Opinion of the European Data Protection Supervisor

on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)

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 the request for an Opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

I.1. Consultation of the EDPS

1. On 28 February 2013 the Commission adopted the following proposals (hereinafter: "the proposals"):
   - Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union (hereinafter: "the EES proposal")[3];
   - Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme (RTP) (hereinafter: "the RTP proposal")[4] ;

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.01.2001, p. 1.
[3] COM(2013) 95 final.
[4] COM(2013) 97 final.

- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP) (hereinafter: "the amending proposal")[5].

2. On the same day, the proposals were sent to the EDPS for consultation. The EDPS had been given the opportunity to provide informal comments to the Commission before the adoption of the proposals.

3. The EDPS welcomes the reference to the consultation of the EDPS which has been included in the Preamble of both the EES proposal and the RTP proposal.

I.2. Background

4. The 2008 Commission's Communication "Preparing the next steps in border management in the European Union" suggested new tools for the future management of European borders, including an entry/exit system (hereinafter "EES") for the electronic recording of the dates of entry and exit of third country nationals and a registered traveller programme to facilitate border crossing for bona fide travellers (hereinafter "RTP"). It also considered the introduction of an Electronic System of Travel Authorisation (ESTA) for visa-exempted third country nationals.

5. These proposals were endorsed by the European Council of December 2009 in the Stockholm Programme[6]. However, in its 2011 Communication on smart borders, the Commission[7] considered that the establishment of an ESTA should be discarded for the moment as "the potential contribution to enhancing the security of the Member States would neither justify the collection of personal data at such a scale nor the financial cost and the impact on international relations."[8] It further announced that it intended to present proposals for an EES and an RTP in the first half of 2012.

6. Subsequently, the European Council of June 2011 requested that the work on "smart borders" be pushed forward rapidly and asked for the introduction of the EES and the RTP[9].

[5] COM(2013) 96 final.
[6] "An open and secure Europe serving and protecting the citizens", Official Journal of the European Union of 4.5.2010, C 115/1.
[7] Communication of 25 October 2011 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on "Smart borders - options and the way ahead" (COM(2011) 680 final).
[8] Communication from the Commission on smart borders, cited above, p.7.
[9] EUCO 23/11.

7. The Article 29 Working Party commented on the Communication from the Commission on smart borders, which preceded the Proposals, in a letter to Commissioner Malmström of 12 June 2012[10]. More recently, on 6 June 2013, the Working Party adopted an opinion questioning the necessity of the Smart Borders package[11].

8. The present Opinion builds on these positions, as well as on a previous EDPS Opinion[12] on the 2011 Commission's Communication on migration[13] and on the EDPS Preliminary comments[14]on three Communications on border management (2008)[15]. It also uses input given in the EDPS Round Table on the Smart borders package and data protection implications.[16]

I.3. Aim of the Proposals

9. Article 4 of the EES proposal specifies its purpose. The proposal aims at improving the management of the EU external borders and the fight against irregular migration, the implementation of the integrated border management policy and the cooperation and consultation between border and immigration authorities. It provides for a system that would:

   a. enhance checks at external border crossing points and combat irregular immigration;
   b. calculate and monitor the calculation of the duration of the authorised stay of third-country nationals admitted for a short stay;
   c. assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, or stay on the territory of the Member States;

[10] The Article 29 Working Party, set up under Directive 95/46/EC, is composed of a representative of every national data protection authority, the EDPS and a representative of the European Commission. It has advisory status and acts independently. The letter of 12 June 2012 of the Working Party to Ms. Cecilia Malmström on smart borders is available on http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120612_letter_to_malmstrom_smart-borders_en.pdf.

[11] Article 29 Working Party, Opinion 05/2013 on Smart Borders**.** http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf

[12] EDPS Opinion of 7 July 2011, available on http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-07-07_Migration_EN.pdf.

[13] Communication of 4 May 2011 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration (COM(2011) 248/3).

[14] EDPS Preliminary comments of 3 March 2008, available on http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

[15] Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Preparing the next steps in border management in the European Union" (COM(2008) 69 final); "Examining the creation of a European Border Surveillance System (EUROSUR)" (COM(2008) 68 final); and "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final.

[16] EDPS Round Table on the Smart borders package and data protection implications, Brussels, 10 April 2013, Venue: EDPS Building, Rue Montoyer 30, Brussels. See summary at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/2013/13-04-10_Summary_smart_borders_final_EN.pdf

d. enable national authorities of the Member States to identify overstayers and take appropriate measures;
e. gather statistics on the entries and exits of third country nationals for the purpose of analysis.

10. The system should help monitoring the authorised stay by providing quick and precise information to border guards and to travellers. It would replace the current system of manual stamping of passports, which is considered slow and unreliable and improve the efficiency of border management[17].

11. It should also assist, through the storing of biometrics, in the identification of persons who do not fulfil the conditions for entry to, or stay in the EU, especially in the absence of identification documents. In addition, the EES would provide a precise picture of travel flows and of the number of overstayers, allowing evidence-based policy making, for example on visa obligations. The statistics mentioned in Article 4 are used for this last aim.

12. The EES would be the basis for the RTP, aimed at facilitating border crossings to pre-vetted, frequent third country travellers. Registered travellers would have a token with a unique identifier to be swiped on arrival and departure at the border through an automated gate. The data of the token, the fingerprints and, if applicable, the visa sticker number would be compared to the ones stored in the Central Repository and other databases. If all checks are successful, the traveller would be able to cross the automated gate. Otherwise, a border guard would assist the traveller.

13. Finally, the amending proposal has the objective of accommodating Regulation (EC) No 562/2006 establishing a Community Code on the rules governing the movement of persons across borders (hereinafter: "the Schengen Borders Code") to the new EES and RTP proposals.

I.4. Context and structure of the present Opinion

14. The project to develop an electronic system to control entries and exits to the EU territory is not new, and several Communications of the Commission mentioned above have paved the way for the proposals now under analysis. It is therefore in the perspective of these developments that the smart border package should be assessed. In particular, the following elements need to be taken into account.

15. In the Stockholm programme, the Commission has taken the strategic approach of assessing the need for developing a European Information Exchange Model based on the evaluation of current instruments. This shall be based, amongst others, on a strong data protection regime, a well targeted data collection scheme, and a rationalisation of the different tools, including the adoption of a business plan for large IT systems. The Stockholm Programme recalls the need to ensure consistency of the implementation and management of the different information tools with

[17] See the Explanatory Memorandum of the EES proposal.

the strategy for the protection of personal data and the business plan for setting up large scale IT systems[18].

16. A comprehensive analysis is all the more needed considering the existence and further development and implementation of large scale IT systems, such as Eurodac[19], VIS[20] and SIS II[21]. A smart borders scheme is an additional tool to collect massive amounts of personal data in a border control perspective. This global approach has been confirmed recently by the JHA Council which emphasised the need to learn from the experience of SIS by reference in particular to the escalation of costs.[22] The EDPS has also commented that 'a European information model may not be construed on the basis of technical considerations', in view of the almost limitless opportunities offered by new technologies. Information should be processed only on the basis of concrete security needs[23].

17. The analysis of the EES and the RTP from a privacy and data protection angle must be done in the perspective of the Charter of Fundamental Rights of the European Union[24] (hereinafter: "the Charter"), and in particular its Articles 7 and 8. Article 7, which is similar to Article 8 of the European Convention on Human Rights[25] (ECHR), provides for a general right to respect for private and family life, and protects the individual against interference by public authorities, while Article 8 of the Charter gives the individual the right that his or her personal can only be processed under certain specified conditions. The two approaches are different and complementary. The smart borders package will be assessed against these two perspectives.

---

[18] The Stockholm Programme - an open and secure Europe serving and protecting citizens, O.J. 2010/C 115/01

[19] See Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison 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, OJ L 180, 29.6.2013.

[20] See Regulation (EC) No 767/2008 of the European Parliament and of 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, 13.8.2008.

[21] See 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), OJ L 381/4, 28.12.2006.

[22] See Council doc. nr. 8018/13, Note of the Presidency to the Strategic Committee on Immigration, Frontiers and Asylum/Mixed Committee (UE-Iceland/Liechtenstein/Norway/Switzerland), 28 March 2013 on Smart Border Package.
http://www.statewatch.org/news/2013/apr/eu-council-smart-borders-8018-13.pdf

[23] EDPS Opinion of 10 July 2009 on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen, O.J. 2009/C 276/02.

[24] OJ C 83, 30.03.2010, p.389.

[25] Council of Europe, ETS No 5, 4.11.1950.

18. The present Opinion has a strong focus on the EES proposal - which is most relevant from the perspectives of privacy and data protection - and is structured as follows:

- Section II contains a general assessment of the Entry/Exit System, focusing on compliance with both Articles 7 and 8 of the Charter;
- Section III contains comments on more specific provisions of the EES concerning the processing of biometric data and access by law enforcement authorities;
- Section IV includes comments on other issues raised by the EES;
- Section V focuses on the RTP;
- Section VI refers to the need for additional data security safeguards;
- Section VII lists the conclusions.

II. GENERAL ASSESSMENT OF THE EES

II.1. Article 7 of the Charter: Respect for private and family life

19. According to Article 7 of the Charter, 'everyone has the right to respect for his or her private and family life, home and communications'. Any limitation to this right (just as in the case of Article 8) must comply with Article 52(1) of the Charter, and must therefore be provided by law, respect the essence of the rights and freedoms recognised by the Charter, be proportionate and necessary, and "genuinely meet the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

20. Article 7 of the Charter should be read in combination with Article 8 of the ECHR which protects private and family life in the same terms and adds that "there shall be no interference by a public authority with the exercise of this right except such as is *in accordance with the law* and is *necessary in a democratic society*" for certain purposes[26].

21. The principle of proportionality is closely related to the principle of necessity. According to the European Court of Human Rights (ECtHR), an interference to a right can be considered necessary if it is proportionate to the aim pursued, answers a pressing social need, and the reasons put forward by the public authority to justify it are relevant and sufficient[27]. The Court of Justice of the European Union has further specified that it should be demonstrated that the same purposes cannot be achieved with less intrusive means[28].

[26] I.e., "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (See Article 8(2)ECHR).
[27] See ECtHR, Marper v. United Kingdom, 4 December 2008, applications no. 30562/04 and 30566/04
[28] See CJEU, C-92/09 Volker and Markus Schecke GbR v. Land Hessen and C-93/09 Eifert v. Land Hessen and Bundesanstalt für Landwirtschaft und Ernährung, 9.11.10.

Does EES constitute an interference, and to what extent?

22. It is evident that the routine storage of data on individuals relating to their entry to and exit from the territory of the European Union will often and in many different ways also reveal information about their private and family life. The jurisprudence of the ECtHR recalls that "the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 of the ECHR"[29]. To assess the degree of interference, several aspects can be taken into account, such as the nature of the data, the scale of data collection, the further use and possible change of purpose (for instance the retention of telecommunications data for commercial purposes and their further use by law enforcement authorities), the transfer to third countries (for instance the systematic transfer of passenger name records) or the secret character of the collection and processing (see for instance the conclusions of the ECtHR in the cases Amann and Rotaru[30]).

23. A key element to take into account is the nature of the personal data, and in particular their sensitivity. The collection of biometric data for instance constitutes a clear interference, as stated by the ECtHR in the Marper[31] case, which should be considered quite apart from the general issue of information about a person's private and family life. The fact that the information collected does not relate to persons who are suspected of unlawful conduct or otherwise under investigation is an additional element of interference.

24. With regard to the EES, the EDPS notes that the processing happens on a wide scale as it concerns all short stay visitors to the EU, which are non-suspect travellers, and entails the collection of identification data including biometrics (10 fingerprints) on those visitors. Law enforcement access is also a possibility envisaged and the system has been designed to allow for it. It must therefore be concluded that the proposals imply an interference with the right to respect for private and family life, with possibly wide implications for the individuals concerned.

Is the interference provided for by a clear legal basis?

25. The language of the law has to be sufficiently clear to make interferences foreseeable. The circumstances under which the right to private life, family life, home or correspondence may be limited have to be precisely indicated in the legal basis[32].

26. This is the object of the EES proposal, which aims at providing for a clear framework for the collection, use and storage of third country nationals' data, as well as for their rights of information, access and rectification. However, the purposes of the proposal should be defined better and additional safeguards should be added, as will be developed below.

[29] *Idem*, para. 67.
[30] See ECtHR, Rotaru v. Romania, 4 May 2000, application no. 28341/95; and Amann v. Switzerland, 16 February 2000, application no. 27798/95.
[31] *Op. cit.*
[32] See ECtHR, Kruslin v France, application no. 11801/85, para 30 – 3.

Is the measure necessary and proportionate in a democratic society for any of the purposes listed in Article 8(2) ECHR or Article 52(1) Charter[33]?

27. Paragraph 9 of this opinion shows that the proposal has different, not well defined, but in any event closely linked, purposes, with an emphasis on border management and better dealing with illegal stay. The assessment under Article 7 should take account of these purposes.

28. In the first place, the EDPS considers that, in principle, large scale databases are created to support an established EU policy, laid down in Union law. However in this case it appears that the database is created without the existence of a comprehensive policy, and even in order to find out whether and how such an EU policy should be developed. This is of particular concern since the EES is created with the aim of identifying overstayers, but without the establishment of a clear European policy on management of overstayers.

29. The Proposal states that the EES will facilitate calculation of stay and thus identification of overstayers (which is already possible but arguably more difficult on the basis of stamps[34]). One main consequence of identifying the overstayer is the *refusal of a new visa,* when the individual has finally left the EU territory and is coming back. If the overstayer has been found and identified on the EU territory, it is also presented as facilitating *return* to the country of origin. However, if the EES may facilitate *identifying* over-stayers, it does not address their effective *location in the EU territory* and the conditions of return to his or her country of origin[35]. The efficiency of the system in an area with *land borders* remains also unclear[36]. According to the EDPS, these issues should have been addressed as a preliminary condition to the development of this large scale border control scheme.

30. In the second place, a separate purpose seems to be facilitating the calculation of overstay and creating statistics. This purpose could be connected only indirectly with the purposes listed in Article 8(2) ECHR, and can hardly justify an interference with the right to respect for private life. The EDPS therefore questions the necessity and proportionality of the interferences with the right to privacy provided by the Proposal in relation the purposes of improving calculation and developing statistics.

[33] I.e.: a general interest recognised by the Union / in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[34] The travel documents of non-EU country nationals are systematically stamped upon entry and exit.If a travel document does not bear an entry stamp, it may be presumed that the holder does not fulfil, or no longer fulfils, the conditions of stay.

[35] On the question if transmission of identification data to the country of origin is the main solution to return issues, especially in the absence of cooperation of the third country, see the Note of the Meijers Committee of 3 May 2013 on the Smart Borders proposals, p. 2.

[36] See the Impact assessment of the Proposal, p. 14 and 15, also commented by the WP29 Opinion, p. 6.

31. In this context, the EDPS questions the need that information be identifiable, and takes the view that anonymous statistical data could lead to the same result[37] and be even more cost-effective. Existing possibilities can be explored in the Schengen Border Code to this purpose[38]. This objective of migration management should also be reconciled with already existing policies for migration, as rightly pointed by the Article 29 Working Party in reference to the 'Global Approach to Migration and Mobility'[39].

32. In the third place, the question of necessity should also be analysed in the broader context of large scale IT systems. A number of those systems have been developed during recent years (Eurodac, VIS and most recently SIS II replacing the first generation SIS)[40], in order to ensure a more effective external border control, as a corollary of the lifting of the internal borders for individuals who travel within the territory of the European Union. These information systems share common features. Normally, they consist of national units and a central unit, and supervision of data processing is shared between the national data protection authorities and the EDPS.

33. As mentioned above, the EDPS has supported and commented on the conclusions of the Stockholm programme inviting to a thorough reflection on such systems, to take duly into account both the costs for privacy and data protection, and the effectiveness for border control and public security. In particular, it 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*'.[41] In the present context, the analysis should include proposed instruments such as EES and RTP, but also those instruments that have been implemented.

---

[37] See ECJ, C-92/09, *op. cit.*

[38] See Articles 11 (2) and 13 (5) of the Schengen Border Code where Member States are asked to inform each other and the Commission and the Council General Secretariat of their national practices with regard to the presumption of illegal stay and its rebuttal as referred to in Article 11 and Member States are asked to collect statistics on the number of persons refused entry, the grounds for refusal, the nationality of the persons refused and the type of border (land, air or sea) at which they were refused entry. Member States shall transmit those statistics once a year to the Commission. The Commission shall publish every two years a compilation of the statistics provided by the Member States.

[39] Developed in the WP29 opinion, p.10. See COM(2011) 743 final.

40 The VIS system has been launched partially in 201140 and it is in the roll out phase in different parts of the world.. On 9 April 2013, the second generation Schengen Information System (SIS II) entered into operation.

The EDPS would like to refer to his findings concerning the VIS inspection carried out in 201140 where several of the problems found represented important risks for the security in the operations of the VIS.

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/VIS/12-06-01_VIS_security_audit_report_summ_EN.pdf

[41] Stockholm Programme, point 1.2.2.

34. The EDPS takes note of the analysis made by the Commission in the EES Impact Assessment[42]on the compatibility of EES with other large scale IT systems and its conclusion that none of these systems addresses the administrative requirements for managing the right to stay in the EU and for identifying and preventing irregular immigration, especially with regard to overstayers. However, some remaining unclarities should be pointed out.

35. While existing systems may not fully address the objectives of the smart border package, they can still address some of them, and may also be developed to address more in the future. For instance, one of the main objectives of the VIS Regulation[43] is to assist in the identification of persons that do not meet the requirements for entering, staying or residing in the national territories. An alert could also be entered under Article 24 of the SIS II Regulation[44].

36. The main problem is the lack of sufficient experience with the functioning of these systems to be able to draw useful conclusions. The experience with VIS and other current systems (Eurodac, SIS II) is limited: VIS[45], in particular, is not yet fully operational, with data protection issues to be managed at Central Unit level[46].

37. The EDPS therefore has doubts about the timing of envisaging a new border control system before a thorough evaluation of existing systems can effectively be performed, in order to ensure consistency and avoid repeating difficulties already encountered in the past.

[42] See p. 20 and 69-76 EES IA.

[43] The VIS should have the purpose to facilitate the fight against fraud and to facilitate checks at external border crossing points and within the territory of the Member States. The VIS should also assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States, and facilitate the application of Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanism for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national , and contribute to the prevention of threats to the internal security of any of the Member States.

[44] See Article 24 (3 of SIS II Regulation)- Conditions for issuing alerts on refusal of entry or stay
"An alert may also be entered when the decision referred to in paragraph 1 is based on the fact that the third-country national has been subject to a measure involving expulsion, refusal of entry or removal which has not been rescinded or suspended, that includes or is accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of third-country nationals."

[45] "At the end of 2011, the most critical risks identified were the following: a) system capacity being consumed quicker than foreseen due to Member States rolling out to other regions ahead of the planned gradual rollout; b) handover of the central VIS from the C.SIS to the EU Agency responsible for the management of IT systems, and c) fingerprint quality during operations."
See p. 10 in the Report from the Commission to the European Parliament and the Council on the Development of the Visa Information System (VIS) in 2011 (submitted pursuant to Article 6 of Council Decision 2004/512/EC).

[46] See also footnote 24.

38. In conclusion, even if the *objective* pursued could be considered legitimate and necessary in a democratic society, the *legislative measures* put in place do not fully meet the requirements of Article 8(2) ECHR in relation to necessity and proportionality. The EDPS therefore considers that, without further assessment by the legislators:

    a. An EES should not be created with the aim of identifying overstayers, without the establishment of a clear European policy on management of overstayers;

    b. Facilitating calculation of overstay and creating statistics should not lead to the establishment of a large scale database with personal data.

    c. An EES should not be created before a thorough evaluation of existing systems can effectively be performed, in order to ensure consistency and avoid repeating difficulties already encountered in the past.

39. As a second step, the scheme will have to comply with the specific safeguards of Article 8 of the Charter.

II.2. Article 8 of the Charter: Protection of personal data

40. This provision foresees "that everyone has the right to the protection of personal data concerning him or her". It further states that data can only be processed fairly, for specified purposes, on the basis of the consent of the person concerned or some other legitimate basis laid down by law, and that everyone has the right to access to data which have been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority. These are the essential requirements for the processing of personal data, which are further refined in the various legal instruments for data protection.

Fair processing

41. The type of measures that should contribute to ensuring fair processing range from general transparency to the minimisation of data collected, including steps taken to prevent discrimination. The EDPS welcomes the fact that several provisions of the Proposal aim at ensuring that data collected are not excessive (without prejudice to the assessment of the use of biometric data, which will be addressed in a distinct chapter below), and that awareness measures are taken, especially with regard to staff processing the data[47.]

42. The EDPS nevertheless calls attention on the risks linked to the automated calculation of dates and the decisions which could be taken against the individual on the basis of such automated processing. The conditions in which an individual will be informed of the fact that he may have been registered (unduly) as an overstayer remain unsatisfactory, as developed below.

[47] See in particular Article 8 on the general use of the EES and the prevention of discrimination, Article 11 and 12 on the list of data to be collected, which has been partially limited to take into account some EDPS observations, Article 25 about the training of staff, Article 33 on the information of individuals.

Specified purpose

43. The purpose(s) of any measure aiming at processing personal data must be clear and precise enough to ensure transparency for those concerned by the measure. The degree of specification shall take into account the scope and the impact of the data processing: the more intrusive it is, the clearer it should be. Article 4 of the Proposal lists a series of connected purposes and some further consequences that the scheme also aims at achieving.

44. These purposes have been mentioned earlier in this opinion, but can be recalled as follows:

- The main purposes are indicated in general terms, as improving the management of the external borders and the fight against illegal immigration, the implementation of the integrated border management policy and the cooperation and consultation between border and immigration authorities.
- The means to achieve these purposes are the provision of access to entry and exit information of third country nationals.
- The additional aims are to enhance checks at borders, calculate and monitor the duration of stay, assist in the identification of overstayers and consequently facilitate appropriate measures, and gathering statistics.

45. The EDPS has no further comments as to the details of these purposes. However, the fact that purposes must be specified also means that data should not be processed outside the frame of these purposes. This raises a specific issue with regard to the re-use of data for law enforcement purposes. Such purposes are mentioned as a future possibility, after evaluation of the system. In his comments on the Stockholm programme, the EDPS called for specific attention with regard to such re-use of personal data, and he insisted on a strict necessity test and narrow conditions for access to the data. This will be developed further in Chapter III.

Legitimate basis

46. Since the EES is obviously not based on the free and informed consent of the persons concerned, the need for a legitimate basis laid down by law relates in essence to the issue whether the proposed scheme complies with Article 7 of the Charter and Article 8 ECHR, as already discussed in Section II.1, with the conclusions set out in point 38. However, it should be emphasized that general principles of data protection also require that the processing of personal data is necessary and proportionate to the legitimate purposes that may be involved.

Rights of the individual

47. The EDPS insists on the need to pay specific attention to the legal consequences that can be attached to the automated processing of personal data. If the reality of the facts is not sufficiently taken into account, the effects on the data subjects can be particularly negative.

48. Article 9 of the EES proposal in particular deserves specific attention as it provides that, in order to facilitate calculation of stay, the system will automatically calculate which entry records do not have exit data immediately following the date of expiry of the authorised length of stay and inform competent authorities. This raises questions on how to avoid mistakes caused by an automated decision which could fail to register exits due to various reasons (dual status of the third country national - e.g. entry with an ordinary passport and exit with a diplomatic one - medical reasons or technical problems of the system).

49. Moreover, individuals must be fully informed in due time about any decision taken, to be able to exercise their rights properly. This is all the more needed considering the multiplication of data bases in the field of border management, which risks making it increasingly complicated for individuals to exercise their rights. The EDPS considers that the following provisions could be amended in order to enhance the rights of individuals in that perspective.

Right of erasure (Article 21.2)

50. The EDPS welcomes the obligation for Member States to delete without delay personal data relating to overstayers in case the relevant third country national provides evidence that he or she was forced to exceed the authorised duration of stay due to an unforeseeable and serious event. He considers however that it should be specified that data subjects should be informed of this right and should benefit from judicial remedies in case it is not respected (see recommendations below).

Information to be given to the data subject (Article 33)

51. The EDPS suggests adding in Article 33(1) that overstayers "*shall be informed of the following by the Member State responsible* ***for entering their data***". Without this addition the criteria for identifying the Member State responsible would remain unclear.

52. Furthermore, the EDPS suggests including information about:

- the automated processing of data in order to calculate duration of stay;
- the fact that overstay will lead to the publication of the individual's personal data on a list of overstayers;
- the categories of recipients of this list;
- the right to have personal data deleted in case of evidence that the overstay is due to an unforeseeable and serious event;
- the right to receive information about the procedures for exercising rights and about possible remedies, including arrangements allowing the person concerned to put his point of view considering the automated character of the processing of data.

53. In addition, the EDPS welcomes the fact that the information shall be provided in writing (Article 33(2)) but recommends adding: "in an intelligible form, using clear and plain language, adapted to the data subject" as it is foreseen in Article 11.1 of the proposed Data Protection Regulation[48]. Translations of this information should be available for third country nationals not understanding the language of the responsible Member State.

Remedies (Article 36)

54. Article 36 provides for remedies where the right of access, deletion and/ or rectification provided for in Article 35 have been refused. However it is not clear whether this provision includes the deletion of data referred to in Article 21(2). The EDPS therefore recommends amending Article 35 (or Article 36) to ensure that judicial remedies will also cover the situation referred to in Article 21(2).

Oversight by independent authorities (Articles 37-39)

55. The EDPS welcomes the provisions on supervision of data processing. Due account is taken of the responsibilities at national level and at EU level, and a system is laid down for coordination between all involved data protection authorities, based on experience and on existing, tried and trusted mechanisms. The EDPS is available to take up his duties in respect of EES (and of RTP).

56. The EDPS notes the responsibilities of various stakeholders within the smart borders framework, i.e. the Commission, eu-Lisa and the Member States. This triggers in parallel the responsibilities of data protection authorities at European and national level.

57. This distribution of competences requires a multi-level cooperation, among data controllers, among data protection authorities, and between authorities and controllers, in order to avoid any possible gray areas.

58. The EDPS welcomes the coordinated supervision model foreseen in Article 39 of the Proposal with regard to oversight, with a view to ensure consistent interpretation and application of the Regulation. He considers that this approach should be complemented with a clear allocation of competences at national level, to ensure that data subjects exercise their rights with the relevant authority. The identification of the Member State responsible should in that sense be clarified and be transparent to the public, as already mentioned above in point 51.

[48] 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.

III. SPECIFIC COMMENTS ON THE EES

III.1. Biometrics

59. The proposals rely on the use of biometric elements (fingerprints). The EDPS notes that in accordance with the policy options elaborated in the Impact Assessment[49] the Commission envisages that fingerprints will be added automatically three years after the EES starts to operate.

60. The EDPS points out that there is a need to demonstrate that the use of biometrics in this context, which represents a separate interference with the right to respect for private life, is "necessary in a democratic society" and that other less intrusive means are not available. In the S. and Marper case, the ECtHR ruled that fingerprints and photographs contain unique information that is "capable of affecting the private life of an individual" and that retention of this information without the consent of the individual concerned "cannot be regarded as neutral or insignificant"[50]. In addition the processing of such information should be accompanied by stringent safeguards and should take into account the risk of error.

61. Therefore, the EDPS would have preferred that an ex ante evaluation had been performed, also on the introduction of possible safeguards, rather than taking already now a definitive decision to introduce biometrics in the system. The EDPS suggests amending the text of the proposal in this sense. More precisely, the Commission should undertake a targeted impact assessment on biometrics (fingerprints) instead of an automatic introduction as stated in the current proposal (Article 12). The EDPS suggests including this as an obligation in Article 12 (5) of the EES Proposal.

62. In support of this recommendation, the EDPS takes note of developments in the United States, with a recent preliminary Report of the Government Accountability Office that refers to the challenges of planning a biometric exit capability[51]. It refers to significant questions such as the effectiveness of current biographic air exit processes, the error rates in collecting or matching data, the additional value that biometric air exit would provide compared with the current biographic air exit process, and the overall value and cost of a biometric air exit capability. This project of the United States to develop a biometric exit system is still under analysis.

[49] See p. 26-39 of the EES Impact Assessment.

[50] It also stated that that a blanket and indiscriminate retention of "the fingerprints, cellular samples and DNA profiles" of persons who are not convicted of offences failed "to strike a fair balance between the competing public and private interests"; ECHtR, S. and Marper v. the UK, *op. cit,* para. 125.

[51] Preliminary Observations on DHS's Overstay Enforcement Efforts, available on http://www.gao.gov/assets/660/654752.pdf.

63. The EDPS would also like to draw attention to the Australian Movement Reconstruction database which could represent an alternative on how a similar system could work based only on alphanumeric data[52]. These 'movement records' may include the traveller's name, date of birth, gender and relationship status, country of birth, departure and/or arrival date, travel document number and country, port code and flight/vessel details, visa subclass and expiry date, and the number of movements.

64. Moreover, the EDPS recognised at several occasions the advantages provided by the use of biometrics, but also stressed that these benefits would be dependent on the application of stringent safeguards.

65. In his opinion on SIS II[53], the EDPS proposed a non exhaustive list of common obligations or requirements which need to be respected when biometric data are used in a system, including a targeted impact assessment, emphasis on the enrolment process, highlight of the level of accuracy and a fallback procedure. These elements will help avoid that the third country national is to carry the burden of imperfections of the system, such as the impact of misidentification or failure to enrol. In this context, the EDPS welcomes Article 12(3) of the EES proposal which takes into account those persons for whom fingerprinting is physically impossible.

66. In addition, the EDPS notes the collection of 10 fingerprints instead of two or four which would in any case be sufficient for verification purposes. Collecting from the start 10 fingerprints would only be needed if this pursues a different purpose, i.e. the identification of traces in a law enforcement context. The EDPS considers that no such wide collection of biometric data should be foreseen from the beginning, whilst the evaluation of a possible access by law enforcement authorities is not to be done before two years after the entry into force of the system.

III.2. Law enforcement access

67. The EDPS notes that the EES proposal does not allow access by law enforcement authorities to the EES as a principle, but only after a period of evaluation. The proposal provides that the first evaluation of the EES shall specifically deal with the issue of access for law enforcement purposes including conditions of access, retention period and access for authorities of third countries.

[52] See more at: http://www.immi.gov.au/managing-australias-borders/border-security/systems/movement-records.htm.

[53] Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II) (COM(2005) 230 final, COM(2005) 236 final and COM(2005) 237 final) (OJ C 91, 19.4.2006, p. 38).

68. Access to the EES would fit in the general trend to grant law enforcement authorities access to several large-scale information and identification systems (see for instance the access to Eurodac[54]), and would also constitute a further step in a tendency towards giving law enforcement authorities access to data of individuals who in principle are not suspected of committing any crime.

69. The EDPS considers that the introduction of the possibility for law enforcement authorities to have access to EES - which would entail a separate interference with the right to respect for private life as well as a breach of the key principle of purpose limitation in data protection law - should be based on a proper evaluation which provides for clear evidence that such an access is necessary. In particular, the precise added value of such access compared with access to already existing biometric databases should be identified, and it should be demonstrated that the necessity overrides the intrusion into the private life of individuals. The EDPS recalls that the persons whose data are stored in the EES are in principle not suspected of any crime and should not be treated as such, since the system is in the first place designed mainly as a calculation tool for the duration of stay of third country residents.

70. Would access be necessary, strict conditions are needed, such as the condition that requests for data should be proportionate, narrowly targeted and based on suspicions as to a specific person.

III.3. Transfer of data to third countries

71. According to the EDPS, the reasons for which the transfer of EES data to third countries is necessary for the return of third country nationals should be further substantiated.

72. The EDPS welcomes that the transfer is in principle forbidden, and that Article 27 (2) contains a number of conditions, in case a derogation applies. However, in his view the transfer of personal data stored in the EES to third countries, international organisations and private parties[55] for the general purpose of proving the identity of third country nationals and the purpose of return is formulated too broadly. The EDPS understands the need to exchange some data with a third country where necessary for the purpose of the return of the individual concerned. However, it is not clear from the proposal under what conditions and for what purposes third countries will be allowed to ask for evidence on the identity of a third country national.

[54] See the Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison 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 (recast), OJ, 29.6.2013, L 180/1.

[55] See Article 27 (2).

73. Since a similar provision can be found in the VIS Regulation[56], the EDPS would also recommend the EU legislator to wait for evidence on how the VIS provision is applied in practice and then to evaluate the possibility to apply the exceptions now in Article 27 (2) also for the EES.

IV. OTHER COMMENTS ON THE EES

Definition of overstayer

74. In Article 5 (13) an "overstayer" is defined as a third country national who does not fulfil, or no longer fulfils the conditions relating to the duration of a short stay on the territory of the Member States. It is not clear if this definition is meant only to cover the situation where a third country national entered legally the territory of the EU but exceeded his/her stay or also the situation in which a third country national did not respect the conditions to stay set out in the Schengen Border Code (valid visa and travel documents, sufficient means of subsistence etc)[57] . This could entail different legal consequences for those who overstayed their legal period in the EU and for those who did not respect the conditions established to enter legally in the EU territory but did not over stay the legal period of 90 days in any 180 days period. The EDPS suggests that the Commission clarifies this definition.

Verification of identity

75. Article 18 (1) allows the access to data for the purpose of verifying the identity of the third country nationals and/or whether the conditions for entry to or stay on the territory of the Member State are fulfilled. The wording of this provision is too broad. In particular, the use of the word "or" may imply that personal data may be used for verification of identity, independently of the verification of entry of stay conditions. In order to avoid any possible access by authorities which are not specifically competent for immigration issues and for unrelated purposes, the EDPS recommends the EU legislator to delete the word "or" and keep both conditions (verifying identity and conditions of stay) linked.

Data retention for overstayers

76. The EDPS welcomes the maximum period of six months for keeping the data in the EES, as laid down in Article 20. As regards the retention period of five years for data related to overstayers, neither the impact assessment nor the proposal explains the reason for this period and it seems disproportionate with the aim pursued. The EDPS recommends the EU legislator to better justify in a recital the need for keeping the data on overstayers for such a long period of time, or limit this period in a substantive manner.

[56] See Article 30 (2) of Regulation (EC) No 767/2008 of the European Parliament and of 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).

[57] See Article 5 (1) of the Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 105/1, 13.4.2006.

Anonymous statistics

77. Article 40 allows competent authorities to access some categories of data for the purposes of reporting and statistics 'without allowing identification'. The use of the wording 'without allowing identification' creates confusion, since some of the categories of data accessed will allow - at least indirectly, especially when the data are combined - the identification of the individuals. Furthermore, the purpose of "reporting" mentioned in Article 40 should be clarified (what has to be reported, who has to report to whom and at which frequency). The EDPS therefore recommends the EU legislator to add the following wording: 'for the purposes of reporting and developing *anonymous* statistics' and to define the meaning of "reporting" in a Recital.

V. COMMENTS ON THE RTP PROPOSAL

Aim of the Proposal and the role of consent

78. RTP is designed to speed border-crossing for pre-vetted travellers. The scheme is based on automated identity checks and border crossing gates, with the aim of reducing or removing the need for border guards to check travel documents. According to the RTP Proposal the system is to be established on a voluntary basis where frequent travellers will be offered the possibility to apply for a faster border crossing[58].

79. Consent of the traveller is presented as the ground legitimising the processing of personal data. To be valid, this consent must be "freely given, specific and informed"[59]. As stated in WP29 Opinion 15/2011[60], consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent is not free.

80. The setting up of the EES scheme and the full implementation of VIS[61] are likely to increase time spent at border checks, which would make RTP a favourite option for frequent travellers. In this context, it should be made sure that consent can effectively be considered as a valid legal basis for the processing. Besides, the fact that the system is voluntary does not prejudge the assessment of the necessity and proportionality of the system and the fact that its development and functioning is dependent upon another system, i.e. the EES.

[58] Ibid p. 5.
[59] See Article 2(h) of Directive 95/46/EC.
[60] Article 29 Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf
[61] Ibid., p. 16.

81. It also appears that RTP may imply time consuming and administrative burdens for frequent travellers, at least at the moment of enrolment, since they will have to give fingerprints again for an additional purpose and provide once more administrative documents required by Article 9 of the RTP Proposal. Moreover, their alphanumeric and biometric data will remain for 5 years in the system in order to allow for the checking of the travel history in a person centric manner. It is still not clear how efficiently the RTP will work in practice.

RTP and possible risks for discrimination

82. The RTP requires that all participants are pre-vetted and pre-screened. The vetting criteria are therefore crucial. This is also emphasised in the Explanatory Memorandum which mentions that *"Paragraph 2 (of Article 12) is crucial because it establishes the criteria for examining RT"*[62]. Looking at the supporting documents to be provided by the applicant and the conditions to be examined by visa or border authorities, it seems that vetting criteria for RTP have been aligned to the ones used for examining multiple-entry visa applications[63]. The EDPS welcomes that the criteria for both instruments are aligned.

83. However, the purpose of the proposal as mentioned in its Article 2 is 'to facilitate the crossing of the EU external borders by frequent, pre-vetted third country travellers'. There may be a risk of discrimination[64] as only the travellers taking specific steps through ad hoc registration and provision of detailed information would be considered 'low-risk' travellers while the vast amount of travellers who do not travel frequently enough to undergo such a registration or whose fingerprints are unreadable[65], would thus, by implication, de facto be in the 'higher-risk' category of travellers.

84. The Impact Assessment mentions that the potential issue of discrimination arises especially if the vetting is too strict. This issue should therefore be incorporated into the training programme on fundamental rights which Frontex organises for border guards. It should be made clear, as stated in the Impact Assessment, that those not using the ABC are not considered as more risky travellers[66]. In order to raise awareness with the general public, this should also be covered during the information campaign organised before the RTP starts operations. The leaflets and posters

[62] p. 10.
[63] See Articles 14 , 21 and 24 of the Visa Code.
[64] See also EDPS Preliminary comments on three Communications from the Commission on border management (COM (2008) 69, COM (2008)68 and COM (2008)67), 3 March 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf;
Opinion of 7 July 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration, OJ C 34/02, 08.02.2012, p.18;
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-07-07_Migration_EN.pdf
[65] See Article 8 and Explanatory memorandum of the proposal which does not allow exemption from collecting biometric data.
[66] See p. 39 of the Impact Assessment.

should clearly state that travellers are free to choose whether or not to apply for the RTP and use the Automated Border Control (ABC). The EDPS considers that, to a certain extent, these initiatives could help avoiding risk of stigmatisation.

Subjective criteria of assessment

85. Both Articles 5 and 9 mention the criterion of "integrity and reliability" for the applicant. In order to ensure legal certainty and equal treatment, subjective criteria such as "if the applicant is known to them for his/her integrity and reliability" should be removed or replaced by more objective criteria allowing consistent application across the EU.

Categories of data to be collected

86. The Proposal refers in Articles 12 and 15 to the obligation for visa or border authorities to verify that the applicant is not considered to be a threat to public policy, internal security, public health or the international relations of any of the Member States, in particular where no alert has been issued in Member States' national databases on the same grounds (Articles 12.2 (h) and 15.1 (d)). The EDPS recommends clarifying how such verification should take place, what kind of information visa or border authorities should be taken into account, with or without interconnecting databases, as well as the impact of such processing.

87. The Proposal should also provide for a mechanism to handle applications and requests of individuals, with a view to prevent simultaneous requests of one individual in different Member States and possible diverging outcome. The Central Repository, which is to be used for applications according to Article 24, could be checked in order to prevent such multiple handling of requests.

Prohibition of international transfers

88. The EDPS welcomes Article 42 which expressly forbids transferring or making available data processed in the Central Repository or during the examination of applications to third countries or international organisations under any circumstances.

VI. SECURITY RECOMMENDATIONS FOR EES AND RTP

89. Under Article 23 of the EES Proposal and Article 37 of the RTP Proposal the Commission will be required to adopt measures necessary for the development and technical implementation of the required systems. EU-Lisa, the Agency for large-scale information systems, will be responsible for the rest of the development of these systems

90. Development of systems such as the EES or the RTP are often complex and require following a sound methodology in order to ensure a high quality output. Typically, before designing or implementing any part of such a system, sound development methodologies analyse the needs first so as to manage all requirements. They can be linked to functional needs, data protection needs, security or other needs, and must be identified,

carefully described and documented so as to be implemented using the best possible cost-effective approach. Furthermore, the analysis phase is a key point where Privacy by Design[67] and Privacy by Default[68] need to be taken into account. Additionally, a proper analysis will show how the requirements fit together and ensure that different requirements do not negatively impact each other in any significant way.

91. The EDPS recommends to ensure in the proposals that a proper analysis of the needs be performed before designing or implementing any part of the system. This analysis should be performed jointly by the Commission and the Agency in order to ensure that all requirements are managed and that they do not come into conflict with one another.

Development and Operational management

92. Article 24 of the EES Proposal and Article 38 of the RTP Proposal provide that the Agency will be responsible for the development of the different parts of each system. The development is defined in Articles 24(1) EES and 38(1) RTP as "the elaboration and implementation of the technical specifications, testing and overall project coordination".

93. During the testing phases of the development of any system, and in order to detect development errors, some data (called test data) must be used in order to check whether or not the newly developed software behaves as expected. Thus, the test data should have similar characteristics as the "real" data (personal data from data subjects that will be processed by the EES). This is typically achieved by examining the "real" data and building a test data set that resembles it without revealing any personal data.

94. However, Article 24(1) EES and Article 38(1) RTP do not specify what the Agency may or may not do with the "real" data with regard to the development of the system, such as in the context of tests, verification, validation or test migration to new versions of the system. It should be made clear in those provisions that personal data is not to be used for any such functions.

95. In Article 24(2) EES and Article 38(2) RTP the availability of the platform is fixed to 24h/day, 7 days a week, which shows that these systems are of critical importance and cannot in any circumstances stop functioning. Setting up systems requires a Business Continuity Plan setting out how the organisation should react to incidents in order to ensure that operations are kept under control even under the most severe disruptions. The need for a Business Continuity Plan should therefore be included in Article 24(2) EES and Article 38(2) RTP and a legal basis should be provided for implementing measures containing the modalities of such plan.

[67] Embedding privacy in all elements at the early start of the deployment of a system.
[68] Building the activities in the most privacy-friendly way by default.

National responsibilities

96. The suggestions made above are also applicable to the Member States for the development of their National Systems. Personal data should not be used for tests, verification, validation nor to test migration to new versions of their National System, as should be stated in Article 25 EES and Article 39 RTP.

Data Security

97. The EDPS welcomes the fact that Article 28 EES and Article 43 RTP aim at ensuring a sufficient level of security to protect EES and RTP data against threats. However, the definition of measures should be based on a continuous process of managing and monitoring information risks. This continuous process - often referred to as Information Security Risk Management - aims at identifying, assessing and prioritising risks to the organisation's information, and determining and implementing security measures in order to minimise the risks to a level aligned with the needs and acceptable for the Agency and the Member States. Information Security Risk Management also ensures that the context in which data is processed and facilities are used is clearly understood (also in terms of data protection needs) and thus a selection of cost-effective security controls may be selected and implemented to achieve the appropriate level of security.

98. Hence, the EDPS recommends specifying in Article 28 EES and Article 43 RTP that Information Security Risk Management practices shall be used in order to define the appropriate technical and organisation measures in order to protect all relevant data, taking into account all data protection needs. An obligation should be included to ensure security through proper Information Security Risk Management practices based on:

- recognised international standards,
- regular reviews of all analysis performed in that context,
- monitoring and review of all technical and organisational measures implemented in this context, and
- strong collaboration between the Agency and Member States, in order to tackle security risks across information system boundaries.

99. Furthermore, with regards to the specific measures listed in Article 28 EES and Article 43 RTP:

- In Article 28(2)(a) EES and Article 43(2)(a) RTP "critical" should be replaced by "relevant".
- In Article 28(2)(f) EES and Article 43(2)(f) RTP the term "confidential access modes only" should be clarified.
- In Article 28(2)(g) EES and Article 43(2)(g) RTP, it should be added: "make their profiles and any other relevant information the authorities require for the purposes of carrying out supervision available".

- In Article 28(2)(i) EES and Article 43(2)(i) RTP 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, Article 28(2)(k) EES and Article 43(2)(k) RTP should include not only auditing (a picture of the situation at a given point in time), but also near real-time observation of the system using specialised tools. Both provisions should be redrafted to clearly distinguish these two concepts and apply them appropriately.
- Article 28(3) EES and Article 43(3) RTP should also include measures to be taken by the Agency to ensure the availability of the system as described in Article 24 EES and Article 38 RTP and ensure the backups.
- Article 28(3) EES and Article 43(3) RTP should also mention the Business Continuity Plan (see above).

100. As regards security incidents, Article 28 EES and Article 43 RTP should also include:

- the necessity for the Agency and the Member States to agree to a common evaluation scheme for security incidents;
- the necessity for the Agency and the Member States to manage security incidents, following a documented process, as well as keep a record of all security incidents and their resolution;
- the necessity for the Member States to inform their national supervisory authorities and the Agency of severe security incidents they detected on their system;
- the necessity for all parties to collaborate during a security incident;
- the necessity for the Agency to inform the affected Member States, the corresponding national supervisory authority(ies) and the EDPS if a severe security incident occurs.

Keeping of records

101. As regards Article 30(2) EES and Article 45 RTP, it should be noted that (i) the logs used for data security and (ii) those used to monitor, audit and inspect that personal data was processed in accordance with the rules are different. The EDPS recommends splitting these records in two sets (one set might be a subset of the other) to avoid giving out personal data contained by the system to security staff. Furthermore, these records should be protected from unauthorised access and unauthorised modification.

VII. CONCLUSIONS

102. The Smart borders package aims at creating a new large scale IT system in order to supplement the existing border control mechanisms. The lawful character of this system needs to be evaluated against the principles of the Charter, in particular Article 7 on the right to respect for private and family life and Article 8 on the protection of personal data, with the objective to assess not only the interference with fundamental rights of the new scheme but also the data protection safeguards provided in the Proposals.

103. In that perspective, the EDPS confirms that the proposed EES scheme constitutes an interference with the right to respect for private and family life. While he welcomes the safeguards in the Proposals and recognises the efforts made by the Commission in that sense, he concludes that necessity remains the essential issue: the cost/efficiency of the system is at stake, not only in financial terms, but also in relation to fundamental rights, seen in the global context of existing schemes and border policies.

104. The EDPS makes the following recommendations as to the EES:

- The necessity and proportionality of the system could only be positively demonstrated in accordance with Article 7 of the Charter after a clear European policy on management of overstayers has been established, and the system is assessed against the more global context of existing large scale IT systems.

- Data protection principles should be improved in accordance with Article 8 as follows:

  - Purposes should be limited and the design of the system should not pre-empt on the future assessment of any possible law enforcement access to EES data.
  - Data subjects rights should be reinforced, especially with regard to the right to information and redress possibilities, taking into account the need for specific safeguards concerning automated decisions taken in relation to the calculation of the duration of stay.
  - Oversight should be complemented with a clear picture of the allocation of competences at national level, to ensure that data subjects exercise their rights with the relevant authority.
  - The use of biometrics should be subject to a targeted impact assessment, and if considered necessary, the processing of such data should be subject to specific safeguards regarding the enrolment process, the level of accuracy and the need for a fallback procedure. Besides, the EDPS strongly questions the collection of 10 fingerprints instead of two or four which would in any case be sufficient for verification purposes.
  - The reasons for which the transfer of EES data to third countries is necessary for the return of third country nationals should be substantiated.

105. While the RTP does not raise the same substantial questions with regard to interference with fundamental rights as the EES, the EDPS still calls the attention of the legislator on the following aspects:

  - The voluntary basis of the system is acknowledged, but consent should only be considered as a valid legal ground for processing the data if it is freely given, which means that RTP should not become the only valid alternative to long queues and administrative burdens.
  - Risks of discrimination should be prevented: the vast amount of travellers who do not travel frequently enough to undergo registration

or whose fingerprints are unreadable should not be de facto in the 'higher-risk' category of travellers.

- The verification process leading to registration should be based on selective access to clearly identified databases.

106. With regard to security aspects, the EDPS considers that for EES and RTP a Business Continuity Plan and Information Security Risk Management practices should be developed to assess and prioritise risks. Moreover, strong collaboration should be foreseen between the Agency and the Member States.

Done in Brussels, 18 July 2013

(**signed**)

Peter HUSTINX
European Data Protection Supervisor