Decision of 2009. None of the elements introduced are considered new and all of them were assessed in the previous 2008[17] and 2009[18] Impact Assessments. Therefore, the Commission does not attach a new impact assessment, but uses the 2008 and 2009 impact assessments to justify the adoption of the present Proposal. The EDPS disagrees with this approach and still sees the need for a new Impact Assessment.

15. According to the EDPS there are two reasons why the two impact assessments carried out three and four years ago are not sufficient to demonstrate the actual necessity and consistency of the present Proposal.

[16] See on this group: http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Supervision/Eurodac.
[17] SEC(2008) 2981, 3.12.2008.
[18] SEC(2009) 936, 10.9.2009.

16. The first reason is that the results of the previous impact assessments were not relevant or not convincing. The 2008 Impact Assessment is irrelevant as it does not assess the introduction of law enforcement access to EURODAC. The 2009 Impact Assessment does evaluate the possibility to use EURODAC data for law enforcement purposes, but this assessment lacked comprehensive analysis[19].

17. In the 2009 Impact Assessment four policy options were considered for regulating access to asylum seekers' data for law enforcement purposes.[20] The first option (maintaining the status quo) was ruled out without explanation. Two out of the three other options consisted of analysing the reasons why access to the EURODAC database would be essential in order to identify alleged criminals, as well as to prevent, combat and investigate a crime. However, the analysis failed to at least provide specific examples which justify a real necessity of this access.[21] Moreover, the analysis failed to take into account that asylum seekers as such are a vulnerable group of people which would require assessing the need for additional protection.

18. The fourth policy option concerned the possibility to create a decentralised network that would allow each Member State to search the national asylum seekers databases of all other Member States in an automated manner. This option suggested that the new network would use only existing instruments such as the mechanism foreseen under Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime ('the Prüm Decision').[22] This option was ruled out arguing that it would be complicated and costly.

19. The 2009 Impact Assessment repeatedly stated that existing law enforcement instruments are insufficient and not practical in comparing fingerprints for the investigation of a crime. In particular, the impact assessment pointed out that searching fingerprints through the national automated fingerprint identification systems ('AFIS')[23] of other Member States using the Prüm Decision was not fully reliable because some Member States may not store fingerprints of asylum seekers in their national AFIS unless they were related to crime.[24] Moreover, the impact assessment stressed that Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities[25] could only be used to collect data on asylum seekers if there were factual reasons to believe that the information was actually available in

[19] For further details, see the 2008 and 2009 EDPS Opinions; see also the EDPS Opinion of 15 December 2010 on the establishment of 'EURODAC' for the comparison of fingerprints, OJ C101, p. 14.
[20] SEC(2009)936, p. 17-19.
[21] The examples given in p. 11-12 of the impact assessment are too general and vague. They are not based on real and specific cases, but rather hypothetical situations in which the comparison of asylum seekers' fingerprints might be useful for law enforcement purposes. See also pt. 46-48 of the EDPS Opinion of 2009.
[22] OJ L210, 6.8.2008, p. 1-11.
[23] See Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210 , 06.08.2008, p. 12 (' the Prüm Implementing Decision').
[24] SEC(2009)936, p. 9.
[25] OJ L 386, 29.12.2006, p. 89.

a particular Member State.[26] Finally, the impact assessment noted that mutual legal assistance would require a request to be addressed to all Member States that are believed to have the relevant information, which was time consuming.[27]

20. The EDPS considers that it should be demonstrated that the combination of these three instruments, and their simultaneous use would not cover all possible situations in which the identity of asylum seekers is needed for law enforcement purposes. Furthermore, in all the examples provided by the 2009 Impact Assessment, the Prüm Decision as well as other instruments were dismissed assuming that they would be insufficient because not all asylum seekers have their fingerprints recorded in other systems. Yet, the impact assessment failed to give consistent and justified arguments for an additional instrument especially focusing on asylum seekers[28], whereas comparable instruments are not foreseen and therefore presumably not necessary for other groups of individuals.

21. The second reason why a new impact assessment is needed is that the two previous Impact Assessments are out of date. They were written against a background where the Prüm Decision and the Prüm Implementing Decision were only partially applied in the Member States. The EDPS takes the view that the progress made since 2009 in the application of those decisions should be part of the assessment whether law enforcement access to EURODAC is actually needed.

22. Moreover, the Proposal does not include a Fundamental Rights Impact Assessment in accordance with the Commission's Communication 'Strategy for the Implementation of Fundamental Rights by the European Union' from 2010 which was adopted in light of the entry into force of the Lisbon Treaty which gave the Charter of Fundamental Rights of the European Union primary EU law status.[29] The Impact Assessment should examine the impact of the proposal on fundamental rights using the checklist provided in this Communication.[30]

23. This checklist requires that answers be given to fundamental questions such as whether the impact is beneficial (promotion of fundamental rights) or negative (limitation of fundamental rights) or/and if the limitation of fundamental rights is necessary to achieve an objective of general interest or to protect the rights and freedoms of others, whether the measure is proportionate to the desired aim and preserves the essence of the fundamental rights concerned.

24. On the basis of the foregoing, the EDPS strongly recommends that the Commission provides a new impact assessment in which all four policy options are considered, in which solid evidence and reliable statistics are provided and which includes a fundamental rights assessment. This should all be done with due account to the practical and legal developments that took place since 2009.

[26] SEC(2009)936, p. 9.
[27] *Ibidem*, p. 9-10.
[28] See more in detail points 31-32.
[29] COM (2010)573.
[30] See also the Commission's Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC(2011)567, 06.05.2011.

3. ACCESS TO EURODAC DATA FOR LAW ENFORCEMENT PURPOSES

3.1. Purpose limitation and the risk of function creep

25. When the Regulation establishing EURODAC was adopted and the database became operational in 2003, it did not contemplate police access to its database. The fingerprints are collected and processed for purposes of determining which Member State is responsible for examining an asylum application, for preventing multiple asylum applications within the EU and, more in general, for facilitating the application of the Dublin Regulation.[31] Specific safeguards are provided to ensure that the EURODAC database is *not* used for other purposes.

26. The Proposal suggests a new legal regime, in which data will still be collected for the purpose of examining asylum applications, but the data could - under certain circumstances - be used for another purpose, i.e. law enforcement outside the context of asylum and migration. This constitutes what is often described as "function creep", namely, a gradual widening of the use of a system or database beyond the purpose for which it was originally intended.

27. In general, the EDPS has strong reservations against this trend. He calls for a cautious approach as to initiatives with a view to possible use of data or systems for other unrelated purposes. It should not be easily accepted that since the data is already collected, it can just as well be used for other purposes which might have a bigger impact on the life of individuals. The assessment as to the necessity and proportionality of the creation of EURODAC would have been completely different if law enforcement access was envisaged from the outset.

28. Moreover, this widening of the use of an existing system is difficult to reconcile with the purpose limitation principle, which is one of the key principles of data protection law.[32] Exceptions to the purpose limitation principle are possible, but only under strict conditions. First and foremost, the processing of the data for the other purpose should be necessary and proportionate.

29. The EDPS is not convinced that the necessity and proportionality that could justify an exemption to the purpose limitation principle has been sufficiently demonstrated. A better justification is needed. This is explained in the next sections.

3.2. Necessity of access for law enforcement purposes

30. The Proposal raises questions with regard to the necessity of granting access to EURODAC for law enforcement purposes, since, as indicated, there already exist a number of legal instruments which permit that one Member State

[31] The Dublin Convention was in 2003 replaced by Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ L 50, 25.2.2003, p. 1 ("Dublin Regulation").

[32] The principle can be found in Article 5(b) of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 28.1.1981 ('Convention 108'), Article 6(1)(b) of Directive 95/46/EC and Article 3 of Framework Decision 2008/977/JHA.

consults fingerprints and other law enforcement data held by another Member State.[33]

31. First, Member States can make use of the Prüm Decision, the aim of which is stepping up cross-border cooperation between EU countries in criminal matters, including through networking Member States' national databases[34]. Under Article 8 of the Prüm Decision, Member States shall ensure availability of reference data from national AFIS established for the prevention and investigation of criminal offences. These reference data shall only include a reference number and dactyloscopic data (i.e 'fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae), when they are stored and dealt with in an automated database'[35]).

32. Second, other instruments could be applied. Framework Decision 2006/960/JHA could be used for consultations of fingerprints. The measures foreseen in this instrument can be used subject to some conditions such as the need to give factual reasons to believe that the information is available in the other Member State, as well as the need of a prior authorisation by a judicial authority. Moreover, the European Convention on Mutual Assistance in Criminal Matters[36] could also be used by judicial authorities of Member States to seek access to criminal and non-criminal fingerprint collection, including asylum seekers. Finally, if a third-country national has applied for a Schengen visa, his or her fingerprints will already be stored in the Visa Information System as visa applicant;[37] and if the third-country national is wanted for arrest or an alert has been issued for the purpose of refusing entry, he/she will be in the Schengen Information System.[38]

33. Therefore, the EDPS suggests that before creating a new instrument providing law enforcement authorities with access to asylum seekers' data, a thorough and more up-to-date evaluation should be carried out, in order to see whether a full implementation of the existing instruments would not be sufficient. The EDPS believes that there are sufficient reasons to assume that the existing instruments may already be effective and sufficient.

34. The state of play of the Prüm Decision and the Prüm Implementing Decision has recently been examined by the Council. The Council noted that some implementation difficulties still existed[39] and called in December 2011 on the Member States to finalise their domestic legal and technical implementation procedures in order to fully implement the Prüm Decisions.[40] Likewise, the Council invited Member States to prepare the assessment of the effectiveness

[33] See on this more in detail also the EDPS Opinion of 7 October 2009.
[34] See Article 1 and Recital 13 of the Prüm Decision.
[35] Article 2 (i) of the Prüm Implementing Decision.
[36] European Convention on Mutual Assistance in Criminal Matters , CETS No 030, 20.04.1959.
[37] On the basis of Art 8 of Regulation (C) No 767/2008 of the European Parliament and the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). OJ L 218/60, 13.08.2008.
[38] On the basis of Art. 95 and 96 of the Shengen Convention.
[39] Council of Ministers, 18676/11, 20.12.2011.
[40] Council of Ministers, 17762/11, 5.12.2011.

and efficiency of the Prüm Decisions as an information exchange tool.[41] This is also in line with the Stockholm programme, which points out that '*increased attention needs to be paid in the coming years to the full and effective implementation, enforcement and evaluation of existing instruments*'.[42]

35. Furthermore, the EDPS is highly interested in this respect in the Commission Communication on the European Information Exchange Model which has been announced for 2012 and which will be based, amongst others, on the results of the Information Mapping Exercise launched by the Commission in 2010.[43] The objective of the latter was to analyse the current systems and channels of information to establish whether there is a need for new instruments and measures. As long as the implementation of current instruments is not fully in place and further analysed, the EDPS considers that granting access to EURODAC data for law enforcement purposes would be premature.

3.3. Proportionality of access for law enforcement purposes

36. The EDPS also has doubts as to whether access to EURODAC data by law enforcement authorities would comply with the requirement of proportionality.

37. It should be underlined that asylum seekers constitute a vulnerable group of people and, accordingly, their precarious position has to be taken into account when assessing the necessity and proportionality of the proposed action.[44] This has not been considered in the Proposal.

38. The net result of the proposed changes to the current system is that an asylum seeker can be identified from a crime scene if a finger print is found, while other individuals cannot, because similar data is not available for all other groups of the society. The Commission has not given any justification for a difference in treatment between asylum seekers and other individuals in this respect. Processing of EURODAC data for law enforcement purposes could therefore lead to a potential discrimination of asylum seekers, which, without justification, cannot be seen as a proportionate measure.

39. It should be underlined that the Court of Justice of the EU and the European Court of Human Rights ('ECtHR') have condemned databases which led to an unjustified unequal treatment of persons.[45] In *S. and Marper*, the ECtHR pointed at the risks of stigmatisation in this respect.[46]

40. Proportionality also means that, would the necessity of access be demonstrated and the balance of rights and interests be respected, law enforcement access should be subject to strict conditions, as also highlighted in Recital 9 of the Proposal, including the condition that there should be a substantiated suspicion

[41] *Ibidem*.
[42] Stockholm Programme, point 1.2.2.
[43] At http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/eixm/index_en.htm.
[44] See also de EDPS Opinion of 2009, pt. 29.
[45] See CJEU 16 December 2008, Case C-524/06, *Huber*, [2008] ECR I-09705 and ECtHR 4 December 2008, 30562/04 and 30566/04, *S. and Marper v. United Kingdom*.
[46] *Ibidem*, para 122.

that the perpetrator of a terrorist or other serious criminal offence has applied for asylum (see also point 56 below).

4. APPLICABLE DATA PROTECTION LAW

41. Currently, Directive 95/46/EC applies to all data processing operations carried out by the Member States within the framework of the EURODAC system. However, granting law enforcement authorities access to EURODAC data, leads to the applicability of the complicated legal framework adopted on the basis of the former third pillar. Processing of personal data by national competent authorities is covered by the provisions of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[47] in so far as it falls within its scope. Processing of personal data by Europol is covered by Council Decision 2009/371/JHA establishing the European Police Office (Europol)[48].

42. The Proposal contains several provisions specifying certain data protection rights and obligations. According to recital 32 of the Proposal, these are supplements or clarifications of Directive 95/46/EC. However, it remains unclear, how these specifications relate to Framework Decision 2008/977/JHA or to Council Decision 2009/371/JHA.[49] Article 33, which declares that both decisions are applicable to EURODAC data processing by law enforcement authorities and Europol respectively, does not provide further clarity on this. This leaves open the question whether certain specifications of the Proposal must also be seen as supplementing or clarifying these two decisions.

43. The main example is Article 35 which explicitly prohibits the sharing of personal data with third countries, international organisations or private entities. It is not made clear how this prohibition relates to the possibility of transferring personal data under Framework Decision 2008/977/JHA. In this respect it is relevant to point at the fact that Framework Decision 2006/960/JHA does not contain a prohibition on transferring of data to third countries.[50] The EDPS takes the view that the transfer of EURODAC data is indeed prohibited, also in case of use of EURODAC data for law enforcement purposes and recommends the legislator to clarify this in Article 35 of the Proposal.

44. Article 35 contains an exception to the prohibition. Member States have the right to transfer personal data to third countries to which the Dublin Regulation applies. According to the EDPS, it should be clarified in the recitals or in a substantive provision that this exception does not apply to transfer to those particular third countries in the context of law enforcement.

45. Another example concerns Article 29 of the Proposal which defines the rights of the data subject. If Article 29 would indeed constitute a supplement to or

[47] OJ L 350, 30.12.2008, p. 60.
[48] OJ L 121, 15.5.2009, p. 37.
[49] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office ('EUROPOL'), OJ L121/37, 15.5.2009.
[50] OJ L386, 29.12.2006, p. 89-100.

clarification of Framework Decision 2008/977/JHA or Council Decision 2009/371/JHA, it should pay specific attention to the rights of data subjects in relation to law enforcement access and further use. For instance, on the basis of Article 29(1)(b), the data subject has the right to be informed of the purposes for which his or her data will be processed. However, this provision only mentions that a description of the aims of the Dublin Regulation will be included. If it is decided to grant access to Eurodac for law enforcement purposes, this should be added to the information communicated to the data subject.

46. The need for clarity on how the provisions of the Proposal relate to the Framework Decision 2008/977/JHA as well as Council Decision 2009/371/JHA is even stronger since the proposals for a new data protection framework of 25 January 2012 intend to keep the distinction between a general data protection instrument and a self-standing instrument for law enforcement purposes.[51] Moreover, the proposed new rules do not touch the data protection rules for EU institutions, bodies and agencies as laid down in Regulation (EC) No 45/2001, nor the specific data protection rules such as the ones for Europol and the data protection rules under the Prüm Decision.[52]

5. SPECIFIC PROVISIONS OF THE PROPOSAL RELATING TO LAW ENFORCEMENT ACCESS

47. As stated above, it should first be demonstrated that law enforcement access to EURODAC as such is necessary and proportionate. The conditions under which such access might be provided are part of a further analysis which should only take place in case the necessity and proportionality are sufficiently demonstrated. The comments made below should then be taken into account.

5.1. Designated and verifying authorities

48. Member States shall determine 'designated authorities' (Art. 5 of the Proposal), as well as 'verifying authorities' (Art. 6 and 7 of the Proposal). Both types of authorities must be responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences. However, their responsibilities are very different.

49. Under Article 5, the designated authorities shall be authorised to access Eurodac data pursuant to the proposed Regulation. To ensure unequivocally that such

[51] COM(2012)11 final and COM(2012)10 final.

[52] See the Opinion of the EDPS on the data protection reform package of 7.3.2012, para 26, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.. Asylum seekers are also protected by two other pieces of legislation. First, Directive 2011/95/EC (OJ L337, 20.12.2011, p. 9) enshrines the confidentiality principle (Article 37), and protects the collection, processing and circulation of information of unaccompanied minors (Article 31(5)). Second, Council Regulation (EC) No 343/2003 (OJ L50, 25.2.2003, p. 1) establishes that Member States' requests of personal data shall be appropriate, relevant and non excessive for examining the application for asylum (Article 21(1)), the information exchanged may only be used for the purpose of determining the Member State responsible for examining an application for asylum (Article 21(7)), and the asylum seeker has the right to be informed, in accordance with Directive 95/46/EC (Article 21(9)).

access is limited to law enforcement purposes, the EDPS recommends adding in Article 5(1) 'for the purposes referred to in Article 1(2)'.

50. The verifying authority referred to in Article 6 shall verify the lawfulness of the designated authorities' requests of access to Eurodac data. It will examine and validate[53] whether the conditions of such access are complied with. The EDPS considers the control mechanism as an essential safeguard to prevent unlawful access. He emphasises that the preferred option, from a fundamental rights perspective, would be the requirement of a prior judicial authorisation which offers appropriate and strong safeguards of independence and impartiality. In the absence of a requirement for a judicial authorisation, it is essential to ensure that the verifying authority must be effectively independent from the designated authority to guarantee a real and proper control, and create a proper system of checks and balances.

51. Therefore, the EDPS recommends as a minimum adding to Article 6 of the Proposal that the verifying authority shall perform its duties and tasks independently and shall not receive instructions as regards the exercise of the verification.

52. The same considerations apply to Article 7 of the proposal regarding access to EURODAC data by Europol.

5.2. Procedure and conditions for comparison and data transmission for law enforcement purposes

53. Under Article 19 of the Proposal a request for access to EURODAC data for law enforcement purposes shall be submitted to a prior check of the verifying authority which shall verify whether the conditions for access are fulfilled. Paragraph 3 provides an exception to this prior check in 'exceptional cases of urgency'. In such cases, ex-post verification shall be carried out without undue delay after the processing of the request. However, no guidance is provided about what qualifies as an exceptional case of urgency. This lack of clarity might lead to diverging interpretations and uncertainty about the scope of the exception. The EDPS recommends adding in Article 19 the criterion of the need to prevent an imminent danger associated with serious criminal or terrorist offences.[54]

54. Moreover, Article 19(3) mentions that the ex-post verification shall be carried out 'without undue delay' after the processing of the request. The EDPS considers that the wording 'without undue delay' is too vague and recommends introducing a concrete time limit.

55. In accordance with Article 20, designated authorities may request comparison of fingerprints with those stored in the EURODAC Central Unit for law enforcement purposes only if comparisons of national fingerprint databases and of the

[53] See Article 19(2) of the Proposal.

[54] One could also think of alternative, more specific formulations, such as those mentioned in recital 26 of the proposal, in particular: "a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences".

Automated Fingerprints Databases of other Member States under Prüm Decision return negative results and where:

- the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences (Article 20(1)(a));
- the comparison is necessary in a specific case; systematic comparisons shall not be carried out (Article 20 (1) (b)) and;
- there are reasonable grounds to consider that it will contribute to the prevention, detection or investigation of any of the criminal offences in question (Article 20 (1) (c)).

56. The EDPS welcomes the requirement of a prior consultation of national databases and databases from other Member States through the mechanism set up by Prüm Decision. However, he considers that a prior check of the Visa Information System should also be required. Furthermore, he notes that the list of conditions does not include the requirement referred to in recital 9 of the Proposal and in the Explanatory Memorandum that there should be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offences has applied for asylum.[55] In light of what has been said before about the proportionality of law enforcement access to EURODAC data, the EDPS considers this condition as particularly important and strongly recommends the legislator to add it to the list of Article 20 of the Proposal. The reference in recital 9 is not sufficient to ensure compliance with this requirement.

57. The EDPS considers that the use of the wording in Article 20 (1) (c) 'contribute to' is too broad. As mentioned in the Explanatory Memorandum, the comparison of data should 'substantially' contribute to the prevention, detection or investigation of serious crimes in question.[56] The EDPS suggests amending Article 20 (1) (c) accordingly. In relation to the same provision, the EDPS recommends clarifying what is meant by 'reasonable grounds'.[57]

58. As far as Europol is concerned, neither the explanatory memorandum nor the recitals explain the need for Europol to access EURODAC data. Recital 10 only refers to Europol's 'key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation' to justify its access to EURODAC data within the framework of its tasks. The 2009 impact assessment also provides little details on the concrete need of a direct access by Europol[58]. In practice, a national law enforcement authority may (and most probably will) - prior to the sending of fingerprints to Europol - where relevant compare them with

[55] See especially Recital 9 and p. 7 of the Explanatory Memorandum.
[56] See p. 7 of the Explanatory Memorandum.
[57] See also the EDPS Opinion of 2010, point 49.
[58] The 2009 impact assessment mentions that: '(...) Europol is expected to provide national law enforcement authorities with the necessary tools to exchange information between them, such as exchange of information using the Europol National Units. It follows from the replies of Europol and the Member States to the questionnaire that the exchange of information between those units would benefit if information exchanged in relation to asylum seekers' fingerprints could form part of the information exchanged to them via Europol as part of a concrete file related to cross-border organised crime. Since Europol currently cannot access information on asylum seekers, it cannot ensure that this information be part of its analysis and investigation tasks'.

EURODAC data. The EDPS therefore recommends at least describing in a recital the kind of situations justifying a *direct* access by Europol to the EURODAC Central Unit.

59. Furthermore, the EDPS notes that the stringent criteria for access to EURODAC data by designated authorities 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 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. In the absence of any particular explanation, the EDPS recommends to align Article 21 with Article 20.

5.3. Comparison with latent fingerprints

60. Currently, by comparing fingerprints of a person with EURODAC data, EU countries can determine whether an asylum applicant or a foreign national found illegally present within an EU country has previously claimed asylum in another EU country or whether an asylum applicant entered the Union territory unlawfully. These situations require the person concerned to be physically present (at least at a given moment) to allow relevant national authorities to take his/her fingerprints with a view to compare them with EURODAC data. The carrying out of comparisons for law enforcement purposes is different in its approach since fingerprints can be taken at a crime scene or in another environment in the absence of the person concerned. This brings new concerns about the potential adverse effects it may have on innocent persons.

61. The EDPS has strong doubts as regards the possibility of searching latent fingerprints in the EURODAC system for law enforcement as considered in recital 12. Any search in EURODAC based on a latent fingerprint, particularly if found in public places, may lead to a high number of possible matches, given the wider range of possible correlations with partial or fragmentary prints. The consequences of a false match may be serious and may lead to the wrongful implication of innocent persons in criminal investigations. The rate of error may be influenced by the quality of the latent fingerprints which are often distorted, adding to the difficulty of matching these fingerprints to those stored in 'EURODAC' which are taken in better conditions.

62. Comparison of fingerprints for law enforcement purposes should in any case be subject to at least the same safeguards already foreseen especially in Article 25 (4) of the Proposal.

5.4. Access and retention of personal data for law enforcement purposes

63. Article 33(4) foresees that 'personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for a specific ongoing criminal investigation by that Member State, or Europol'. The EDPS welcomes the retention period for data retrieved from EURODAC for law enforcement purposes. However, he asks for clarification on the requirement of absence of specific ongoing criminal investigation for deleting the data. Access to EURODAC data should only be allowed when there is an existing ongoing criminal investigation. The EDPS therefore recommends specifying more clearly the framework of this exception or deleting it.

5.5. Nature of data accessed for law enforcement purposes

64. Articles 9 (5), 15 (2) and 17 (4) - which concern access to EURODAC in the context of the application of the Dublin Regulation - specify that when there is a hit (i.e. the existence of a match or matches by comparison between fingerprints data recorded in the Central System and those transmitted by a Member State), the Central System shall transmit for all data sets corresponding to the hit, the data referred in Article 11[59] along with where appropriate, the mark referred to in Article 18.1. However, the proposal does not contain similar provisions when comparison of fingerprints is requested for law enforcement purposes.

65. The explanatory memorandum (p.7) mentions that 'the comparison with EURODAC for law enforcement purposes will provide a result on a 'hit/no hit' basis - i.e. it will only determine if another Member State holds data on an asylum seeker. The proposal does not provide for new possibilities to process additional information in the follow-up to a 'hit' '. The EDPS wonders how effective it would be for the law enforcement authorities to only get 'hit/no hit' information, i.e the existence or non existence of a matching. It can reasonably be presumed that the law enforcement authorities would need to know which Member State holds the data on the asylum seeker the fingerprints belong to.

66. This possible need for additional information should be clarified. In the event that the communication of additional information to the 'hit' (e.g. the identification of the Member State holding the data) is considered, the EDPS recalls that pursuant to the principles of necessity and proportionality, the information to be transmitted should be limited to the strict minimum necessary for the purpose for which access has been carried out.

[59] The proposal refers to the data mentioned in Article 8(a). However Article 8(a) concerns the statistics to be drawn up by the Agency. The EDPS deduces from the EURODAC Regulation, that the relevant provision is actually Article 11 of the proposal which lists the data recorded in the Central System. .

5.6. IT Agency and amendments to Regulation (EU) No 1077/2011

67. The EDPS wonders why the rules on professional secrecy contained in Article 17 (5) (g) of Regulation 1077/2011[60] have been withdrawn (see Article 38.4 (a) of the proposal) and recommends restoring them.

68. Article 38 (2) of the proposal introduces in Article 12(1)(t) the obligation for the Management Board to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes. The proposal does not provide for further explanation about this obligation. The EDPS understands that this is linked to reports and statistics to be provided by the Agency. He therefore recommends specifying in Article 38 (2) of the proposal amending Article 12(1)(t) of Regulation 1077/2011 the precise purposes of such request, as well as the anonymisation by law enforcement authorities of the data prior to their transmission to the Management Board.

6. OTHER SPECIFIC PROVISIONS OF THE PROPOSAL

69. The EDPS has commented on other provisions of the Proposal in his Opinions of 2008 and 2009, mentioned in point 6 above. These comments are not repeated here in full. This section will highlight the main concerns and address new amendments. Where relevant, reference is made to the more in-depth analysis in the previous EDPS Opinions.

6.1. Article 4: operational management

70. The EDPS welcomes the obligation to ensure that at all times the best available technology subject to a cost-benefit analysis is used for the Central System (Article 4(1)). However, he recommends replacing the expression 'Best Available Technologies' by 'Best Available Techniques' which include both the technology used and the way in which the installation is designed, built, maintained and operated. This is important because the concept of 'best available techniques' is broader and covers various aspects contributing to the application of 'data protection by design' which is considered a key principle in the review of the EU data protection legal framework.[61]

71. In Article 3(1), a Business Continuity System is foreseen. Furthermore, in Article 4(5), the availability of the platform is fixed to 24hours a day, 7 days a week. This shows the system is considered as critical. However, no details on this "Business Continuity System" or its security and data protection needs are provided.

---

[60] Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011, p.1.

[61] See Article 23 of the Commission proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final and paras 177-182 of the EDPS Opinion of 7 March 2012. See also EDPS Opinion of 15 December 2010 and EDPS Opinion of 18 February 2009.

72. A critical system should be covered by a sound and tested Business Continuity Plan (in case of major disruptions or disasters) which has repercussions on data protection, security and costs. Due care should be taken in defining the availability needs for the system which should take into account maintenance needs and unforeseen downtime. Additionally, requirements in terms of business continuity should be described. When defining business continuity measures, their impact on data protection should be taken into account. Impact may exist due to the existence of duplicates of the data, backup media and additional physical locations and systems at which data could be physically accessed. The EDPS recommends replacing the Business Continuity System by the need for a Business Continuity Plan in Article 3(1) and 4(5) and providing a legal basis for implementing measures containing the modalities of such plan.

6.2. Articles 9, 14 and 17: failure to enrol

73. The EDPS recalls the problem of so-called 'failure to enrol', i.e. the situation in which a person's fingerprints are not usable. It is important to ensure that 'failure to enrol' does not automatically lead to a denial of rights for asylum seekers. The Proposal already envisages partly the failure to enrol in Article 9(1) and 9(2). However, these provisions only envisage the hypothesis of temporary failure to enrol, whereas in some cases this impossibility will be permanent. Therefore, the EDPS recommends adding to Articles 9, 14 and 17 a provision stating that temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual. In any case, it can not represent sufficient grounds to refuse to examine or to reject an asylum application.[62]

6.3. Article 16: data retention

74. The EDPS welcomes the amendment in Article 16 establishing one year as the retention period for data (instead of two years in the current text of the Regulation). This constitutes a good application of the principle of data quality which stipulates that data should not be kept for longer than necessary to accomplish the purpose for which they are processed.[63]

6.4. Article 29: right of information

75. The EDPS underlines that the information to the data subject should be provided in a way that enables the asylum seeker to fully understand his/her situation as well as the extent of the rights, including the procedural steps he/she can take as follow-up to the administrative decisions taken in his/her case. In that respect, the EDPS welcomes the additions made in Article 29(1), which are in line with the proposal for a general data protection regulation.[64]

---

[62] See EDPS Opinion of 15 December 2010 on the establishment of EURODAC for the comparison of fingerprints, Section IV, OJ C 101/14.

[63] See Articles 6(1)(e) of Directive 95/46 and 4.1 (e) of Regulation 45/2001. See also Article 4(2) of the Council Framework Decision 2008/977/JHA.

[64] See EDPS Opinion of 15 December 2010 and Art. 11 and 14 of the proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing

76. The EDPS welcomes the drawing up of a clear and simple common leaflet containing the information to be given to the data subject and the obligation for Member States to provide information in an age-appropriate manner when the person is a minor. This contributes to better harmonization and compliance with the EURODAC Regulation and follows recommendations of the EURODAC Supervision Coordination Group[65].

6.5. Articles 28 and 36: keeping of records, logging and documentation

77. For purposes of data protection monitoring and data security, the Agency, Member States and Europol shall keep records of all data processing operations within the Central Unit (Article 28) and in relation with requests for comparison with EURODAC (Article 36). However, although the aims are the same (data protection and data security), the wording used in both provisions differs (eg Article 28 mentions the unit *entering in or retrieving the data*, Article 36 refers to the name of the *authority having requested access* for comparison). In order to ensure consistency and allow proper supervision, the EDPS recommends merging both provisions in a single one using the wording of Article 36 which is more precise and complete.

78. Furthermore, Article 36 provides for additional logs/documentation to be kept by Member States and Europol in comparison to the records kept by the Agency. (e.g. the identifying mark of the official who carried out the search and of the official who ordered the search or supply). The EDPS welcomes this obligation which is in line with the principle of accountability and will help ensuring effective supervision.

79. Finally, the EDPS notes that while Article 36 refers to the access by the national supervisory authorities to these logs, there is no mention of a similar access for the EDPS and the Europol's supervisory authority to the records kept by the Agency and Europol respectively. The EDPS recommends amending Article 28 accordingly.

6.6. Articles 31 and 32: supervision model

80. The EDPS welcomes the supervision model laid down in Article 31 and 32 of the Proposal. This model is similar to the model for the Schengen Information System (2nd generation) and the Visa Information System.[66] It reflects the current practice

---

of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final.

[65] See Second coordinated inspection on information to data subjects and assessment of the age of young asylum seekers, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/09-06-24_Eurodac_report2_EN.pdf.

[66] See Art. 41 to 43 of VIS Regulation, Art. 46 of Regulation (EC)No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJL381, 28.12.2006, p. 4 and Art. 62 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L265, 7.8.2007, p. 63.

which proved efficient and encouraged close collaboration between the EDPS and national DPAs. Therefore, the EDPS welcomes its formalisation in the Proposal and the fact that while providing for this, the legislator ensured consistency with the systems of supervision of other large-scale IT systems.

81. Recital 34 of the proposal explicitly refers to the monitoring of the lawfulness of data processing activities of Europol by the supervisory authority set up by the Europol Decision. Although the proposal contains specific provisions on supervision when data are processed by Member States or by the Agency (see Articles 31 and 32), the EDPS notes that the text does not contain a similar provision on the supervision of Europol's data processing activities, and recommends addressing this issue.

6.7. Article 34: data security

82. The EDPS has a number of suggestions in respect of Article 34 on data security.
    - Article 34(2)(a) should not refer to general critical infrastructure but to the infrastructure required for the system. We suggest replacing "critical" by *"relevant"*
    - In Article 34(2)(f) the term "confidential access modes only" should be clarified.
    - In Article 34(2)(g) the EDPS recommend adding *"make their profiles and any other relevant information the authorities require for the purposes of carrying out supervision available"*. The EDPS also recommends adding an explicit reference to Article 28 of Directive 95/46/EC as the requirements about data security provided for in Article 34 apply to transmission of data are performed for facilitating the application of Dublin Regulation, as well as to transmission for law enforcement purposes.
    - In Article 34(2)(i) it should be ensured that the logs, as well as the data they refer to, are protected.
    - In order to ensure the monitoring of the effectiveness of the security measures, the EDPS recommends including in Article 34(2)(k) not only auditing (i.e. providing a picture of the situation at a given point in time), but also near real-time observation of the system using specialised tools.
    - Article 34 should also mention the Business Continuity Plan[67]. As regards security incidents, it should also include:
        - the necessity for Member States to inform the Agency of security incidents they detected on their system;
        - the necessity for the Agency to inform all stakeholders in case of security incidents;
        - the necessity for all parties to collaborate during a security incident;
        - the necessity to inform the national supervisory authorities and the EDPS.

[67] See paras 72-73 above.

6.8. Article 40: self-audit and annual report

83. Under Article 40(1), the Agency shall submit to the European Parliament and the Council an annual report on the activities of the Central System. The EDPS asks also to be included for the submission of the Agency's annual report.

84. Furthermore, Article 40(2) of the proposal provides for monitoring procedures. The EDPS takes the view that this monitoring should not only concern the aspects of output, cost-effectiveness and quality of services, but also compliance with legal requirements, especially in the field of data protection. Article 40 (2) should be amended accordingly.

85. In order to perform this self-auditing of the lawfulness of processing, the Commission should be enabled to make use of the records kept in accordance with Article 28 of the proposal. Accordingly, Article 28 should provide that these records shall not only be stored for monitoring data protection and ensuring data security, but also for conducting regular self-auditing of EURODAC. The self auditing reports will contribute to the supervisory task of the EDPS and the other supervisory authorities who will be better able to select their priority areas for supervision.

6.9. Article 43: publication of list of authorities

86. The EDPS welcomes the obligation for the Commission to publish the list of authorities having access to EURODAC data (Article 43). With a view to increase transparency and create an effective and practical tool for better supervision of the system (e.g. by the national DPAs), the EDPS recommends adding an obligation on Member States and Europol to constantly update the information they have provided to the Commission. Furthermore the EDPS recommends requiring that the Commission makes this information available to Member States, Europol and to the public 'via a constantly updated electronic publication'.

7. CONCLUSIONS

87. The EDPS notes that over recent years the need of accessing EURODAC data for law enforcement purposes was extensively debated within the Commission, the Council and the European Parliament. He also understands that the availability of a data base with fingerprints can be a useful additional instrument in the combat of crime. However, the EDPS also recalls that this access to EURODAC has a serious impact on the protection of personal data of the persons whose data are stored in the EURODAC system. To be valid, the necessity of such access 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 intrusion in the rights of individuals constituting a vulnerable group in need of protection, as foreseen in the proposal.

88. Evidence provided until now - also taking into account the specific context described above - is according to the EDPS not sufficient and up to date to demonstrate the necessity and proportionality of granting access to EURODAC

for law enforcement purposes. There are already a number of legal instruments which permit that one Member State consults fingerprints and other law enforcement data held by another Member State. A much better justification, as a precondition for law enforcement access is necessary.

89. In this context the EDPS recommends that the Commission provides a new impact assessment in which all relevant policy options are considered, in which solid evidence and reliable statistics are provided and which includes an assessment in a fundamental rights perspective.

90. The EDPS has identified several additional issues which are:

Applicable data protection law

91. The EDPS stresses the need for clarity on how the provisions of the Proposal specifying certain data protection rights and obligations relate to Council Framework Decision 2008/977/JHA as well as Council Decision 2009/371/JHA (see section 4).

Conditions for law enforcement access

As stated above, it should first be demonstrated that law enforcement access to EURODAC as such is necessary and proportionate. The comments made below should then be taken into account.

92. The EDPS recommends:

- clarifying that the transfer of EURODAC data to third countries is prohibited also in case of use of EURODAC data for law enforcement purposes (see points 43-44);
- adding the law enforcement purposes to the information communicated to the data subject (see point 45);
- ensuring unequivocally that access by designated authorities to EURODAC data is limited to law enforcement purposes (see point 49);
- submitting the access to EURODAC data for law enforcement purposes to a prior judicial authorisation or as a minimum providing that the verifying authority shall perform its duties and tasks independently and shall not receive instructions as regards the exercise of the verification (see points 50-51);
- adding the criterion of the 'need to prevent an imminent danger associated with serious criminal or terrorist offences' as exceptional case justifying the consultation of EURODAC data without prior verification by the verifying authority and introducing a concrete time limit for the ex-post verification (see points 53-54);
- as regards the conditions of access, adding the conditions of (i) a prior consultation of the Visa Information System, (ii) a 'substantiated suspicion that the perpetrator of a terrorist or other serious criminal offences has applied for asylum' and (iii) the 'substantial' contribution for law enforcement purposes and clarifying what is understood by 'reasonable grounds' (see points 56-57);
- describing in a recital the kind of situations justifying a *direct* access by Europol to the EURODAC Central Unit and providing that the strict conditions of access

applying to national designated authorities also apply to Europol (see points 58-59);
- ensuring that comparison of fingerprints for law enforcement purposes shall in any case be subject to at least the same safeguards foreseen for Dublin Regulation purposes (see point 62);
- specifying more clearly the rules on retention or deletion of data (see point 64);
- clarifying which additional information to the 'hit' will be communicated to EUROPOL if applicable (see points 65-66);
- specifying the precise purpose(s) of the request by the Agency's Management Board of the comparisons with EURODAC data by Member State's law enforcement authorities as well as the anonymisation by law enforcement authorities of the data prior to their transmission to the Management Board and restoring the rules on professional secrecies (see points 67-68);
- providing an access for the EDPS and Europol's supervisory authority to the records kept by the Agency and Europol respectively as well as the obligation to store records also for conducting regular self-auditing of EURODAC (see points 79 and 85);
- clarifying the supervision of Europol's data processing activities (see point 81).

Other provisions

93. The EDPS recommends:

- replacing the Business Continuity System by the need for a Business Continuity Plan and providing a legal basis for implementing measures containing the modalities of such plan (see point 72);
- ensuring that temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual and shall in any case represent sufficient grounds to refuse to examine or to reject an asylum application (see point 73);
- ensure consistency between the obligations of the Agency, the Member States and Europol to keep records and documentation of data processing activities (see point 77);
- improving provisions on data security (see point 82);
- including the EDPS for the submission of the Agency's annual report (see point 83);
- adding in Article 43 an obligation on Member States and Europol to constantly update the information they have provided to the Commission and requiring that the Commission makes this information available to Member States, Europol and to the public 'via a constantly updated electronic publication' (see point 86).

Done in Brussels, 5 September 2012

(**signed**)

Peter HUSTINX
European Data Protection Supervisor