Opinion of the European Data Protection Supervisor

- on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and
- on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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 the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 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, sent to the EDPS on 11 August 2009[2],

HAS ADOPTED THE FOLLOWING OPINION

I. Introduction - context of the Opinion

Description of the proposals

1. On 24 June 2009, the Commission adopted a legal package establishing an agency for the operational management of large-scale IT systems in the area of freedom, security and justice. The package consists of a proposal for a Regulation of the European Parliament and of the Council establishing the Agency and a proposal for a Council Decision conferring upon the Agency tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty.[3] The two proposals are further explained in a communication adopted on the same date.[4] On 11 August 2009,

1 OJ 1995, L 281/31.
2 OJ 2001, L 8/1.
3 See COM(2009)293 final and COM(2009)294 final.
4 See COM(2009)292 final.

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

the proposals and the communication were sent to the EDPS for consultation together with the Impact Assessment and the summary of the Impact Assessment.[5]

2. The proposed Regulation finds its legal basis in Title IV of the EC Treaty. Since the use of SIS II and VIS for the purpose of police and judicial cooperation in criminal matters is currently based on Title VI of the EU Treaty, the proposed Regulation is complemented by a proposal for a Council Decision which is based on Title VI of the EU Treaty.

3. The respective legal instruments establishing SIS II, VIS and Eurodac determine that the Commission is to be responsible for the operational management of these three systems.[6] In case of SIS II and VIS this is only intended for a transitional period, after which a Management Authority is to be responsible for the operational management. In a Joint Statement of 7 June 2007, the European Parliament and the Council invited the Commission to present, following an impact assessment in which alternatives are analysed, the necessary legislative proposals entrusting an agency with the long-term operational management of SIS II and VIS.[7] This invitation has led to the current proposals.

4. The Agency established by the proposed Regulation will indeed be responsible for the operational management of SIS II and VIS, but also for Eurodac and possible other large-scale IT systems. The reference to 'other large-scale IT systems' will be discussed in points 28-31 of this Opinion. According to the preamble of the proposed Regulation, the reasons for putting the three large-scale IT systems, and possible other systems, under the direction of one Agency are to achieve synergies, to benefit from economies of scale, to create critical mass and to ensure the highest possible utilisation rate of capital and human resources.[8]

5. The proposed Regulation establishes a regulatory agency which has legal, administrative and financial autonomy and has legal personality. The Agency will perform the tasks which are conferred on the Management Authority (or the Commission) as described in the legal instruments establishing SIS II, VIS and Eurodac. The Agency shall furthermore monitor research and, upon specific request of the Commission, implement pilot schemes for the development and/or operational management of large-scale IT systems, in application of Title IV of the EC Treaty and possibly the broader area of freedom, security and justice as well (see points 28-31 below).

6. The Agency's administrative and management structure will comprise a Management Board, composed of one representative of each Member State and two representatives of the Commission, an Executive Director, appointed by the Management Board and Advisory Groups, which provide the Management Board with the expertise related to the respective IT systems. At the moment, the proposal foresees three Advisory Groups for SIS II, VIS and Eurodac.

---

5 See SEC/2009/0836 final and SEC/2009/0837 final.

6 See Article 15 of Regulation (EC) No 1987/2006 on SIS II (OJ 2006, L 381/4), Article 26 of Regulation (EC) No 767/2008 on VIS (OJ 2008, L 218/60) and Article 13 of Council Regulation 2725/2000 (OJ 2000, L 316/1).

7 See the Joint Statement of 7 June 2007, which is attached to the Legislative Resolution of the Parliament of 7 June 2007 on the proposed VIS Regulation.

8 See Recital 5 of the proposed Regulation.

7. The proposed Council Decision confers upon the Agency the tasks entrusted to the Management Authority as laid down in Council Decision 2007/533/JHA on SIS II and Council Decision 2008/633/JHA on VIS.[9] The proposed Decision furthermore grants Europol observer status at the meetings of the Management Board of the Agency when a question relating to SIS II or VIS is on the agenda. Europol may also appoint a representative to the SIS II and VIS Advisory Groups.[10] Eurojust equally has observer status and may appoint a representative, but only in relation to SIS II.

EDPS consultation

8. The EDPS welcomes that he is consulted on this matter and recommends that reference to this consultation is made in the recitals of the proposals, as is usually done in legislative texts on which the EDPS has been consulted in accordance with Regulation (EC) No 45/2001.

9. Prior to the adoption of the proposal the EDPS has been informally consulted. The EDPS welcomed this informal consultation and is pleased to see that most of his remarks have been taken into account in the final proposal.

10. Obviously, the EDPS is closely following the developments regarding the creation of the Agency which is supposed to become responsible for the proper operation and security of databases, such as SIS II, VIS and Eurodac, which contain large amounts of personal data. As will be further explained in this Opinion, the EDPS is not opposed to the creation of such an Agency, as long as certain possible risks, which could have great impact on the privacy of individuals, are sufficiently addressed in the founding legislative instrument(s).

11. Before explaining this point of view in greater detail in **Part III** and **part IV**, the EDPS will first analyse in **part II** the impact on the current proposals of the Lisbon Treaty which entered into force on 1 December 2009. In **Part V** the EDPS will provide comments on several specific provisions of both proposals.

II. Impact of the Lisbon Treaty

12. The legal structure of the European Union has changed considerably with the entry into force of the Lisbon Treaty on 1 December 2009. Especially with regard to the area of freedom, security and justice, EU competence has been broadened and legislative procedures have been adjusted. The EDPS has analysed the impact of the changes in the Treaties on the current proposals.

13. The legal bases mentioned in the proposed Regulation are the Articles 62(2)(a), 62(2)(b)(ii), 63(1)(a), 63(3)(b) and 66 of the EC Treaty. The text of these Articles can to a large extent be retraced in the Articles 77(1)(b), 77(2)(b), 77(2)(a), 78(2)(e), 79(2)(c) 74 TFEU. The legislative procedure which should be followed for adopting

[9] OJ 2007, L 205/63 and OJ 2008, L 218/129.

[10] If Europol is granted access to Eurodac after the adoption of the proposed Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (see COM (2009)344 final), it will probably be entitled to the same positions in relation to Eurodac. See on the proposed Council Decision however the critical opinion of the EDPS of 7 October 2009 which is available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-10-07_Access_Eurodac_EN.pdf.

measures on these legal bases will not change, the co-decision procedure was applicable and will still be applicable but is now called the 'ordinary legislative procedure'. The impact of the amended Treaties on the legal basis and the legislative procedure for the proposed Regulation therefore seems to be limited.

14. The Articles on which the proposed Council Decision is currently based are Article 30(1)(a), 30(1)(b) and Article 34(2)(c) of the EU Treaty. In the new Treaties, Article 34 of the EU Treaty has been repealed. Article 30(1)(a) is replaced by Article 87(2)(a) TFEU, which creates the basis for measures concerning the collection, storage and processing, analysis and exchange of relevant information, adopted in accordance with the ordinary legislative procedure. Article 30(1)(b) of the EU Treaty, which deals with operational cooperation between the competent authorities, is replaced by Article 87(3) TFEU which prescribes a special legislative procedure which means that the Council acts unanimously after consulting the European Parliament. Since the two legislative procedures are not compatible with each other, Article 87(2)(a) and Article 87(3) TFEU can no longer form the combined legal basis for the Council Decision. A choice therefore has to be made.

15. The EDPS takes the view that Article 87(2)(a) TFEU could be the sole basis for the proposed measure. It would also be the preferred option since the use of the ordinary legislative procedure implies the full involvement of the European Parliament and ensures democratic legitimacy of the proposal.[11] In that respect it must be underlined that the proposal deals with the establishment of an agency which will be responsible for the protection of personal data, which stems from a fundamental right acknowledged by Article 16 TFEU and Article 8 of the Charter of Fundamental Rights, which has become binding since 1 December 2009.

16. Taking Article 87(2)(a) TFEU as the sole legal basis would furthermore enable the Commission to merge the two current proposals into a single instrument for the establishment of the Agency, a Regulation to be adopted in accordance with the ordinary legislative procedure.

17. The EDPS in any event invites the Commission to clarify this situation at a short notice.

III. The establishment of an agency from a data protection point of view

18. As mentioned above in point 3, the European Parliament and the Council invited the Commission to analyse alternatives and to present the necessary legislative proposals entrusting an agency with the long-term operational management of SIS II and VIS. Eurodac was added by the Commission. In the Impact Assessment the Commission explores five options for the operational management of the three systems:

    - continuation of the current arrangement, namely management by the Commission, which, with regard to SIS II and VIS, includes a delegation of tasks to two Member States (Austria and France);
    - same as the first option, and in addition the delegation of the operational management of Eurodac to Member States' authorities;
    - setting up of a new regulatory agency;

[11] In the so-called Titanium Dioxide judgement, the ECJ attached particular weight to the participation of the European Parliament in the decision making process, see ECJ 11 June 1991, *Commission v. Council*, Case C-300/89, [ECR] 1991, p. I-2867, par. 21.

- handing over operational management to Frontex;
- handing over operational management of SIS II to Europol and continuation of Commission management of VIS and Eurodac.

The Commission analysed these options from four different angles: operational, governance, finance and legal.

19. As part of the legal analysis, the Commission compared how these different structures would allow for the effective safeguarding of fundamental rights and freedoms, and in particular of the protection of personal data. It concluded that option 3 and 4 were the preferable options in that respect.[12] With regard to the first two options the Commission pointed at the possible difficulties regarding the supervision by the EDPS which were discussed during the development of SIS II. In relation to the first two options, the Commission furthermore referred to the problematic situation, in terms of liability stemming from Article 288 of the EC Treaty (now: Article 340 TFEU), if operations were challenged which are carried out by national staff.

20. The EDPS agrees with the Commission that in the perspective of EDPS supervision, it would be preferable to have one European entity which is responsible for the operational management of a large-scale IT system such as SIS II, VIS and Eurodac. The establishment of one single entity would furthermore clarify issues of liability and applicable law. Regulation (EC) No 45/2001 would be applicable to all the activities of such a European entity.

21. The next question, however, is which or what kind of European entity that should be. The Commission discusses the establishment of a new agency and the use of two existing entities, namely Frontex and Europol. There is a strong argument against the operational management of large-scale IT systems by Frontex or Europol, since in the performance of their tasks, Frontex and Europol have their own interest in using personal data. Access by Europol to SIS II and VIS is already foreseen and legislation for access by Europol to Eurodac is currently under discussion.[13] The EDPS takes the view that a preferable option would be one which entrusts the combined operational management of a large-scale database such as SIS II, VIS and Eurodac, to an independent entity which does not have its own interest as user of the database. This diminishes the risk of misuse of data. In that respect, the EDPS would like to point at the basic data protection principle of purpose limitation, which requires that personal data may not be used for purposes which are incompatible with the purpose for which the data were originally processed.[14]

22. One option which is not discussed by the Commission is the operational management of the systems by the Commission itself, without any delegation to the national level. Close to this option is the establishment of an executive agency instead of a regulatory agency. Although there is no point of principle from a data protection point of view against the Commission taking up the task itself (the Commission itself is not the user of these systems) the EDPS sees the practical benefits of a separate agency. The choice for a *regulatory* instead of an *executive* agency can be welcomed as well, as it prevents the agency, and its scope of activities, from being established and determined on the basis of a Commission decision only. The current Agency will be established

12 See the Impact Assessment at page 32.

13 See on the latter the Opinion of the EDPS of 7 October 2009 referred to in footnote 10.

14 See Article 4(1)(b) of Regulation (EC) No 45/2001.

on the basis of a Regulation which is adopted in accordance with the ordinary legislative procedure and is therefore subject to a democratic decision.

23. The EDPS sees the advantages of creating an independent regulatory agency. The EDPS wishes to underline, however, that such an agency should only be established when the scope of its activities and its responsibilities are clearly defined.

IV. Two general concerns regarding the establishment of the Agency

24. During the current legislative and public debate on this proposal, concerns have been voiced about the possible creation of a 'big brother agency'. This statement relates to the possibility of function creep, but also to the issue of interoperability of the different IT systems. These two concerns will be addressed in this part of the Opinion.

25. Before doing so, the EDPS would like to pose - as a basic assumption - that the risk of mistakes or wrongful use of personal data may increase when more large-scale IT systems are entrusted to the same operational manager. The total number of large-scale IT systems managed by one and the same Agency should therefore be restricted to a number with which the data protection safeguards can still sufficiently be assured. In other words, the point of departure should not be to bring as many large-scale IT-systems as possible under the operational management of one Agency.

IV.1. Function creep

26. In the present context the fear of function creep refers to the idea that the new Agency will be able to create and combine on its own motion the already existing and new large-scale IT systems to an extent which is unforeseen at the moment. The EDPS is of the opinion that function creep by the Agency can be avoided if, first, the scope of (possible) activities of the Agency is limited and clearly defined in the founding legal instrument and, second, if it is ensured that any expansion of this scope will be based on a democratic decision making procedure, which normally is the ordinary legislative procedure.

27. As to the limitation of the scope of (possible) activities of the Agency the current proposal refers in Article 1 to the operational management of SIS II, VIS and Eurodac, as well as to 'developing and managing other large-scale [IT] systems, in application of Title IV of the EC Treaty'. In terms of determination of scope, this last part raises three questions: what is meant by 'developing', what is meant by 'large-scale IT systems' and what is the meaning of the phrase after the comma? These three questions will be dealt with below in reverse order.

What is the meaning of the phrase 'in application of Title IV of the EC Treaty'?

28. The phrase 'in application of Title IV of the EC Treaty' puts a limitation to the large-scale IT systems which can be brought under the responsibility of the Agency. The EDPS notices, however, that this phrase implies a more limited scope of possible activities than can be derived from the title of the proposed Regulation, Recital 4 and Recital 10. Those texts differ from Article 1 in the sense that they have a broader scope: they refer to the 'area of freedom, security and justice' instead of the more limited field of competence as laid down in Title IV of the EC Treaty (visas, asylum, immigration and other policies related to the free movement of persons).

29. The distinction between Title IV of the EC Treaty and the broader notion of the area of freedom, security and justice (which also encompasses Title VI of the EU Treaty) is recognised in Article 6 of the proposed Regulation, which deals in paragraph 1 with the possibility for the Agency to implement pilot schemes for the development and/or operational management of large-scale IT systems, *in application of Title IV of the EC Treaty,* and in paragraph 2 with the possibility that pilot schemes related to other large-scale IT systems are implemented by the Agency *in the area of freedom, security and justice*. Article 6(2) is strictly speaking not in conformity with Article 1 of the proposed Regulation.

30. The contradiction between Article 1 and the title of the proposed Regulation, as well as Recitals 4 and 10 and Article 6(2) has to be solved. With reference to the basic assumption made in point 25 above, the EDPS is of the opinion that at this stage it would be recommended to indeed limit the area of competence to large-scale IT systems in application of Title IV of the EC Treaty. Since 1 December 2009, with the entry into force of the Lisbon Treaty, this would imply a limitation to the policy fields mentioned in Chapter 2 of Title V of the TFEU. After having acquired experience and after a positive evaluation of the functioning of the Agency (see Article 27 of the proposal, and the comments in point 49 below) the reference in Article 1 could perhaps be broadened to cover the whole area of freedom, security and justice, as long as such a decision is based on the ordinary legislative procedure.

31. Should the legislator, however, decide to opt for a scope as can be derived from the title and Recitals 4 and 10, then another issue regarding Article 6(2) should be clarified. Contrary to the first paragraph of Article 6, the second paragraph does not specify that the implementation of the pilot scheme is for the *development and or operational management* of large-scale IT systems. The deliberate distinction between the two paragraphs and the absence of the additional phrase in the second paragraph raises the question what the Commission actually tried to establish. Does it mean that the pilot schemes referred to in the first paragraph should include an assessment of the possible development and operational management by the new Agency, and that such an assessment is not part of the pilot schemes in the second paragraph? If that is the case, then it should be better clarified in the text because a deletion of the specification does not exclude the implementation and operational management of such systems by the agency. If the Commission meant something else it should be clarified as well.

What is a large-scale IT system?

32. The notion of 'large-scale IT systems' is a rather disputable one. There is not always a common understanding of which systems must be considered as large-scale IT systems and which should not. The interpretation of the notion has important implications for the scope of possible future activities of the Agency. The three large-scale IT systems which are explicitly mentioned in the proposal have as a common feature the storage of data in a centralised database for which the Commission is (currently) responsible. It is not clear whether the possible future activities of the Agency are limited to large-scale IT systems with such a characteristic, or whether it might also include decentralised systems whereby the Commission's responsibility is limited to the development and maintenance of the common infrastructure of such a system, such as the Prüm system and the European Criminal Records Information

System (ECRIS).[15] In order to prevent any future misunderstanding, the EDPS invites the legislator to clarify the notion of large-scale IT systems in relation to the establishment of the Agency.

What is meant by 'developing' large-scale IT systems?

33. Next to the operational management of large-scale IT systems, the Agency will also perform the tasks laid down in Article 5 (monitoring of research) and Article 6 (pilot schemes). The first implies the monitoring of relevant research and the reporting thereof to the Commission. Activities in relation to the pilot schemes are the implementation of pilot schemes for the development and/or operational management of large-scale IT systems (see, however, the comments in point 31 above). Article 6 defines how the word 'development' should be understood. The use of the word in Article 1 triggers the idea that the Agency could be responsible for the development of large-scale IT systems on its own motion. This, however, is excluded by the wording of Article 6(1) and (2). It is clearly stated that the Agency may do so '[u]pon specific and precise request of the Commission'. In other words, the initiative for the development of new large-scale IT systems lies with the Commission. Any decision to actually establish a new large-scale IT system should of course be based on the legislative procedures foreseen in the TFEU. To make the wording of Article 6 of the proposed Regulation even stronger, the legislator could decide to add the word 'only' at the start of Article 6(1) and (2).

To sum up

34. As stated, the risk of function creep can be avoided if, first, the scope of (possible) activities of the Agency is limited and clearly defined in the founding legal instrument and, second, if it is ensured that any expansion of this scope will be based on a democratic decision making procedure, which normally is the ordinary legislative procedure. The current text already contains specifications which limit the risk of function creep.

35. However, some uncertainties remain with regards to the precise scope of possible activities of the new Agency. The legislator should, in the first place, clarify and consciously decide whether the scope of activities is limited to Chapter 2 of Title V of the TFEU, or whether it potentially should cover all large-scale IT systems developed in the area of freedom, security and justice. The legislator should, in the second place, clarify the notion of large-scale IT systems within this framework, and make clear whether it is limited to large-scale IT systems which have as a feature the storage of data in a centralised database for which the Commission or the Agency is responsible. In the third place, although Article 6 already prevents the development of new IT systems by the Agency on its own motion, the text of Article 6 could be made even stronger by adding the word 'only' to paragraphs 1 and 2, if the latter is upheld.

IV.2. Interoperability

15 See for the Prüm-system Council Decisions 2008/615/JHA and 2008/616/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ 2008, L 210/01) and the Opinions of the EDPS of 4 April 2007 (OJ 2007 C 169/2) and 19 December 2007 (OJ 2008, C 89/1). And for ECRIS Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) (OJ 2009, L 93/33) and the Opinion of the EDPS of 16 September 2008 (OJ 2009, C 42/1).

36. The notion of 'interoperability' is not unambiguous. The EDPS came to this conclusion in his comments of 10 March 2006 on the Communication of the Commission on interoperability of European databases.[16] With regard to the new Agency, the notion of interoperability must be understood as including the risk that by putting several large-scale IT systems under the operational management of one Agency, similar technology will be used for all systems which can therefore easily be interconnected. In general, the EDPS endorses this concern. In his comments of 10 March 2006, the EDPS stated that making it technically feasible to interconnect different large-scale IT systems, constitutes a powerful drive to actually do so. It is a strong reason to once more emphasise the importance of the data protection rules. The EDPS therefore underlined that interoperability of large-scale IT systems can *only* be made possible with full respect for data protection principles and in particular with full respect to the earlier mentioned purpose limitation principle (see point 21 above).

37. The possible encouragement to make large-scale IT systems interoperable if technology is used which can easily interconnect is, however, not necessarily related to the establishment of a new Agency. Also without such an agency systems might be developed in similar ways which could trigger interoperability.

38. Whatever operational management structure is chosen, interoperability may only be made possible if it is in conformity with data protection rules and the actual decision to do so is based on an ordinary legislative procedure. It is clear from the proposed Regulation that the decision to make large-scale IT systems interoperable is not a decision which can be taken by the Agency (see also the analysis in point 33 above). To put it even stronger, as also follows from the Commission Communication on European agencies of 11 March 2008, the Commission is not allowed to delegate the power to adopt such a general regulatory measure to an agency.[17] As long as such a decision is not taken, the Agency is obliged to put into place proper security measures in order *to prevent* any possible interconnection of the large-scale IT systems it manages (see on security measures also points 46 and 47).

39. Interoperability (envisaged or possibly envisaged in the future) could be part of the request of the Commission to the Agency to implement a pilot scheme for the development of new large-scale IT systems, as described in Article 6 of the proposed Regulation. It triggers the question what procedure the Commission will follow for asking the Agency for such a pilot scheme. The request of the Commission should in any event be based on at least a preliminary assessment of whether the large-scale IT system as such, and the interoperability in particular, would be in conformity with the data protection requirements and more generally with the legal basis creating these systems. Furthermore, a compulsory consultation of the European Parliament and the EDPS could be part of the procedure leading to the request. The actual request of the Commission to the Agency should in any case be made accessible to all relevant stakeholders, including the Parliament and the EDPS. The EDPS urges the legislator to clarify this procedure.

V. Specific comments

[16] Comments of the EDPS of 10 March 2006, to be found at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf.

[17] COM(2008)135 final, p. 5.

Recital 16 and Article 25 of the proposed Regulation: references to Regulation (EC) 45/2001

40. The proposed Regulation establishes an independent regulatory agency having legal personality. In Recital 6 of the proposed Regulation it is stated that such an agency will be established since the Management Authority should have legal, administrative and financial autonomy. As already stated in point 20 above the establishment of one single entity clarifies issues of liability and applicable law.

41. Article 25 of the proposed Regulation confirms that the processing of information by the new Agency is subject to Regulation (EC) No 45/2001. Recital 16 furthermore highlights that this means that the EDPS shall have the power to obtain from the Agency access to all information necessary for his or her enquiries.

42. The EDPS is pleased to see that the applicability of Regulation (EC) No 45/2001 to the activities of the new Agency is underlined in such a way. Reference to Regulation (EC) No 45/2001 is missing in the proposed Council Decision, although it is clear that the Agency will also be bound by the provisions of that Regulation when the database is used for activities which fall under judicial and police cooperation in criminal matters. With the entry into force of the Lisbon Treaty, and should the legislator decide to uphold the division among two legal instruments (see the comments in **Part II** above), there is no reason against a reference to Regulation (EC) No 45/2001 in the recitals and/or provisions of the Council Decision as well.

Article 9(1)(o) of the proposed Regulation: the Data Protection Officer

43. The EDPS is also pleased to see that the appointment of a Data Protection Officer (DPO) is made explicit in Article 9(1)(o) of the proposed Regulation. The EDPS wishes to emphasise the importance of appointing a DPO at an early stage, taking into account the EDPS position paper on DPOs.[18]

Article 9(1)(i) and (j) of the proposed Regulation: annual working programme and activity report

44. On the basis of Regulation (EC) No 45/2001, and through legal instruments establishing the IT systems, the EDPS has supervisory powers over the Agency. These powers, which are listed in Article 47 of Regulation (EC) No 45/2001, are mostly invoked when a breach of data protection rules has already occurred. The EDPS takes an interest in being regularly informed, not only afterwards but also beforehand, about the activities of the Agency. Currently the EDPS has developed a practice with the Commission which satisfies this interest. The EDPS expresses the hope that such a satisfactory cooperation will also be achieved with the newly established Agency. In the light of this, the EDPS recommends the legislator to include the EDPS in the list of recipients of the annual work programme and the annual activity report, as regulated in Article 9(1)(i) and (j) of the proposed Regulation.

Article 9(1)(r) of the proposed Regulation: audits by the EDPS

45. Article 9(1)(r) of the proposed Regulation deals with the EDPS' report about the audit pursuant to Article 45 of Regulation (EC) No 1987/2006 on SIS II and Article 42(2) of

[18] Position Paper of the EDPS of 28 November 2005, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf.

Regulation (EC) No 767/2008 on VIS. The current wording gives the impression that the Agency has total discretion as to the follow-up of the audit including the possibility not to follow recommendations at all. Although the Agency can make comments on the report and will be free as to how to implement the recommendations of the EDPS, not following the recommendations at all is no option. The EDPS therefore suggests either deleting this Article or replacing the phrase 'and decide on the follow-up of the audit' by: 'and decide on how to implement the recommendations in the most appropriate way following the audit'.

Article 9(1)(n), Article 14(6)(g) and Article 26 of the proposed Regulation: rules on security

46. The proposed Regulation states that the Executive Director shall submit to the Management Board for adoption, the draft for the necessary security measures including a security plan (see Article 14(6)(g) and Article 9(1)(n)). Security is also mentioned in Article 26 which deals with the security rules on the protection of classified information and non-classified sensitive information. Reference is made to Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 and in the second paragraph to the security principles relating to the processing of non-classified sensitive information as adopted and implemented by the European Commission. Apart from the comments to follow in the next point, the EDPS recommends the legislator to include a reference to specific documentation in the second paragraph as well since the paragraph is rather vague as it stands now.

47. The EDPS wishes to point at the fact that the legal instruments underlying SIS II, VIS and Eurodac contain detailed provisions regarding security. It is not self evident that these specific rules are completely similar or fully compatible with the rules referred to in Article 26. Since the highest level of security should be ensured by the security plan, the EDPS recommends the legislator to change Article 26 into a broader provision which addresses the issue of security rules in a more general way and include references to the relevant provisions of the legal instruments concerning the three large-scale IT systems. This should be preceded by an assessment of how far the rules referred to are similar and compatible with each other. A link should furthermore be established between this broader provision and Article 14(6)(g) and Article 9(1)(n) which deal with the drafting and adoption of security measures and a security plan.

Article 7(4) and 19 of the proposed Regulation: the accommodation of the Agency

48. The EDPS is conscious of the fact that the decision on the seat of the Agency, as foreseen in Article 7(4), is to a large extent a political one. Still, the EDPS recommends that, in light of Article 19 which deals with the headquarters Agreement, the choice of seat will be based on objective criteria such as the accommodation available, which should be a single building dedicated to the Agency only, and the possibilities to ensure the security of the building.

Article 27 of the proposed Regulation: evaluation

49. Article 27 of the proposed Regulation determines that within three years from the date on which the Agency takes up its responsibilities and every five years thereafter, the Management Board shall commission an independent external evaluation on the basis of terms of reference issued by the Management Board after consultation of the Commission. In order to ensure that data protection is part of these terms of reference, the EDPS recommends the legislator to make explicit reference to this in the first

paragraph. The EDPS furthermore invites the legislator to specify in a non-limitative way the stakeholders referred to in the second paragraph and include the EDPS. The EDPS recommends the legislator also to include the EDPS in the list of institutions which receive the documents referred to in the third paragraph.

VI. Conclusion and recommendations

50. As a preliminary matter, the EDPS points at the impossibility of basing the proposed Council Decision on the two articles of the TFEU which are the successors of the articles of the EU Treaty on which the proposal is currently based. The EDPS invites the Commission to clarify the situation and to consider using as a legal basis the article which grants most power to the European Parliament and to consider merging the two proposals into one Regulation.

51. The EDPS has analysed the different options for the operational management of SIS II, VIS and Eurodac, and sees the advantages of creating a regulatory agency for the operational management of certain large-scale IT systems. The EDPS underlines, however, that such an agency should only be established if the scope of its activities and its responsibilities are clearly defined.

52. The EDPS discussed two general concerns regarding the establishment of an agency with data protection relevance: the risk of function creep and the consequences for the interoperability of the systems.

53. The EDPS takes the view that the risk of function creep can be avoided if, first, the scope of (possible) activities of the Agency is limited and clearly defined in the founding legal instrument and, second, it is ensured that any expansion of this scope will be based on a democratic decision making procedure. The EDPS notes that the current proposals already contain such specifications but that some uncertainties remain. The EDPS therefore recommends the legislator:

    - to clarify and consciously decide whether the scope of activities of the Agency is limited to Chapter 2 of Title V of the TFEU, or whether it potentially should cover all large-scale IT systems developed in the area of freedom, security and justice;
    - to clarify the notion of large-scale IT systems in relation to the establishment of the Agency, and make clear whether it is limited to such systems which have as a feature the storage of data in a centralised database for which the Commission or the Agency is responsible;
    - to make the text of Article 6 even stronger by adding the word 'only' to paragraphs 1 and 2, if the latter is upheld.

54. In general, the EDPS is concerned about ambiguities in the developments regarding possible interoperability of large-scale IT systems. The EDPS, however, does not consider the establishment of the Agency as the most threatening factor in that respect. The EDPS noticed that the Agency will not be able to decide on interoperability on its own motion. The EDPS encourages the legislator, in the context of the proposed pilot schemes, to clarify the procedure which the Commission should follow before requesting for a pilot scheme. According to the EDPS, such a procedure should include an assessment, which might require a consultation of the European Parliament and the EDPS, of the possible impact on data protection of the initiative developed following such a request.

55. The EDPS furthermore makes the following specific recommendations:

- to include the EDPS in the list of recipients of the annual work programme and the annual activity report, as regulated in Article 9(1)(i) and (j) of the proposed Regulation;
- to either delete Article 9(1)(r) of the proposed Regulation or replace the phrase 'and decide on the follow-up of the audit' by: 'and decide on how to implement the recommendations in the most appropriate way following the audit';
- to change Article 26 of the proposed Regulation into a provision which addresses the issue of security rules in a more general way and which includes references to the relevant provisions of the legal instruments concerning the three large-scale IT systems and to establish a link between this broader provision and Article 14(6)(g) and Article 9(1)(n) of the proposed Regulation;
- in relation to the previous point, to include a reference to specific documentation in Article 26(2) of the proposed Regulation;
- to take into account objective, practical, criteria when the seat of the agency is chosen;
- to include the EDPS in the list of institutions which receive the documents referred to in Article 27(3) of the proposed Regulation.

Done in Brussels, 7 December 2009

(signed)

Peter HUSTINX
European Data Protection Supervisor