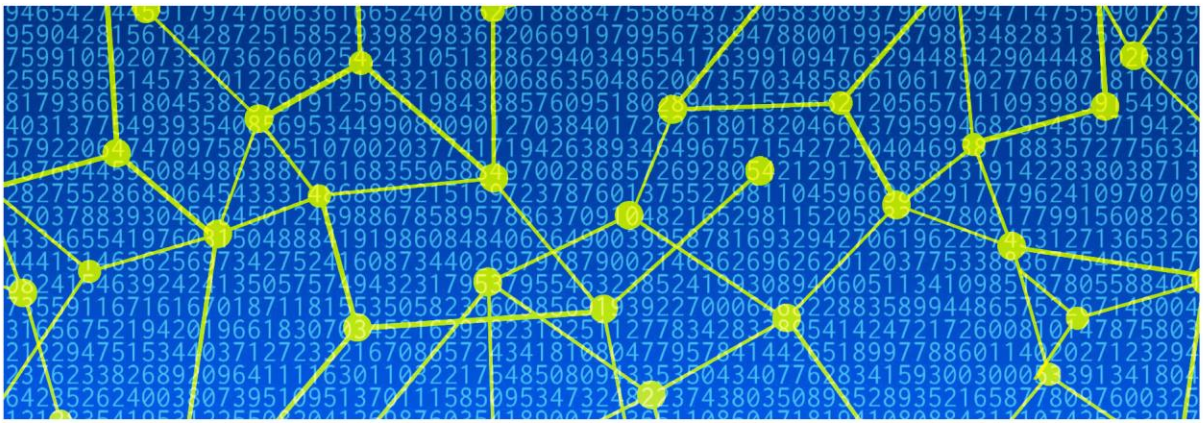

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 06/2016

EDPS Opinion on the Second EU Smart Borders Package

Recommendations on the revised Proposal to establish an Entry/Exit System

EDPS

21 September 2016

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. The EDPS considers that compliance with data protection requirements will be key to the success of the renewed Smart Borders Package and the exchange of information on entries and exits of third country nationals through the Entry/Exit System.

Executive Summary

The establishment of an Entry/Exit System (EES) that will record entries and exits of third country nationals on the territory of the European Union has been envisaged for a long time by the EU legislator. The Commission adopted three proposals as part of the first Smart Borders Package in 2013; the co-legislators expressed serious concerns and the package did not reached a consensus. Then the Commission launched a Proof of Concept exercise in response to those concerns, and released this year a second Smart Borders Package now composed of two revised proposals.

The EDPS has carefully analysed these proposals and issues recommendations with a view to assist the legislator so as to ensure that the legal framework applicable to the EES scheme will be fully compliant with EU privacy and data protection law, in particular Articles 7 and 8 of the EU Charter of Fundamental Rights.

The EDPS recognises the need for coherent and effective information systems for borders and security. These proposals come at a crucial moment when the EU is confronted with serious challenges in this area. However the EDPS underlines the significant and potentially intrusive nature of the proposed processing of personal data under the EES, which must therefore be considered under both Articles 7 and 8 of the Charter. Necessity and proportionality of the EES scheme are to be assessed both globally, taking into consideration the already existing large-scale IT systems in the EU, and specifically, in the specific case of these third country nationals who are lawful visitors of the EU. The EDPS notes that EES data will be processed for two different purposes, on the one hand for border management and facilitation purposes and on the other hand for law enforcement purposes. The EDPS strongly recommends clearly introducing the difference between these objectives throughout the 2016 EES Proposal itself, as these purposes entail a different impact on the rights to privacy and data protection.

While he welcomes the attention to privacy and data protection concerns previously expressed and the improvements in the revised proposals, the EDPS raises serious concerns as regards several aspects of the EES Proposal that should be better justified, or even reconsidered by the legislator, in particular:

- the five years retention period of EES data. The EDPS notes that the need for keeping overstayers' data for five years should be better demonstrated, and that a retention period of five years for all personal data stored in the EES appears to be disproportionate;

- the collection of the facial image of visa-required travellers, whose facial image is already stored in the VIS;

- the need for access to EES data by law enforcement authorities, which is not sufficiently supported by convincing evidence;

- the prerequisite for a data subject to provide fingerprints when exercising his/her rights of access, correction and/or deletion of his/her personal data which could be an important obstacle to the effective exercise of these rights.

The Opinion further provides additional recommendations in terms of data protection and privacy that should be taken in consideration in the legislative process, including the security of the system.

TABLE OF CONTENTS

1. INTRODUCTION AND BACKGROUND 5

2. AIM OF THE PROPOSALS 6

3. ANALYSIS OF THE PROPOSALS 7

I. IMPACT OF THE EES ON PRIVACY AND DATA PROTECTION 7

II. OBJECTIVES OF THE EES 8

III. BORDER MANAGEMENT AND FACILITATION 9

III.1 Data retention for five years 9

III.2 Data collected 11

III.3 Additional recommendations on the Proposals 12

IV. ACCESS BY LAW ENFORCEMENT AUTHORITIES 19

IV.1 Law enforcement as a secondary objective 19

IV.2 Necessity of law enforcement access 19

IV.3 Conditions for access and safeguards 20

4. CONCLUSION 21

NOTES 24

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty of 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], and in particular Articles 28(2), 41(2) and 46(d) thereof,

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

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1. The Commission first announced its intention to build a European Entry/Exit System in order to control entries and exits of third country nationals on the territory of the European Union in 2008[4]. At that time the EDPS first gave his preliminary comments[5] on the idea and then highlighted specific issues in an Opinion of July 2011[6]. The Commission further elaborated its views in a Communication[7] entitled '*Smart borders - Options and the way ahead*' of October 2011, on which the Article 29 Working Party provided comments[8]. The EDPS also gave input in a joint round table with various stakeholders[9].

2. In February 2013, the Commission adopted three proposals as part of the first Smart Borders Package: a proposal to build and Entry/Exit System[10] (hereinafter "the 2013 EES Proposal"), a proposal to establish a Registered Traveller Programme[11] (hereinafter "the 2013 RTP Proposal") and a proposal amending the Schengen Border Code[12] to introduce these changes accordingly. The Package immediately faced criticisms from both co-legislators due to technical, operational and cost concerns, as well as important data protection concerns. The same year, the EDPS provided his first concrete recommendations on the three proposals in the form of an Opinion[13]. The Article 29 Working Party also issued an Opinion[14], to which the EDPS contributed, which questioned the necessity of the Entry/Exit System as such.

3. Early 2014, in response to those concerns, the Commission announced the launch of a Proof of Concept exercise consisting of two steps: first a Technical Study[15] and a Cost Study[16] to identify the most suitable options and solutions to implement Smart Borders, followed in the course of 2015 by a Pilot Project[17] led by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereinafter "eu-LISA") in order to test the different options identified. In parallel, the Commission launched a three-

month public consultation[18] in July 2015 to collect views and opinions from citizens and organisations, to which the EDPS also contributed[19].

4. On 6 April 2016, the Commission released a second Smart Borders Package[20]. This time, only one system is proposed: the Entry/Exit System (hereinafter "the EES"). The Commission decided to revise its 2013 EES Proposal and the 2013 Proposal amending the Schengen Borders Code, but to withdraw its 2013 RTP Proposal. Today's Smart Borders Package is composed of:

- a Communication on 'Stronger and Smarter Information Systems for Borders and Security'[21];
- a Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011[22] (hereinafter "the 2016 EES Proposal"); and
- a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) 399/2016[23] as regards the use of the Entry/Exit System[24] (hereinafter "the 2016 Proposal Amending the Schengen Borders Code").

5. In addition, a detailed Impact Assessment[25] accompanies the two proposals.

6. The Smart Borders Package has gained new momentum following the current migration crisis and recent terrorist attacks in Europe. The Dutch Presidency and the Slovakian Presidency announced that they plan on working intensely on the Package with a view to reaching a political agreement by the end of 2016[26].

7. The EDPS welcomes that he has been consulted informally by the Commission before the adoption of the new proposals. He also welcomes the good cooperation[27] between DG HOME and the EDPS throughout the process of renewing the first Smart Borders Package.

2. AIM OF THE PROPOSALS

8. The proposed EES comes at a crucial moment when the EU is confronted with serious challenges for its border control and its security. It will complement existing EU large-scale IT systems concerning ayslum seekers and visa applicants. In this context, the **2016 EES Proposal** aims to improve the management of the EU external borders and reduce irregular immigration by addressing the phenomenon of 'overstaying'[28]. Looking at stamps in travel documents is currently the sole method available to border guards and migration authorities to calculate the duration of stays of third country nationals and verify if they have overstayed. To this aim, the Proposal will apply to third country nationals who legally enter the EU. The EDPS understands that the circumstances of third country nationals' entry in the EU will determine if their data are stored in the EES or in the Eurodac database: those who enter legally through an official border crossing point and are admitted for a short stay (i.e. maximum 90 days in any 180 day period) in the Schengen area will have their data registered in the EES, while third country nationals who seek asylum or illegaly enter the EU or have illegaly entered and are found within the EU, will have their data registered in Eurodac. The EES system will collect their

personal data, including biometric data, and register the time and place of their entries and exits. The system will also record refusals of entry.

9. In addition, the proposed EES intends to contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences, and serve as an identification tool and an intelligence tool.

10. The main changes introduced by the 2016 EES Proposal compared to the 2013 EES Proposal include an increased data retention period of five years for *all* EES data, access by law enforcement authorities from the start of operation of the system, specification of the biometric identifiers used and interoperability with the Visa Information System (hereinafter "the VIS") through a direct communication channel between both databases.

11. The **2016 Proposal Amending the Schengen Borders Code** has the aim to introduce the technical changes that result from the 2016 EES Proposal into the Schengen Borders Code, in particular the recording in the EES of refusals of entry of third country nationals, the fall-back procedures for the EES and the interoperability between the EES and the VIS. The 2016 Proposal also introduces the new possibility for Member States to create national facilitation programmes on a voluntary basis.

3. ANALYSIS OF THE PROPOSALS

I. Impact of the EES on privacy and data protection

12. In light of the serious migratory challenges faced by the EU, the EDPS recognises the need for the EU to take action. However, such action must be fully respectful of the EU legal framework. The proposed EES scheme will relate to third country nationals who are lawful visitors. The legislator has to consider, among others, their fundamental rights to privacy and data protection enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (hereinafter "the Charter") both of which apply because the EES scheme will involve the significant collection, storage and use of personal data concerning them.

13. In principle, such processing is compatible with the fundamental rights protected by the Charter if it complies with the conditions laid down in Article 52(1) thereof; limitations must:

- be provided for by law,
- respect the essence of the right,
- genuinely meet objectives of general interest recognised by the Union, and
- once proved necessary, comply with the principle of proportionality.

14. Necessity and proportionality of this scheme are to be assessed both globally, taking into consideration the already existing large-scale IT systems in the EU, and specifically, in the specific case of these third country nationals legally visiting and entering the EU. **The EDPS would first like to stress that from the point of view of Articles 7 and 8 of the Charter the processing of personal data under the proposed EES will entail is significant and intrusive,** taking into consideration the number of persons affected by this scheme, the type of information processed, the means used to process such information and the different purposes pursued, as explained below.

15. First, the EES will cover *all* entries and exits of third country nationals[29] coming in or going out of the territory of the EU, and thus concerns millions of individuals each year. According to the Commission itself, the total number of regular border crossings is expected to rise to 887 million in 2025, of which around one-third will be by third country nationals[30]. The sheer volume of personal data that would be processed through this system will make of the EES one of the largest European databases. In this regard, the EDPS welcomes that the 2016 EES Proposal aims at reducing the amount of personal data processed, in line with the data minimisation principle: a maximum of 26 data items per person is expected to be recorded in the EES[31] (instead of the 36 data items foreseen in the 2013 EES Proposal[32]).

16. Second, the EES is expected to lead to the fingerprinting of third country nationals and the capture of their facial image upon entry, thus significantly expanding the amount of biometric data already held by the EU in existing databases such as Eurodac, the Schengen Information System (hereinafter "the SIS") and the VIS. Biometric data are of a peculiar nature and considered more delicate as they are unequivocally linked to one individual, whose body is made "readable"[33]. The EDPS takes note of the need to use biometrics in order to ensure higher assurance of the identity of third country nationals crossing the EU borders. Nonetheless, due to their very nature, processing of biometric data implies a more serious interference and therefore requires ensuring a higher level of data protection.

17. Third, the EDPS also notes that following the Pilot Project led by eu-LISA, the 2016 EES Proposal provides for a reduced number of biometric data to be stored. Based on the findings of this Pilot, the 2016 EES Proposal proposes the enrolment of four fingerprints plus the facial image considered to be enough for verification and identification purposes (while the 2013 EES Proposal relied on ten fingerprints without facial image). However, the EDPS points out that a lower number of biometric data is not necessarily synonym of a lower interference as the Proposal provides for the collection of a combination of two types of biometric data, thus allowing the use of both fingerprint matching software and facial recognition software to quickly process and sift through the data stored.

18. Finally, the impact of the EES will be twofold as EES data will be processed both for border management and facilitation purposes and for law enforcement purposes.

II. Objectives of the EES

19. In the Explanatory Memorandum to the 2016 EES Proposal[34], the Commission states that the EES will pursue three general objectives:

1) addressing border check delays and improving the quality of border checks for third country nationals (‘facilitation’),
2) ensuring systematic and reliable identification of so-called ‘overstayers’ (‘border management’),
3) supporting the fight against terrorism and serious crime and ultimately contributing to a higher level of internal security (‘law enforcement’).

20. The EDPS notes that objectives 1) and 2) are often referred to as *"the two primary objectives of the EES"*[35] in the Impact Assessment accompanying the 2016 EES Proposal, while access to EES data for law enforcement purposes is referred to as a *"secondary objective"*[36] of the scheme. However, this difference is not reflected in the text of the 2016 EES Proposal,

neither in its articles nor in its recitals. On the contrary, the 2016 EES Proposal put these three general objectives at the same level in Article 1 of the Proposal, which defines its subject matter, and in Article 5, which lists twelve specific purposes for collecting, storing and accessing EES data. **The EDPS strongly recommends clearly introducing this difference between the objectives throughout the 2016 EES Proposal itself.**

21. The EDPS understands that the EES system will be primarily created for border management and facilitation purposes, with a potential access to EES data for law enforcement purposes. Therefore, the present Opinion will analyse consecutively the setting up of the EES for border management and facilitation purposes as the two primary objectives of the system in Section III, and the access granted to law enforcement authorities to this border control tool as a secondary objective in Section IV.

III. Border management and facilitation

22. The EDPS acknowledges that the EU is presently facing increasingly serious migratory challenges, and notes that the 2016 EES Proposal is part of a more global EU policy on border control and migration management. An assessment of the effective impact of the EES on this policy together with all the relevant large-scale IT systems already available in this area such as Eurodac, SIS and VIS, which will also be further developed in the near future, is needed.

23. The EDPS welcomes that the Commission has paid attention to privacy and data protection concerns previously expressed as regards the EES, and has taken the time to gather and produce more documentation in support of the creation of this system and the policy choices made in the second Smart Borders Package through various exercises such as the Pilot Project led by eu-LISA, the FRA Survey, the Public consultation and a thorough Impact Assessment accompanying the 2016 proposals. Although evidence is not always fully comprehensive[37], there do appear to be sufficient elements to justify the setting up of the EES for the purposes of border management and facilitation.

24. Given the wide-ranging impact on privacy and data protection that would arise from the proposed EES scheme[38], it is important that the future EES Regulation fully meets the proportionality requirement set by Article 52(1) of the Charter in case a review by the CJEU were to take place. Even if considered necessary, it should be better demonstrated that the benefits of building an Entry/Exit System outweigh the intrusion in the privacy of *all* third country nationals. The CJEU provided guidance in the Digital Rights Ireland judgment delivered in joined cases C-293/12 and C-594/12[39] (hereinafter "the DRI Ruling"). The EDPS has taken note of the Proportionality test carried out by the Commission in the Impact Assessment[40].

25. The EDPS has comments on two main aspects of the 2016 EES Proposal that are directly related to the proportionality of such a scheme for border management and facilitation purposes (sections III.1 and III.2). The EDPS has additional recommendations regarding specific aspects of the 2016 EES Proposal (section III.3), which he invites the Commission to consider.

III.1 Data retention for five years

26. When choosing the data retention period, EU data protection standards call for a period of time as short as possible. Recital 25 of the 2016 EES Proposal rightly states that *"The personal*

data stored in the EES should be kept for no longer than is necessary for the purposes of the EES". The Proposal now[41] provides for an increased retention period of five years for *all* entry and exit records of *all* third country nationals following the date of the exit record (Article 31(1)), and five years and one day for individual files[42] *"following the date of the* last *exit record if there is no entry record within five years from that last exit record"* (Article 31(2)). In addition, the 2016 EES Proposal provides for one minor exception in Article 31(4) as regards entry/exit records of non EU family members of EU citizens, which will be kept for one year, while their individual files should be kept for the same period of five years.

27. The EDPS first points out that, given the starting date of the retention period for individual files laid down in Article 31(2), third country nationals who travel to the EU at least once every five years will have their personal data, including their facial image and four of their fingerprints, stored in the EES not solely for five years but on a more permanent basis. Indeed if they travel again to the EU within less than five years, their personal file will not be deleted but instead kept for another period of five years following their exit of the EU territory.

28. **The EDPS would like to draw the attention of the legislator on the need to fully justify the proportionality of a retention period of personal data for five years,** in view of the objective of reducing border check delays and improving border checks for third country nationals, and of the objective of identifying overstayers.

29. **Indeed, the 2016 EES Proposal should meet the requirements laid down by the Court in the DRI Ruling**. In this regard, the CJEU held that *"the determination of a period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary"*[43]. The EDPS takes note of the fact that a period of five years would correspond to the average duration of passports' validity delivered by third countries, as well as to the maximum length of validity of multiple-entry visas, as referred to in the Impact Assessment[44] accompanying the proposals. However, the fact that the chosen retention period is aligned to those of other existing systems such as the VIS does not *per se* justify this choice as proportionate.

30. The Proposal also provides for the advance deletion of the individual file and entry and exit records before the end of the chosen period, in the case where the person concerned has acquired the nationality of or a residence permit from an EU Member State[45] (Article 32(6)). The EDPS welcomes that the Proposal specifies the Member State responsible for the deletion, and that such deletion should take place "without delay". However, the EDPS suggests specifying the notion of "without delay" in connection to the deletion of retained data that have become excessive and are no longer necessary for the purposes of the EES.

31. In the specific case of overstayers, Article 31(3) of the 2016 EES Proposal provides for a data retention period of five years following the last day of the authorised stay (similarly to the 2013 EES Proposal[46]). However, the recitals of the current Proposal do not bring any additional justification of such a need compared to the former Proposal[47], despite EDPS' previous recommendations to the legislator to better justify in a recital of the EES Proposal the need for keeping overstayers' data for such a long period of time or to limit this period in a substantive manner[48].

32. In addition, the 2016 EES Proposal provides that the future system will automatically inform the relevant Member State three months in advance of the scheduled deletion of data concerning overstayers in order to allow the adoption of appropriate measures (Article 31(3)).

In this regard, the Explanatory Memorandum of the EES Proposal explains that data concerning overstayers who have not been found at the end of the five years retention period could possibly be recorded as an alert for refusal of entry in the SIS following a national decision[49]. However, the adoption of appropriate measures, including the creation of an alert in the SIS, could take place earlier than five years following the identification of a third country national as overstayer.

33. **The EDPS therefore still fails to understand the need for keeping these data for such a long period of time for the purpose of identifying overstayers, and asks the legislator to justify this period and/or to reduce it to ensure that is limited to what is strictly necessary.**

III.2 Data collected

34. The 2016 EES Proposal provides for the collection, storage and use of alphanumeric data and biometric data concerning third country national entering and exiting the EU, as detailed in Articles 14 to 18. The EDPS welcomes that the Proposal reduces the overall amount of personal data from 36 to 26 data items per individual, as well as the number of fingerprints[50] processed from ten to four for visa-exempted third country nationals (Article 15(1)). For visa-required third country nationals, the facial image will be the only biometric identifier enrolled in the EES (Article 14(1)) since their ten fingerprints are already stored in the VIS. Collection of ten fingerprints would be typically linked to the pursuit of law enforcement purposes.

35. However, the EDPS questions the need to store facial images of visa-required third country nationals in the EES, while their facial image is already stored in the VIS. The EDPS takes note of the observation in the Impact Assessment that to date *"a visa holder cannot be searched in the VIS on the basis of his/her picture"*[51], but questions why the VIS cannot be used to the full for both EES and VIS functionalities. **The EDPS asks for justification of the need to store facial images of visa-required third country nationals in the EES. The consequence of this requirement will be that visa-required third country nationals will have their facial image stored twice in two different databases that will be interconnected. In the absence of a convincing justification for storing the facial images in two different databases, the EDPS recommends removing the facial image from Article 14(1) of the Proposal so that the EES will rely on both the fingerprints and the facial image already stored in the VIS for visa-required third country nationals, in order to avoid duplication of biometric data in EU IT systems and limit the collection and storage of data in the EES to what is strictly necessary.**

36. Finally, Article 15 of the 2016 EES Proposal envisages several cases in which it would be impossible to take third country nationals' fingerprints due to legal reasons (e.g. the individual is under the age of 12) or factual reasons (e.g. missing hand or fingers, damaged fingertips). Article 15(3) describes the situation where it is physically impossible to take a third country national's fingerprints. Some of these situations may be of temporary nature and would typically be linked to a medical condition. The process described in Article 15(3) entitles the border authorities to request further clarification on the grounds for the temporary impossibility to provide fingerprints. However, there is no further explanation on what happens to the data collected, neither regarding where, how and for how long that data is stored, nor regarding how that data may be used and how that data is secured. **The EDPS recommends that Article 15(3) be amended so as to specify what information may be collected, stored and used by the border authorities.**

III.3 Additional recommendations on the Proposals

a) Biometric data

37. The 2016 EES provides for the collection, storage and use of biometric data of third country nationals: the facial image only for visa-required travelers (Article 14(1)) and a combination of four fingerprints plus the facial image for visa-exempted travelers (Article 15(1)). The EDPS welcomes the justification for the particular use of biometric data included in recital 10 of the 2016 EES Proposal itself, as well as throughout the Impact Assessment accompanying the Proposal[52]. The EDPS recognised at several occasions the advantages that could be provided by biometrics, but he always stressed that, given their very nature, these benefits would be dependent on the application of more stringent safeguards[53]. Any error of the system could have important adverse consequences[54] on third country nationals whose data will be in the system.

38. Any proposed system requiring the processing of biometric data should be accompanied by sufficient guarantees and safeguards in order to ensure the effective protection of data stored against the risk of abuse, mistake, unlawful access and use of these data. These guarantees and safeguards move the pendulum towards more proportionality. The EDPS already recommended implementing a non-exhaustive list of safeguards for automatically processing biometric data through the EES, in order to avoid that third country nationals carry the burden of imperfections of the system, e.g. in case of failure to enrol or error of the system in the use of biometrics[55].

39. The EDPS welcomes the impact assessment on fundamental rights carried out by the Commission[56], which focuses on the impact of the future EES on Article 7 and 8 of the Charter and addresses the relevance of biometric data in this context and the reasons behind the biometric identifiers chosen in the Proposal. However, the EDPS regrets that this document does not include an analysis of the impact of errors and failures of the biometric matching technology on third country nationals.

40. Article 33 of the 2016 EES Proposal rightly identifies the need to have high quality fingerprints. However, the quality of facial images when not taken from the electronic Machine Readable Travel Document (eMRTD) (i.e. passports) is not addressed, although the quality of facial images is of paramount importance. **The EDPS thus recommends that, in Article 14, a provision is added providing that in cases where facial images are taken live, a minimum quality level is required for these pictures. Furthermore, Article 33 should specify that the Commission will provide, by way of implementying measure, detailed information on how to reach this necessary quality level for facial images taken live.**

41. The EDPS also welcomes that Article 19 of the 2016 Proposal provides for fall-back procedures in case of a technical impossibility to enter data in the Central system or in case of failure.

b) Security of the system

42. Security of a system as described in Article 6 of the EES Proposal, which is spread across multiple entities (a central unit at eu-LISA and a National Uniform Interface (NUI) in each Member State) can only be achieved by taking a holistic view on the system, i.e. not limiting

oneself only to the security of the central unit but taking into account all other parts of the system and all users of the system. Furthermore, the security of the proposed EES system will be impacted by the security of other interconnected systems such as the national border infrastructure of each Member State.

43. The security measures taken on the system (central unit and NUI), including obligations of the users in the Member States, must be aligned as weakened security on any part of the system would affect the security of the system overall. For example, a security incident on one part of a national border infrastructure connected to a NUI might affect the security of the central unit of the EES.

44. Although Article 39 of the 2016 EES Proposal lays down security responsibilities for eu-LISA and the Member States, there is no mention of the need to ensure this alignment of security efforts across the board. **The EDPS recommends that Article 39 provides for this strong need for coordination between eu-LISA and Member States with regard to ensuring security. This alignment of security should be based on a proper information security risk management process that encompasses all elements of the new system, including the parts under the responsibility of the Member States.**

45. Article 6(c) mentions the need to have a *"Secure Communication channel between the EES Central System and the VIS Central System"* but Article 6(d) does not specifically mention security for the *"Communication Infrastructure between the Central System and the National Uniform Interfaces"*. **The EDPS recommends changing the text of Article 6(d) to *"a secure Communication Infrastructure between the Central System and the National Uniform Interfaces".***

46. Article 34 describes the development and operational management responsibilities for the Central System, the National Uniform Interfaces, the Communication Infrastructure and the Secure Communication channel between the EES Central System and the VIS Central System. However, Article 34 does not address security. It does not address privacy either. The EDPS submits that any new system, and any major change to an existing system (in this case, the VIS) can only be professionally achieved by:

- following a proper security process which includes a detailed analysis of the risks, and
- following Privacy by Design and by Default principles.

47. **The EDPS recommends adding the following requirements to Article 34:**

- performing a risk assessment as part of the development of this new system;
- following Privacy by Design and by Default principles in the whole lifecycle of the system development;
- updating the risk assessment for the VIS to take into account the new connection with the upcoming EES, and following up by implementing the additional security measures highlighted by the updated risk assessment.

c) Security of the web service

48. The EDPS understands the need to provide information to third country nationals in order for them *"to verify at any moment the remaining authorised length of stay"*, as well as the fact

that carriers would need to *"verify whether or not third country nationals holding a single or double entry visa have already used the visa"*. Pursuant to Article 12 of the 2016 EES Proposal, this would be achieved via a so-called secured internet access to a web service hosted by eu-LISA. However, from a security perspective, there are insufficient details in the 2016 EES Proposal as to the specific measures to ensure security of the personal data held within this web service and the specific allocation of responsibilities to ensure the security of the personal data in this web service, including when the personal data have been extracted and stored by the carriers.

49. **The EDPS understands that eu-LISA will be responsible for the security of the web service, the security of the personal data it contains and the process to get the personal data from the central system into the web service, and should thus be considered as controller as regards these issues. The EDPS recommends to clearly specify these responsibilties in the 2016 EES Proposal.** The specific security needs should be the outcome of an information security risk assessment performed by eu-LISA. This information security risk assessment should be updated on a regular basis. Eu-LISA should also be responsible for the proper implementation and monitoring of security controls defined as an outcome of the risk assessment.

50. The EDPS also has concerns with regard to the security of the personal data once the carriers have extracted them from the web service as there are no indications of their responsibility towards the security of these data. Article 33(1)(g) refers to implementation measures that the Commission would need to adopt prior to the development of the new system with regard to this web service; those implementation measures could be an opportunity to impose the need for some level of security on the personal data once it is extracted by the carriers.

51. Another security issue of this web service relates to how third country nationals and carriers would authenticate to the web service in order to request information. The authentication to the web service would be achieved by:

- for third country nationals: providing the data listed in Article 14(1)(b), i.e. the type, number and three letter code of the issuing country of the travel document or documents (Article 12(1));

- for carriers: providing the data listed in Article 14(1)(d), i.e. the short stay visa sticker number, including the three letter code of the issuing Member State, the type of visa, the date of end of maximum duration of the stay as authorised by the visa which needs to be updated at each entry and the date of expiry of the validity of the visa, if applicable (Article 12(2)).

52. With regard to third country nationals, authentication to the web service (only providing type, number and three letter code of the issuing country of the travel document or documents) may be weak; an a third party might just attempt to enter properly formatted data in the web service with the hope of confirming the link between a third country national of interest and his/her travel document details, and then get information on the third country national authorised length of stay. Additional pieces of information should be requested to the third country national using the web service in order to increase the difficulty of this type of attack on the web service whilst at the same time increasing the assurance that the person entering the request for a specific set of data is indeed the third country national concerned. For example,

requesting the date of birth in addition to the type, number and three letter code of the issuing country of the travel document or documents could be such a piece of information. However, determining exactly which additional pieces of information to request for a proper authentication of third country nationals should be one of the results of the risk assessment recommended in paragraph 49 above.

53. As carriers would have access to data of a wide number of third country nationals, it is necessary to ensure that only authorised staff members working for the carriers get access to the web service. Thus, a proper authentication scheme, not linked to third country nationals' data, should be set up (e.g. using login and password, token). The appropriate level of authentication should be determined based on the risk assessment mentioned previously. Furthermore, proper traceability of carrier requests to the web service should be ensured (logging) so as to hold them accountable if misuse of the web service is detected.

d) Interoperability between the EES and the VIS

54. The 2016 EES Proposal builds 'interoperability' between the EES and the VIS from the start, or more specifically 'interconnectivity' between the two systems. The Commission considers the interconnectivity of information systems as one dimension of interoperability and defines it as the fact that *"different systems or databases are able 'to talk to each other' technically"*[57]. Interconnectivity between the future EES and the existing VIS is a first step towards a long-term objective of the Commission, which was announced in the Communication on 'Stronger and Smarter Information Systems for Borders and Security' included in the second Smart Borders Package: to improve interoperability between existing and future EU information systems for border management and security.

55. The 2016 EES Proposal entrusts eu-LISA with the establishment of a direct communication channel between the central systems of both databases, allowing for direct consultation in-between these two systems (Article 7). The EES and the VIS will share the same technical features and a common biometric matching system. As a consequence, border authorities using the EES will also be able to consult the VIS for specific purposes defined in Article 7(2) of the 2016 EES Proposal, while visa authorities using the VIS will be able to consult the EES for specific purposes defined in Article 7(3). Article 55 of the 2016 EES Proposal also amends the VIS Regulation in order to ensure the interoperability between the two systems.

56. The Commission states that *"This will reduce the duplication of personal data processing in accordance with the 'privacy by design' principle"*[58]. Concretely, fingerprints of visa holders already stored in the VIS will not be stored once more in the EES, but instead the EES will re-use fingerprints of the VIS for the purposes of the EES avoiding that visa holders' fingerprints are stored twice, once in each system. The EDPS wonders why the same cannot be achieved with the facial images of visa required third country nationals, which are already stored in the VIS[59].

57. The EDPS is not *prima facie* against the interoperability of European large scale IT systems as long as full compliance with fundamental rights is ensured. He emphasises, however, that by doing so the risks of infringement of data protection principles, and in particular of the purpose limitation principle, may increase. As far as the EES and the VIS are concerned, the compatibility of the re-use of data collected in the context of the VIS for each

purpose of the EES should be assessed, and vice versa. The EDPS considers that the primary purposes of the two systems are closely related, and the data concerned identical to some extent. This would limit the risks of misuse.

58. Beyond the specific 2016 EES Proposal, the EDPS will analyse more in details the implications of the general objective of the Commission to move towards more interoperability in a separate exercise.

e) National facilitation programmes

59. The Commission decided to remove its 2013 RTP Proposal from the second Smart Border Package, but tabled a revised Proposal amending the Schengen Borders Code. One of the main changes of the 2016 Proposal amending the Schengen Borders Code is a new Article 8e, which introduces the possibility for Member States to establish national facilitation programmes for third country nationals who cross the external borders and who may benefit upon entry from derogations to the thorough checks. The Member States that voluntarily choose this option will be obliged to ensure a pre-vetting of the third country nationals applying to their programmes.

60. The new Article 8e also requires the Commission to carry out an evaluation of its implementation within three years of application. Based on this evaluation, the European Parliament or the Council may invite the Commission to propose the creation of a *"Union programme for frequent and pre-vetted third country national travellers"*. The EDPS will closely follow these developments.

61. National facilitation programmes will not require the development of any new system and rely on data retained in the EES. Therefore, Article 23 of the 2016 EES Proposal allows access to EES data by authorities referred to in Article 8e, for the purpose of examining applications for access to national facilitation programmes. The EDPS recommends to include this purpose in the list of specific purposes in Article 5 of the 2016 EES Proposal to ensure consistency.

62. In addition, there is no description of security measures or even the mention of the need for security in the new Article 8e. **The EDPS recommends that security responsibilities are made clear for all steps of the process, including when interconnecting voluntary programmes from different Member States to the EES. The EDPS also recommends specifying in the new Article 8e of the Schengen Borders Code that security must be ensured following a proper information security risk assessment.**

f) Data subjects' rights

63. The EDPS welcomes Articles 44 and 46 of the 2016 EES Proposal which provides for the third country nationals' right of information and rights of access, rectification and deletion of personal data.

64. The EDPS first has concerns regarding Article 46(6) of the Proposal, which makes requests for access, correction and deletion of personal data by *all* data subjects conditional upon the provision of their fingerprints. The EDPS understands the need to accompany such requests with personal data allowing the identification of some third country nationals as the rightful data subject. However, such requirement could create an important obstacle to the effective

exercise of the right of access which is an important guarantee for the data subject, even included in Article 8(2) of the Charter. **The EDPS advises the EU legislator to reconsider this prerequisite to the exercise of the right of access, for instance by limiting the use of fingerprints to cases where there are substantive doubts about the identity of the applicant.**

65. As regards the right of information, the EDPS welcomes that the 2016 EES Proposal now provides for a common leaflet and a website available in different languages possibly with additional specific information from Member States, in addition to the information already provided to third country nationals at the time of creation of their individual file. Nevertheless, **the EDPS recommends adding to the information listed in Article 44(1) the following elements**:

1) an explanation of the fact that the EES data will be accessed for border management and facilitation purposes, specifying that overstay will automatically lead to the addition of the individual's data on a list[60], as well as the possible consequences of overstaying;

2) the data retention period set for entry and exit records and for individual files; and

3) the right for overstayers to have their personal data deleted in case they provide evidence that they exceeded the authorised duration of stay due to unforeseeable and serious events[61].

66. As regards the right of access, **the EDPS recommends fixing a strict harmonised deadline that would be no longer than a few months to answer access requests in Article 46 (1)[62].** Respect for the right of access, as guaranteed by Article 8 of the Charter, and follow-up to access requests are of paramount importance since the exercise of this right allows data subjects to control the processing of their personal data and possibly to discover errors or unlawful access to their personal data. Moreover, Article 48 regarding 'Remedies' gives the possibility to data subjects to file an action or a complaint when the rights of access, correction and deletion were denied. For these rights to be effective, the same should apply in case requests to exercise these rights were not answered to within a strict deadline or were never dealt with by the controller.

67. The EDPS also welcomes Article 9(2) which explains that the EES' use may not lead to discrimination against third country nationals on the grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. Furthermore, the EDPS welcomes that special attention is directed towards children, the elderly and persons with a disability. However, the proposal fails to specify what additional safeguards would be implemented to ensure that this special attention towards children, the elderly and persons with a disability is duly respected. **The EDPS recommends that Article 9(2) be amended with a clear description of safeguards that would ensure that a proper attention is given to data relating to children, the elderly and persons with a disability.**

g) Statistics

68. The EDPS understands the need for the duly authorised staff of the competent authorities of the Member States, the Commission, eu-LISA and Frontex to produce reporting and

statistics on the data contained in the EES. However, the amount of data that may be accessed may allow for identification of individuals, contrary to what is stated in Article 57(1) and 57(2). For example, the combination of nationality, gender and date of birth of a third country national may lead to identification.

69. Furthermore, as eu-LISA will be required to extract that data and move them to a central repository, the risks of data leaks increase significantly as proper security measures are not devised.

70. **The EDPS therefore recommends a redrafting of Article 57 on "The use of data for reporting and statistics"**, recognising that the data listed under Article 57(1)(a to i) may lead to identification of individuals and thus must be protected in a similar way as the central EES repository. This includes performing a proper information security risk assessment, and implementing adequate security measures, prior to providing this additional central repository. The EDPS strongly cautions that the current proposed solution in Article 57 would impose a heavy burden on eu-LISA, which would have to maintain and secure appropriately a second repository, and on the EDPS which would have to supervise this second repository. **The EDPS would favour a solution which does not require an additional central repository but rather requires eu-LISA to develop functionalities that would allow the Member States, the Commission, eu-LISA and Frontex to automatically extract the required statistics directly from the EES Central System, without the need for an additional repository.**

h) The EDPS as Supervisor

71. Article 50 of the 2016 EES Proposal lays down the responsibilities of the EDPS as Supervisor of the future EES, one of which is to ensure that an audit of eu-LISA's personal data processing as regards this new system is carried out at least every four years.

72. However, the 2016 EES Proposal fails to provide the EDPS with the appropriate information so that these new responsibilities may be carried out effectively and efficiently. The EDPS should likewise be informed by eu-LISA of all reports that it will have to present to the Commission, the Council or the Parliament pursuant to the Proposal. **Thus, the EDPS recommends that:**

- in Article 36(3), the EDPS be informed of the measures eu-LISA takes pursuant to Article 36(2) not only for the start of the operations of the EES but throughout the whole lifecycle of the EES and its data;

- in Article 64(2), the EDPS also be informed of the reports regarding the state of play of the development of the Central System, the Uniform Interfaces and the Communication Infrastructure between the Central System and the Uniform Interfaces;

- in Article 64(4), the EDPS be provided the report regarding the technical functioning of EES every two years after the start of operations of the system;

- in Article 65(5), the EDPS be provided the Commission's reports regarding the overall evaluation of the EES.

73. Furthermore, **the EDPS recommends that a similar provision to Article 49(3) be added to Article 50 so that the EDPS be allocated the resources necessary to perform an adequate supervision of this new system**.

IV. Access by law enforcement authorities

74. The 2016 EES Proposal provides access to EES data to Member States' law enforcement authorities and Europol from the start of operations of the system[63]. The EES will be used as an identification tool to identify unknown suspects, perpetrators or victims, and as an intelligence tool to consult the travel history of known suspects.

75. The EDPS recognises the importance for law enforcement authorities to benefit from the best possible tools to find the perpetrators of terrorist acts or other serious crimes. Nonetheless, the EDPS recalls[64] that providing access to EES data to law enforcement authorities will have to comply separately with third country nationals' rights to privacy and data protection, and will trigger the same assessment of the necessity and proportionality in advance.

76. The EDPS recalls[65] that access to EES data by law enforcement authorities fits into a growing tendency of granting these authorities access to personal data of third country nationals who cross the EU borders[66], even though these travellers are in principle not suspected of unlawful conduct or otherwise under investigation.

IV.1 Law enforcement as a secondary objective

77. As explained above[67], the EDPS understands that the EES database will be in the first place set up for border management purposes, and that access to EES might then be granted to law enforcement authorities subject to strict conditions and safeguards. **The EDPS considers that the establishment of the described EES directly and primarily for law enforcement purposes would be unacceptable, and that the EES should remain a border management tool purely designed with this purpose in mind.**

78. However, Article 5 of the 2016 EES Proposal lists twelve purposes for *collecting*, *storing* and accessing EES data; the purposes (j), (k) and (l) are related to the secondary law enforcement purposes of the EES system. **The EDPS recommends modifying Article 5, to ensure that it reflects that the EES has primary and secondary purposes, and that specific purposes related to law enforcement be included as secondary purposes in a separate provision so that at least they do not appear listed on the same footing as other purposes related to border management and facilitation**.

IV.2 Necessity of law enforcement access

79. The EDPS stresses that the sole fact that EES data have been primarily collected for specific purposes -and thus are available- cannot itself justify the need to access and use these data for other purposes such as law enforcement[68]. In this respect, the EDPS recommended on several occasions to provide solid evidence of the need to access EES data for law enforcement purposes[69].

80. In the current Proposal, Recital 16 states that *"it is imperative that law enforcement authorities have the most up-to-date information if they are to perform their tasks"* and refers to the existing possibility for law enforcement authorities to access data from the VIS, which *"has already proven its usefulness"*[70]. The EDPS points out that what is considered useful cannot necessarily be considered necessary as such in terms of data protection[71], and that statements regarding necessity must be supported by clear evidence.

81. The Impact Assessment accompanying the Proposal also indicates that the VIS is effectively consulted by law enforcement authorities (i.e. 14000 consultations/months during the first eight months of 2015) and that *"such consultations are leading to successful resolution of serious crimes"*[72] without further indication. However, the EDPS takes note that, according to the Commission's Communication on 'Stronger and Smarter Information Systems for Borders and Security', Member States' law enforcement authorities have been using the possibility to access the VIS in an uneven way and have reported practical problems in the procedures[73]. Moreover, although Europol has the *legal* possibility to access the VIS since end 2013, it is in fact not connected to the database and does not yet exercise this possibility.

82. **The EDPS invites the Commission to provide further information, such as for instance available reports and/or statistics taking into account the experience already gained with the VIS (also for SIS and Eurodac), in order to support these assertions as well as to provide further objective evidence of the need for law enforcement authorities, including Europol, to gain access to EES data.**

IV.3 Conditions for access and safeguards

83. In the event that the necessity of such access were to be established, it should be demonstrated that this further processing complies with the requirement of proportionality set forth in Article 52(1) of the Charter. To meet this requirement, the CJEU gave guidance in the DRI Ruling[74] and specified that such access should be proportionate, narrowly targeted and based on suspicion as to a specific person. This access must be subject to strict conditions limiting access to specific cases and accompanied by appropriate safeguards.

84. The EDPS welcomes that Article 29 of the 2016 EES Proposal defines the conditions to be met for law enforcement authorities to get access to EES data through an electronic reasoned request, as well as the additional conditions laid down in Article 29(2) for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence.

85. Article 29(2) mentions that a prior search does not have to be conducted if there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject. The EDPS fails to see how a designated authority would know in advance, without performing searches on systems of the other Member States, if any relevant data would be found in those systems. **The EDPS invites the Commission to clarify Article 29(2).**

86. Moreover, the EDPS considers that the verifying mechanism of compliance with these conditions of access to EES data is an essential safeguard to prevent unlawful access. Article 26(3) of the EES Proposal places the responsibility of verifying that the conditions of access by national law enforcement authorities are fulfilled on designated central access points.

However, national designated authorities requesting access to EES data and verifying authorities granting such access can be part of the very same authorities. Indeed, Article 26(3) states that "*The designated authority and the central access point may be part of the same organisation if permitted under national law, but the central access point shall act independently when performing its tasks under this Regulation"* and adds that *"The central access point shall be separate from the designated authorities and shall not receive instructions from them as regards the outcome of the verification"*. **The EDPS recommends modifying this provision to impose that designated authorities and verifying authority are not part of the same organisation.** The same recommendation applies to the specialised unit of Europol officials that shall be designated by Europol as central access point pursuant to Article 27(2). Given the specificities of Europol, an effective mechanism should be found by which the prior authorisation to access EES data shall be subject to the scrutiny of a body that is sufficiently independent from the designated authority.[75]

87. The EDPS emphasises that the verifying authority must be effectively independent from the designated authority in order to guarantee a proper verification of compliance with the conditions. In this regard, the CJEU also held in the DRI Ruling that access by the competent national authorities should be *"made dependent on a prior review carried out by a court or by an* independent *administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued"*[76].

88. Furthermore, Article 28(2) provides for exceptional cases of urgency, for which compliance with all the conditions laid down in Article 29 could be checked *ex post*. The EDPS considers that exceptions should be regulated as precisely as possible. The Proposal provides that the *ex post* verification must take place *"without undue delay"* after the processing of the request. **The EDPS recommends setting a strict deadline to perform this verification starting as soon as the request has been processed.**

89. Finally, the EDPS welcomes that specific attention was given to the data subject's right to information in relation to law enforcement access in Article 44(1)(a), according to which a clear explanation regarding the possibility of access by national law enforcement authorities and Europol to EES data will be communicated to third country nationals.

4. CONCLUSION

90. The EDPS welcomes the work done by the Commission in the 2016 EES Proposal to address data protection concerns raised about the 2013 Smart Borders Package. Some of the EDPS' recommendations and comments in his previous Opinion on the Package have been duly taken into account, for example regarding the introduction of fall-back procedures in case of technical impossibility or failure of the system.

91. The EDPS welcomes the efforts made by the Commission to justify the necessity of setting up the EES scheme, but has main recommendations directly related to its proportionality in order to ensure full compliance of the EES with the essential prerequisite of Article 52(1) of the Charter to be both necessary and proportionate. He points out that necessity and proportionality of the EES scheme are to be assessed both globally, taking into consideration the already existing large-scale IT systems in the EU, and specifically, in the specific case of these third country nationals who are lawful visitors of the EU. He considers that a retention period of five years for all personal data stored in the EES should be fully justified. He also

stresses that the following aspects of the 2016 EES Proposal should be better justified and supported by convincing evidence: the collection of the facial image of visa-required travellers, the five years retention period for overstayers and the need for access to EES data by law enforcement authorities. *Quod non*, these aspects should be reconsidered by the EU legislator.

92. Furthermore, considering the wide-ranging interference with fundamental rights to privacy and data protection of third country nationals, the EDPS considers that the EES should remain a border management tool purely designed with this purpose in mind. Therefore, the difference between the stated objectives of EES, i.e. the primary objectives of border management and facilitation and the secondary objective of law enforcement, should be clearly introduced and reflected throughout the 2016 EES Proposal, in particular in relation to Articles 1 and 5.

93. In addition, the EDPS has concerns regarding the requirement for all data subjects to provide in any event fingerprints to submit any request for access, correction and deletion of their personal data. This could create an important obstacle to the effective exercise of the right of access, an important guarantee for the data subject included in Article 8(2) of the EU Charter.

94. Other recommendations of the EDPS in the present Opinion concern the following aspects and articles:

- Article 14 should be detailed so that, in cases where facial images of third country nationals are taken live, a minimum level of quality is reached for these pictures, and Article 33 should specify that the Commission will provide detailed information on how to reach the necessary level of quality for facial images taken live.

- Article 15(3) should be amended so as to specify what information may be collected, stored and use by the border authorities when they request further clarification on the grounds for the temporary impossibility to provide fingerprints.

- Article 39 should provide for the strong need for coordination between eu-LISA and Member States with regard to ensuring security of the EES.

- The security responsibilities should be made clear in the Proposal in case of interconnection of national facilitation programmes from Member States to the EES. The new Article 8e of the Schengen Borders Code should specify that security must be ensured following a proper information security risk assessment and describe the necessary security measures.

- The Proposal should clearly specify that eu-LISA is responsible for the security of the web service, the security of the personal data it contains and the process to get the personal data from the central system into the web service.

- Article 44(1) should be amended in order to include in the information communicated to data subjects: the retention period applying to their data, the right for overstayers to have their personal data deleted in case they provide evidence that they exceeded the authorised duration of stay due to unforeseeable and serious events and an explanation of the fact that the EES data will be accessed for border management and facilitation purposes.

- Article 46 (1) should fix a strict harmonised deadline that would be no longer than a few months to answer access requests.

- Article 9(2) should be amended with a clear description of safeguards that would ensure that a proper attention is given to data relating to children, the elderly and persons with a disability.

- Article 57 should be amended and require of eu-LISA to develop functionalities that would allow Member States, the Commission, eu-LISA and Frontex to automatically extract the required statistics directly from the EES Central System, without the need for an additional repository.

- The Proposal should provide the EDPS with the appropriate information and resources so that his new responsibilities as Supervisor of the future EES may be carried out effectively and efficiently.

- Article 28(2) should provide a strict deadline for the verifying authorities to perform the ex-post verification of the conditions to access EES data for law enforcement purposes in case of emergency.

- Article 28(3) should be modified to impose that designated authorities and the verifying authority are not part of the same organisation.

95. The EDPS insists on the need to address these issues in a global perspective. He encourages the legislator to continue his exercise of mapping the different databases in the border and migration context, better coordinating and avoiding overlap between the different systems, while fully respecting data protection standards and in its relations with third countries.

Brussels, 21 September 2016

(**signed**)

Giovanni BUTTARELLI
European Data Protection Supervisor

NOTES

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] OJ L 350, 30.12.2008, p. 60.
[4] Commission Communication of 13 February 2008 on 'Preparing the next steps in border management in the European Union', COM(2008) 69 final.
[5] EDPS Preliminary comments of 3 March 2008 on three Communications on border management.
[6] EDPS Opinion of 7 July 2011 on the Communication on Migration.
[7] Commission Communication of 25 October 2011 on 'Smart borders - Options and the way ahead', COM(2011) 680 final.
[8] The Article 29 Working Party commented on the Communication from the Commission on Smart Borders in a letter addressed to Commissioner Malmström of 12 June 2012.
[9] EDPS Round Table on the Smart borders package and data protection implications, Brussels, 10 April 2013, see summary available 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.
[10] 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, COM(2013) 95 final.
[11] Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, COM(2013) 97 final.
[12] 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), COM(2013) 96 final.
[13] EDPS Opinion of 18 July 2013 on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP).
[14] Article 29 Working Party Opinion 05/2013 of 6 June 2013 on Smart Borders.
[15] Technical Study on Smart Borders - Final Report, October 2014, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf.
[16] Technical Study on Smart Borders - Cost Analysis, October 2014, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf.
[17] eu-LISA Final Report on the Smart Borders Pilot Project, December 2015, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm
[18] Commission public consultation on Smart Borders, available at: http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm.
[19] EDPS Formal comments of 3 November 2015 on the Commission Public Consultation on Smart Borders.
[20] See Press release available at: http://europa.eu/rapid/press-release_IP-16-1247_en.htm.
[21] Commission Communication of 6 April 2016 on 'Stronger and Smarter Information Systems for Borders and Security', COM(2016) 205 final.
[22] COM(2016) 194 final.
[23] Regulation (Eu) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification), OJ L 77, 23.3.2016, p. 1.
[24] COM(2016) 196 final.
[25] Commission Staff Working Document of 6 April 2016 on 'Impact Assessment on the establishment of an EU Entry/Exit System accompanying the 2016 EES Proposal and the 2016 Proposal amending the Schengen Borders Code', SWD(2016) 115 final (hereinafter "Impact Assessment").
[26] http://data.consilium.europa.eu/doc/document/ST-8485-2016-INIT/en/pdf.
[27] Two workshops between DG Home and the EDPS addressing Smart Borders' aspects were held in 2015: one workshop on 20 March specifically dedicated to the preparation of the Smart Borders proposals, and one interactive workshop on 21 September 2015 on Data Protection and Privacy Considerations in Policies on Migration and Home Affairs during which the 2013 Smart Borders proposals were also touched upon; see Minutes of the workshop of 20 March 2015 in Annex 16 to the Impact Assessment.

[28] The term 'overstayer' is defined in Article 3(1)(18) of the 2016 EES Proposal 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"*.
[29] The 2016 EES Proposal excludes from its scope third country nationals who are beneficiaries of Directive 2004/38/EC and hold the appropriate residence card, holders of residence permits referred to in Article 2(16) of the codified Schengen Borders Code, holders of long-stay visas, nationals of Andorra, Monaco and San Marino, and persons or categories of persons exempted from or benefiting from facilitation of border crossing according to the Schengen Borders Code (Article 2(3)).
[30] See page 5 of the Impact Assessment.
[31] Articles 14 to 18 of the EES Proposal exhaustively list the personal data that will be collected and stored in the EES for both visa-required and visa-exempted third country nationals.
[32] See page 34 of the Impact Assessment according to which e.g. the name at birth and the place of birth should not appear anymore in the future EES.
[33] Article 29 Working Party Opinion 03/2012 of 27 April 2012 on developments in biometric technologies; ECtHR, S. and Marper v. United Kingdom, 4 December 2008, Application nos. 30562/04 and 30566/04, §§ 84-85, in which the European Court of Human Rights considered that fingerprints *"objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances"* and that the retention of such data could give rise to important private-life concerns.
[34] See pages 2 and 3 of the Explanatory Memorandum to the 2016 EES Proposal.
[35] See pages 58 and 65 of the Impact Assessment; border management and facilitation are also referred to as *"the prime purpose of EES"* on page 65 of the document. In addition, Annex 13 to the Impact Assessment on 'Impact Assessment on Fundamental Rights' makes the same reference to *"primary objective"*.
[36] See page 37 of the Impact Assessment; law enforcement is also referred to as *"the secondary purpose"* on pages 38 and 65 of the document. In addition, Annex 13 to the Impact Assessment on 'Impact Assessment on Fundamental Rights' makes the same reference to *"secondary objective"*.
[37] See *infra* § 28, 35 and 82.
[38] See *supra* Section I on 'Impact of the EES on privacy and data protection'.
[39] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), ECLI:EU:C:2014:238 (hereinafter "DRI Ruling").
[40] See Annex 13 to the Impact Assessment on 'Impact Assessment on Fundamental Rights', p. 127.
[41] The 2013 EES Proposal provided for a maximum data retention period of 180 days (Article 20).
[42] The Proposal makes a distinction between so-called 'individual files', which will include "identity data" (e.g. names, date of birth, etc.), passport information and biometric data, and entry/exit records or refusal of entry records that correspond to the date and place of entry/exit or of refusal of entry.
[43] DRI Ruling, §64.
[44] See page 37 of the Impact Assessment.
[45] For instance, in case the third country national marries an EU citizen.
[46] See Article 20(3) of the 2013 EES Proposal.
[47] Recital 27 of the 2016 EES Proposal considers the chosen period of five years necessary *"in order to support the identification and return process"*.
[48] EDPS Opinion of 18 July 2013, §76; EDPS Formal comments of 3 November 2015, p. 9.
[49] See page 6 of the Explanatory Memorandum to the 2016 EES Proposal and Article 24(3) of the SIS II Regulation which provides that *"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"*.
[50] See Articles 10 and 11 of the 2013 EES Proposal.
[51] See page 30 of the Impact Assessment.
[52] See Annex 13 to the Impact Assessment on 'Impact Assessment on Fundamental Rights', p. 125.
[53] EDPS Opinion of 18 July 2013, §64 and EDPS Formal comments of 3 November 2015, p. 6.
[54] Consequences of the identification as overstayer in the EU could be e.g. the refusal of another visa later on, when the individual has finally left the EU territory and wishes to come back, or it is also a reason to return the third country national to his/her country of origin.
[55] EDPS Opinion of 7 July 2011, §31, EDPS Formal comments of 3 November 2015, p. 6 and EDPS Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II), section 4.1. on Biometrics.
[56] Annex 13 to the Impact Assessment on 'Impact Assessment on Fundamental Rights'.
[57] Commission Communication of 6 April 2016 on Stronger and Smarter Information Systems for Borders and Security, COM (2016) 205 final, p. 16.

[58] See page 5 of the Explanatory Memorandum to the 2016 EES Proposal.
[59] See *supra* §35.
[60] See Article 11 of the 2016 EES Proposal.
[61] See Article 32(5) of the 2016 EES Proposal.
[62] Article 12 of Directive 95/46/EC.
[63] The 2013 EES Proposal envisaged such access as a possible option that could intervene based on an evaluation of the system two years after its entry into operation (Article 46(5)).
[64] Annex 16 to the Impact Assessment on 'Preparatory work with the European Data Protection Supervisor', p. 142.
[65] EDPS Opinion of 18 July 2013, §68 and EDPS Formal comments of 3 November 2015, p. 5.
[66] Such tendency has been observed in the past years and will most probably develop further in the near future in light of the proposed ECRIS Regulation, which extends the existing system to criminal records of third country nationals, and the proposed 2016 Recast of the Eurodac Regulation, which will extend the purposes of the system, thus also extending the amount of data that national law enforcement authorities may have access to.
[67] See *supra* §20.
[68] Article 29 Working Party Opinion 03/2013 of 2 April 2013 on purpose limitation.
[69] EDPS Opinion of 18 July 2013, §69 and EDPS Formal comments of 3 November 2015, p. 4 and 10.
[70] Recital 16 of the 2016 EES Proposal.
[71] The ECtHR found that the notion of necessity does not have the flexibility of expressions such as *"admissible"*, *"*ordinary" or *"useful"*, but that it *"implies a pressing social need"*; see ECtHR, Handyside vs United Kingdom, 7 December 1976, Application no. 5493/72, §48.
[72] See page 67 of the Impact Assessment.
[73] Commission Communication of 6 April 2016 on 'Stronger and Smarter Information Systems for Borders and Security', COM (2016) 205 final, p. 8-9.
[74] DRI Ruling, §58-68.
[75] For the same reasoning, see §58 of EDPS Opinion 7/2016 of 21 September 2016 on the First reform package on the Common European Asylum System.
[76] DRI Ruling, §62.