



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 07/2016

EDPS Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)



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 is a key element of the EU first package improving the Common European Asylum System (CEAS).

Executive Summary

Since several years, Europe is faced with a pressing migration and refugee crisis, which became even more challenging in 2015. Therefore, the Commission proposed to reform the Dublin Regulation in order to adapt it to the current situation. This reform is combined with a Proposal for the creation of a European Union Agency for Asylum, to assist Member States to perform their duties regarding asylum.

Since it was established, Eurodac has served the purpose of providing fingerprint evidence to determine the Member State responsible for examining the asylum application made in the EU.

A recast of the Eurodac Regulation was also proposed by the Commission. The main change in this Regulation is the extension of the scope of Eurodac to register the third country nationals illegally found in a Member States or apprehended in connection with the irregular crossing of a border of a Member State with a third country.

The EDPS recognises the need for more effective management of migration and asylum in the EU. However, he recommends important improvements to better consider the legitimate rights and interests of the relevant individuals who may be affected by the processing of personal data, in particular of vulnerable groups of people requiring specific protection such as migrants and refugees.

In his Opinion, the EDPS recommends, among others, the following main points:

- mentioning in the Dublin Regulation that the introduction of the use of unique identifier in the Dublin database may not, in any case, be used for other purposes than the purposes described in the Dublin Regulation;
- the performing of a full data protection and privacy impact assessment in the Eurodac recast 2016 in order to measure the privacy impact of the new text proposed and of the extension of the scope of Eurodac database;
- conducting an assessment of the need to collect and use the facial images of the categories of persons addressed in the Eurodac recast 2016 and on the proportionality of their collection, relying on a consistent study or evidence-based approach;
- conducting a detailed assessment of the situation of minors and a balance between the risks and harms of the procedure of taking fingerprints of the minors and the advantages they can benefit, in addition to the Explanatory Memorandum.

The Opinion further defines other shortcomings of the different proposals and identifies additional recommendations in terms of data protection and privacy that should be taken in consideration in the legislative process.

TABLE OF CONTENTS

I. INTRODUCTION AND BACKGROUND	5
II. EDPS MAIN RECOMMENDATIONS	6
II.1. THE DUBLIN PROPOSAL.....	6
II.2. THE EURODAC RECAST 2016 PROPOSAL	7
a) <i>Extension of the scope of Eurodac</i>	7
b) <i>The obligation to take fingerprints and facial images</i>	8
c) <i>The retention period</i>	10
d) <i>Access for law enforcement purposes</i>	11
III. ADDITIONAL RECOMMENDATIONS	11
III.1. THE EURODAC RECAST PROPOSAL	11
a) <i>Advanced deletion and marking of the data</i>	11
b) <i>International transfers and further processing</i>	12
c) <i>The possibility to introduce sanctions, including detention</i>	13
d) <i>Operational management</i>	14
d) <i>Access</i>	15
III.2. THE EUAA PROPOSAL	16
a) <i>Relations between the experts of the Agency and the Member States' authorities</i>	16
b) <i>Access of databases by the Agency</i>	16
c) <i>The processing of data by the Agency</i>	16
d) <i>The information system to be developed by the Agency and technical means to be used by the Agency</i>	17
IV. CONCLUSION	18
NOTES	21

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,

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, 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,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION AND BACKGROUND

1. On April 2016, the Commission adopted a Communication entitled "Towards a reform of the Common European Asylum System legal avenues to Europe"¹, defining priorities for improving the Common European Asylum System (CEAS). In this context, on 4 May 2016, the Commission issued three proposals as part of a first package of reform of the CEAS:

- a Proposal for a Regulation of the European Parliament and of the Council on the 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 (hereinafter "the Dublin Proposal")² ;
- a Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010 (hereinafter "the Proposal for a European Union Agency for Asylum" or "the EUAA Proposal")³; and
- a Proposal for a Regulation of the European Parliament and of the Council on amending Regulation (EU) No 603/2013 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, for identifying an illegally staying third country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast 2016) (hereinafter "the Eurodac Recast 2016 Proposal")⁴.

2. The EDPS was consulted informally before the publication of the Eurodac Recast and the EASO Proposal and communicated informal comments to the Commission on both texts.

3. The EDPS understands the need for the EU to address the challenges of the migration and refugee crisis since 2015, as well as the need to have an effective and harmonised EU policy to tackle irregular immigration that occurs within the EU as well as to the EU. In full respect for the role of the legislator in assessing the necessity and the proportionality of the proposed measures, the EDPS, in his advisory role, will provide in this Opinion some recommendations in terms of data protection and privacy, in order to help the legislator to meet the requirements of Articles 7 and 8 of the Charter of Fundamental Rights regarding the rights to privacy and data protection and Article 16 of the Treaty on the Functioning of the EU.

4. The EDPS will first address the main recommendations regarding the three proposals. These main recommendations represent the major issues observed by the EDPS and that should in any event be addressed in the legislative process. Additional recommendations are the points identified by the EDPS as requiring clarification, additional information, or minor modifications. This distinction should help the legislator to give priority to the major issues addressed by this Opinion.

II. EDPS MAIN RECOMMENDATIONS

II.1. The Dublin Proposal

5. The Dublin Proposal aims to:

- enhance the Common European Asylum System to determine efficiently and effectively a single Member State responsible for examining the application for international protection,
- complement the current system with a corrective allocation mechanism, in case Member States have to deal with a disproportionate number of asylum seekers, and
- discourage abuses and prevent secondary movements of applicants within the EU, in particular by including clear obligations for applicants to apply for asylum in the Member States of first entry and remain in the Member State determined as responsible.

6. The following remarks will focus on the modifications of the Dublin Regulation that have an impact on individuals' data protection and privacy.

7. The Proposal establishes a new centralised registration and monitoring system that provides for the registration of all applications and that will enable the monitoring of each Member State's share in applications. Under this new database, run by eu-LISA, each Member State shall register the application in the automated system, under a unique application number⁵.

8. The EDPS takes note that the recast of the Dublin Regulation provides an exhaustive list of data which may be stored in the electronic file of each applicant (Article 23)⁶. This list appears *prima facie* to be proportionate to the purpose of the Dublin regulation, *i.e.* ensuring quick access of asylum applicants to an asylum procedure and the examination of an application by a single and clearly determined Member State.

9. However, the use of a unique identifier for each applicant's file requires specific safeguards, because it makes it easier to check one individual in several databases, also outside the domain of asylum, and may also allow the profiling a person on the basis of his or her unique identifier. To prevent misuse of data, the use of a unique identifier must be limited to specific purposes, to a specific context and to a particular environment. Therefore, **the EDPS recommends mentioning in the Regulation that the unique identifier may not, in any case, be used for other purposes than the purposes described in the Dublin Regulation**, in full respect of the purpose limitation principle.

II.2. The Eurodac Recast 2016 Proposal

10. The following remarks will focus on the modifications of the Eurodac Regulation that have an impact in terms of data protection and privacy.

a) Extension of the scope of Eurodac

11. The Eurodac recast 2016 extends the scope of the original Eurodac database. Eurodac was originally set up to provide fingerprint evidence to assist determining the Member State responsible for examining an asylum application made in the EU. Its primary objective was to serve the implementation of the Dublin Regulation.

12. The extension of the scope of Eurodac as proposed in the recast 2016 extends its scope for the purposes of identifying illegally staying third country nationals and those who have entered the European Union irregularly at the external borders, with a view to use this information to assist Member States to re-document a third country national for return purposes.

13. This new purpose of Eurodac has been described in Article 1 (b) of the Recast proposal as follows: “*assist with the control of illegal immigration to and secondary movements within the Union and with the identification of illegally staying third-country nationals for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation*”.

14. The extension of the scope of Eurodac is even more important from the perspectives of privacy and data protection in the light of the Commission's Communication on Stronger and Smarter Systems for Borders and Security, which highlights the need to improve interoperability of information systems as a long-term objective⁷. The EDPS will closely follow and pay the greatest attention to the trend to create communication between the available databases, extend their initial purposes and create more possibilities for massive collection of information on certain categories of individuals. The EDPS intends to deal with the interoperability issue, in a separate document to be adopted soon.

15. In the EDPS' view, the objective as described in Article 1 (b) remains vague since it does not specify which specific measures can be taken by the Member States, along with removal and repatriation. As the scope and the objective of a processing of personal data is to be defined as precisely as possible, **the EDPS recommends further specifying the type of measures that could be taken by the Member States in this context**⁸, for example by including an exhaustive list of the measures that can be taken thanks to Eurodac database in relation to the purposes pursued. Such an explanation could help understanding what is the added value of the Eurodac database.

16. As it was already stated in several Opinions of the EDPS⁹, the **extension of the purpose of a database raises the issue of the purpose limitation principle**, according to which data shall be used in accordance with the original purposes for which they have been collected. **The EDPS has concerns about the extension of the scope of Eurodac, which was primarily designed as a database supporting the implementation of the Dublin Regulation.**

17. **The extension of the scope of the Eurodac database does not only raise** concerns in relation to the purpose limitation principle, but **can in relation to the proportionality of the processing**: a database, regarded as proportionate when used for one specific purpose, can become inadequate or excessive when the use is expanded to other purposes afterwards¹⁰.

18. The EDPS regrets that the recast does not refer to any impact assessment of the new provisions as to the proportionality of the measure (*i.e.*: what kind of measures can be taken once the individuals have been identified as illegal?). Such an impact assessment appears to be an essential requirement for an adequate assessment of an EU policy which will have a substantive impact on the individuals concerned by the database. The mere statements contained in the Explanatory Memorandum referring to the principle of *privacy by design*¹¹ or to the fundamental rights¹² do not explain in substance how the approach followed by the proposal could not have been better addressed by less intrusive measures, or how the proposal could reduce its impact on privacy and data protection rights. **The EDPS therefore recommends that the Commission makes available a full data protection and privacy impact assessment in the Eurodac recast 2016 in order to measure the privacy impact of the next text proposed.**¹³ The EDPS notes, in this context, that such an exercise has been performed for the Second Smart Borders Package, as underlined and welcomed in the EDPS Opinion on the Second EU Smart Borders Package issued on the same day as the current Opinion.

b) The obligation to take fingerprints and facial images

- the use of additional biometric data: the facial image

19. Presently, the Eurodac Regulation only requires that the fingerprints of the applicants for international protection are collected and stored in the Eurodac central System. The Proposal adds another type of biometric data, *i.e.* the facial image of the individuals.

20. The EDPS notes that the Proposal does not give any explanation as to the choice to use additional biometric data, in particular the facial image for the purpose of facial recognition. The Explanatory memorandum refers to the Commission Communication on a European Agenda on Migration¹⁴ where it would be suggested to add biometric data to EURODAC in order to mitigate some of the challenges that Member States were facing with damaged fingertips and non-compliance with the fingerprinting process. However, the Commission Communication does not contain any reference to the case of damaged fingerprints and cannot therefore serve as a justification to collect facial images.

21. In addition, since biometric data are highly delicate, their collection and use should be subject to a strict analysis before deciding to register them in a general database where a large amount of persons will have their personal data processed. In this respect, the Proposal provides that eu-LISA will conduct a study on facial recognition software to evaluate the accuracy and

reliability before the software is added to the Central System¹⁵. The EDPS considers that such an evaluation should have been performed before including such data and the facial recognition software in the Eurodac database.

22. The assessment of eu-LISA is a purely technical assessment, while no evaluation of the necessity to insert facial recognition seems to be performed or foreseen in the Proposal. Therefore, in view of the risks posed by the introduction of such sensitive data in a large scale data base, **the EDPS recommends conducting or making available an assessment of the need to collect and use the facial images of the categories of persons addressed in the Eurodac recast Proposal and of the proportionality of their collection, relying on a consistent study or evidence-based approach¹⁶.**

23. Furthermore, the EDPS notes that Articles 15 and 16 of the Proposal appear to be contradictory: while Article 15 provides that a systematic comparison of fingerprints and facial image shall be ensured by the Member States and eu-LISA, Article 16 provides that facial recognition shall only occur as a last resort where the quality of fingerprints does not allow for a comparison, or where the individual refused to comply with the fingerprinting procedure. **The EDPS recommends clarifying that comparison of fingerprints and/or facial images shall only take place as last resort.**

-the lowering of the minimum age to take fingerprints

24. The Proposal provides for a new minimum age of the children from whom the biometrics data can be taken. This age will now be 6 years, instead of 14 years previously, on the basis of a report of the Joint Research Centre¹⁷ that indicates that fingerprints taken from children age of six and above can be used in automated matching scenarios such as Eurodac when sufficient care is taken to acquire good quality images.

25. Recital 20 a states that *"third-country nationals who are deemed to be vulnerable persons and minors should never be coerced into giving their fingerprints or facial image"*. Article 2.2 provides that the fingerprinting process of children must take place in a child-friendly and child-sensitive manner, with appropriate information to the children, who will be accompanied by an adult.

26. The EDPS welcomes these safeguards, considering that minors under 14 years old are vulnerable and not in a position to fully understand the circumstances surrounding the processing of their data, especially when these data are highly sensitive as biometric information. The EDPS understands the reasons why such an age was lowered as explained in the Explanatory Memorandum¹⁸, relating to the case of separation of the children from their families or escaping from care institutions or child social service.

27. However, the main argument used by the Proposal, based on the fact that many Member States collect biometrics from minors at a younger age than 14 years for visas, passports, biometric residence permits and general immigration purposes, is not convincing as such. The mere fact that some Member States have adopted this practice does mean that such measure is efficient, proportionate and useful. **The EDPS recommends that a detailed assessment of the situation of minors and a balance between the risks and harms of such procedure for the minors and the advantages that they can benefit from should be better developed in the Explanatory Memorandum. Additionally, the EDPS recommends specifying what is**

understood by the terms "in a child-friendly way", since this may lead to numerous interpretations depending on the competent authority.

c) The retention period

28. According to Article 18 (2) and (3), the categories of data mentioned in Articles 14(1) and 17(1) will be stored for a period of five years. To justify this new obligation to retain these categories of data, the Explanatory Memorandum refers to the fact that Eurodac is no longer a database for asylum applicants only and such a retention period would be necessary to ensure that illegal immigration and secondary movements within and to the EU can be sufficiently monitored.

29. Furthermore, according to the Explanatory Memorandum, the five years period is aligned with the maximum period for placing an entry ban on individuals for migration purposes as set out in the Return Directive¹⁹, the data retention period for storing information on a visa in the Visa Regulation²⁰, and the proposed data retention period for storing data in the Entry/Exit System²¹.

30. According to EU data protection law, personal data should only be kept for a period necessary for the purposes for which the data were initially collected and further used²². The EDPS considers that a reference to the retention period of other instruments is not relevant as such as these instruments may have other purposes and their retention period might be justified by other elements. Recital 33 of the Proposal also refers to the right to protection of personal data, as an element having been considered to determine the five years period of retention proposed. However, the Recital does not explain how the right to data protection has been taken into account to define the retention period.

31. For all these reasons, the EDPS considers that the retention period of five years is not sufficiently justified by the Proposal, and recommends giving more details and explanation why such a period of five years (and not a longer or shorter period) is necessary in this context to achieve the new purposes of the Eurodac database. Moreover, the EDPS recommends explaining in more details how data protection has been taken into account in practice.

32. Furthermore, even if it was justified in principle to align the retention period of the said data on the theoretical maximum period for placing an entry ban (*i.e.*, five years), in such case, the retention period should be aligned on the *actual* duration of the entry ban placed upon a specific third country national, which may be less than five years. That means that once an entry ban on an individual has expired, the information on this individual should be erased from the Eurodac database, and not only after a period of five years, which is a theoretical maximum period. **The EDPS recommends therefore reducing in any case the retention period to the actual length of the entry ban upon a specific individual, up to a maximum of five years.**

33. Finally, the starting point of the retention periods is supposed to be the date on which the fingerprints were taken.²³ However, the fingerprints can be taken several times, by different operators which can even be in different Member States. If fingerprints are taken in connection with the irregular crossing of a border for the first time²⁴, they can be taken several times afterwards in case the migrant is found illegally staying in the territory of a Member State²⁵. This way, the EDPS understands that the period of storage can be reviewed each time an

individual is found in relation with the illegal crossing of a border or on the territory of a Member State. This would lead to a retention period which would be theoretically unlimited. For this reason, **the EDPS recommends specifying in the Proposal that the starting point of the retention period will be the date of the first fingerprinting processed by a Member State.**

d) Access for law enforcement purposes

34. While data of applicants for international protection is blocked ("not accessible") for law enforcement purposes after three years, this will not be the case for the data of individuals who do not apply for or were not granted international protection²⁶. The explanation given by the Explanatory Memorandum²⁷ refers to the likelihood of renewal of residence of asylum seekers, which would be greater than for non-asylum seekers.

35. The EDPS does not understand why law enforcement authorities should have a longer access to the data category relating to individuals without international protection. There is no indication or evidence that this category of individuals would be more subject to law enforcement investigations than asylum seekers who obtained international protection. Furthermore, the mere likelihood of a renewal of the residence permit cannot justify such a difference of treatment. **Therefore, the EDPS recommends aligning the blocking of data of both categories of individuals for law enforcement purposes on the existing three years period.**

III. ADDITIONAL RECOMMENDATIONS

III.1. The Eurodac recast Proposal

a) Advanced deletion and marking of the data

36. Under the current Eurodac Regulation, the data of illegally staying third country nationals who do not lodge an application for asylum within the EU are in specific cases erased "in advance", which means that their data are erased before the retention period of 18 months. This advanced erasure of the data occurs once a residence permit or nationality of a Member State is obtained, or when the individual has left the territory of the Member States.

37. The Eurodac recast Proposal provides that data will no longer be deleted in advance for illegally staying third country nationals or stateless persons who were granted a residence document or left the territory of the European Union. According to the Explanatory memorandum, "*it is necessary to retain this data in case at some point a residence document, which normally confers limited leave, is no longer valid and the individual overstays, or the illegally staying third-country national who had returned to a third country may attempt to re-enter the EU in an irregular manner again*".

38. Instead of being erased in advance, the Eurodac recast Proposal provides that the data of migrants who received a residence document will be "marked"²⁸. The EDPS would like to mention that the term "marking" is not defined in the Eurodac Regulation, and the recast Proposal does not indicate what type of information the mark should contain. Therefore, **the**

EDPS recommends defining what is meant by “marking” under the Eurodac Regulation and indicating what information should be contained in such marking.

39. Regarding law enforcement purposes, the marking of data appears to be an intermediary step between the full use of data for the purposes initially provided, and the erasure of the data. In this case it means that the data will still be accessible for law enforcement purposes. However, for the categories of illegally staying third country or stateless persons²⁹, marking under Article 19 (4) would have another function, that is the transmission of the status of an individual with a residence permit in a Member States to the authorities of another Member State. Therefore, **the EDPS also recommends defining in the recast Proposal what the objective of the marking of data is and explaining the difference of marking for law enforcement purposes³⁰ and for migration control purposes³¹.**

40. Individuals, who have obtained a resident permit in a Member State, would then remain in the Eurodac database with a marking of their data, whereas data relating to a person who has acquired citizenship of a Member State shall be erased from the database as soon as the Member State of origin becomes aware that the person concerned has acquired such citizenship. A third category of individuals, the asylum seekers who were granted international protection, will be registered in the Eurodac database for five years, but with a limited access of three years to their data by the law enforcement authorities.

41. The EDPS considers that such a difference of treatment between different categories of non-EU individuals, with respect to the access to their data for law enforcement purposes, is not satisfactorily explained in the Proposal. Indeed, there is no evidence showing the necessity of a longer access for law enforcement purposes for the legally staying individuals with a residence permit compared to the persons who were granted international protection. **The EDPS therefore recommends extending the application of the limited period of access for law enforcement purposes (three years) to the individuals who were granted a residence permit by a Member State.**

42. **Furthermore, the EDPS recommends providing for an obligation for each Member State granting or recognising citizenship to an individual to transmit this information to eu-LISA so that the individual can be removed from Eurodac in an automatic and systematic manner.** The wording used in Article 18 (1) can indeed suggest that the advanced deletion of the data of a former non-EU citizen could not intervene immediately since it depends on the information of the Member State of origin.

b) International transfers and further processing

43. Article 37 of the Proposal refers to a general prohibition to transfer the personal data obtained pursuant to the Proposal to any third country, international organisation or private entity established in or outside the Union. According to this provision, the same prohibition shall apply for any further processing of the data at national level within the meaning of Article 3 of Directive 2016/680³².

44. The reasons why only Directive 2016/680 is mentioned is not clear: the processing of personal data is also regulated in identical terms by Directive 95/46 which will be replaced by the General Data Protection Regulation (Regulation 2016/679)³³ in May 2018. In cases where the processing takes place in the context of law enforcement and asylum/immigration, both

Directive 2016/680 and the General Data Protection Regulation might even be applicable at the same time.

45. One could think that the intention of the last part of this paragraph was to avoid any further use by any other entity of the data collected pursuant to the Eurodac Regulation, for other purposes than the objectives mentioned in Article 1 of the Proposal. Should it be the case, the EDPS would like to recall that the purpose limitation principle is enshrined in Article 5 b) of Regulation 2016/679 and in Article 4 b) of Directive 2016/680. Therefore, a reference to these provisions could help to shed light on the objective of the text.

46. For these reasons, **the EDPS recommends clarifying the meaning of the last part of the first paragraph of Article 37**, and making it consistent with the new data protection framework that will apply and be implemented in May 2018, for example by making a reference to the purpose limitation principle on one hand, and to the principles regarding international transfers on the other hand (such a reference is already stated in paragraph 4).

47. Furthermore, the articulation between the general principles for international transfers as stated in paragraphs 1, 2 and 3 of Article 37, and the cases where such transfers are permissible under the Regulation 2016/679 and Directive 2016/680, as stated in paragraph 4, is not clear. It is difficult to understand whether an international transfer is prohibited as a rule, and whether each of the paragraphs of this provision are cumulative or should be read separately. **The EDPS suggests clarifying in which case an international transfer is allowed or prohibited under the different paragraphs of Article 37.**

48. A new paragraph 3 has been added to Article 37 with the aim of prohibiting the transfer to a third country of information regarding the fact that an application for international protection has been made in a Member State, particularly where that third country is also the applicant's country of origin. First, while the EDPS understands and supports the objective of the measure, this new principle does not seem to add anything to the prohibition of transfers included in Article 37.1 of the Proposal³⁴. Second, the EDPS does not understand the meaning of the last part of the sentence, which specifies that this prohibition should have a particular effect where the country is also the applicant's country of origin³⁵. If the prohibition is general, then the prohibition could not be applied with a greater attention when the data of the applicant might be transferred to his/her country of origin. **The EDPS recommends clarifying the meaning of the last part of this paragraph, for example by explaining whether there should be a difference in case the country that will receive data is the applicant's country of origin.**

49. Article 38 provides for the possibility to transfer data for return purposes. This is derogation to the general prohibition to transfer the data to a third country or an international organisation stated by Article 37. In accordance with the proportionality and the data minimisation principles, **the EDPS recommends mentioning in Article 38.1 that only the data strictly necessary for the purpose of return can be transferred by the Member States.**

c) The possibility to introduce sanctions, including detention

50. Article 2.3 of the Proposal provides that Member States may introduce administrative sanctions, in accordance with their national law, for non-compliance with the fingerprinting process and capturing a facial image. This provision also mentions detention, which should

only be used *"as a means of last resort to verify or determine a third-country national's identity"*.

51. The EDPS believes that the wording of this provision may create some confusion since it seems to imply that detention may be considered as a sanction for non-compliance with the fingerprinting process. However, since the Proposal provides that such a detention measure would only be permissible to verify or determine one's identity, such a measure should not be considered as a sanction for non-compliance with the obligation to provide fingerprints.

52. Furthermore, the EDPS does not understand how a sanction or a penalty can be an "effective, proportionate and dissuasive"³⁶ incentive for an immigrant to comply with the fingerprinting process. The reference to the Commission staff working document³⁷, referred to in the Proposal, does not give further guidance in this respect.

53. In this context, it must be reminded that Return Directive³⁸ does not explicitly provide that a detention penalty can be applied in case of non-compliance with the fingerprinting process, contrary to what seems to be implied by the Commission staff working document mentioned above.

54. Finally, the EDPS shares the views of the Eurodac Coordinated Supervision Group which stated that *"As the purpose of Eurodac is not to add the criterion 'having readable fingerprints' to the list of criteria for being granted asylum, but to detect and prevent multiple applications, the fact that a person has illegible fingerprints should not be used against him/her. In fact, this would be discriminating behaviour"*³⁹.

55. Under EU data protection law, consent is not the only legal basis for the processing of personal data: a legal obligation can be a basis for a processing of data⁴⁰. However, using coercion measures to obtain fingerprints can raise concerns in terms of human dignity. Indeed, forcing someone to give his/her fingerprints is an interference with the right to privacy, since it has a direct impact on the integrity of the body. For these reasons, **the EDPS recommends deleting the possibility to establish sanctions and penalties, including detention, in the context of the collection of biometrics, and to allow detention only when it is strictly limited to what is necessary for the identification of an individual.**

56. Moreover, recital 30 states that *"Third-country nationals who are deemed to be vulnerable persons and minors should not be coerced into giving their fingerprints or facial image, except in duly justified circumstances that are permitted under national law"*. This wording seems to imply that other individuals could be coerced into doing so. Such coercion should not take place in any case. Therefore, **the EDPS recommends clarifying in a recital that in any event coercion cannot be used in order to obtain fingerprints of individuals.**

d) Operational management

57. Article 5.2 proposes to grant eu-LISA the capacity to use real personal data from Eurodac for testing purposes. The use of personal data for testing purposes does not exempt from the full respect of the data protection regime. Notably:

- Article 5 of the Proposal states that Eu-LISA shall be permitted to use the information in Eurodac for testing purposes, *"(a) for diagnostics and repair when faults are*

discovered with the Central System; and (b) for testing new technologies and techniques relevant to enhance the performance of the Central System or transmission of data to it". The same Article also provides that "real personal data adopted for testing shall be rendered anonymous in such a way that the data subject is no longer identifiable". However, Eurodac is mainly a database composed of identifying information: biometrics and biographic information. Fingerprints and facial images identify an individual per se; they are to be considered as personal data. Therefore, it is not possible to make the data anonymous since fingerprints and facial images will still make possible the identification of the individual⁴¹. For this reason, **the EDPS recommends reconsidering the wording of this paragraph to make it consistent with the comments here above**, if the recommendation made in the next paragraph to delete the possibility to use real data for testing purposes is not followed.

- Moreover, despite of the justification given in the Explanatory Memorandum⁴², the EDPS does not see why the use of real data is necessary for testing purposes. In addition, the Proposal rightly points to the need to secure personal data regardless of the use: whatever 'real' or 'testing'. This will impose on eu-LISA the need to have two 'production' environments equivalent from the point of security. No cost/benefit analysis was conducted to confirm that the expected benefit of using real personal data for testing compensates the increased cost. Given the risks of using real data for testing purposes and the absence of added value of the use of such data, **the EDPS recommends deleting Article 5(2) of the recast proposal allowing using real data for testing purposes.**
- The Proposal is appropriately strict on who may have access to Eurodac data and how these data can be accessed. However, once personal data may be used for testing purposes there is no additional safeguard on who can access those data and how and when such data may be used (*e.g.*: what kind of safeguards should eu-LISA implement when employing external contractors for performing those tests?). If real production data are used for testing purposes, it should be clearly specified who can access that personal data, and when and how these data may be accessed. **The EDPS therefore recommends specifying that appropriate safeguards regarding the access to the data by external contractors could be put in place**, for example with a reference to Articles 24 and 28 of the General Data Protection Regulation.

d) Access

58. Article 7 of the Eurodac recast Proposal places the responsibility of verifying that the conditions of access to Eurodac data by national law enforcement authorities are fulfilled on designated single national authorities or units of such an authority. However, national authorities requesting access to Eurodac data and verifying authorities granting such access can be part of the very same authorities. Indeed, Article 7 states that "*The designated authority and the verifying authority may be part of the same organisation if permitted under national law, but the verifying authority shall act independently when performing its tasks under this Regulation*" and that "*The verifying authority shall be separate from the designated authorities and shall not receive instructions from them as regards the outcome of the verification*". Under these circumstances, the verifying authority cannot be independent from the designated authority, since they are part of the same organisation. Therefore, **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 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 Eurodac data shall be subject to the scrutiny of a body that is sufficiently independent from the designated authority.⁴³

III.2. The EUAA Proposal

59. The aim of the **EUAA Proposal** is strengthening the role of EASO and developing it into an agency (European Union Asylum Agency - EUAA) which facilitates the implementation and improves the functioning of the CEAS.

a) Relations between the experts of the Agency and the Member States' authorities

60. Pursuant to Article 17 of the EUAA Proposal, the Agency will be able to deploy asylum support teams to Member States that request operational and technical assistance from the Agency. These teams will consist of experts from the Agency's staff, from the Member States and/or of experts seconded by Member States to the Agency. However, the Proposal does not clarify on whose behalf and under whose authority these experts will carry out their tasks and process personal data, and thus who will hold controllership and will be accountable for the data processing activities. One may infer that the relevant host Member State authorities will be the controllers for processing of personal data. **The EDPS recommends specifying in the text of the Proposal that the final responsibility of the processing of personal data will be with the Member States which will be considered as “controllers” in accordance with EU data protection law.**

b) Access of databases by the Agency

61. According to Article 19(3), the host Member State to which an asylum support team is deployed will not only have the obligation to give access to the experts participating in the team to European databases, but also the possibility to authorise them to consult national databases, in order to achieve the objectives and perform the tasks outlined in the operational plan. The national and European databases that these experts will be authorised to consult should be included in the operational plan (Article 19(2)(e)), which will be binding on the Agency, the host and participating Member States. **The EDPS recommends further specifying that experts should only be allowed to access databases in compliance with the legal acts governing these databases and data protection law.**

c) The processing of data by the Agency

62. The EDPS welcomes that Article 31 (1) of the Proposal exhaustively lists the purposes for which the future Agency will process personal data in line with the purpose limitation principle, as well as requires such processing to respect the principle of proportionality and be strictly limited to personal data necessary to achieve those purposes (Article 31 (2))⁴⁴. In addition, Article 30 states that the Agency may process personal data for “administrative purposes”, without giving more explanation about this term. **The EDPS recommends further specifying what is meant by administrative purposes.** The EDPS also reminds that according to Article

5 (b) of Regulation 45/2001⁴⁵, applicable to EU institutions and bodies, a processing of personal data is possible when it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed. Therefore, the Agency is authorised to process the necessary information in this context without requiring a specific provision in the regulation.

63. The EDPS also welcomes the fact that Article 31(3), on the one hand, explicitly limits transfers of personal data from Member States and other EU agencies to the Agency for other purposes than the ones defined in Article 31(1), and on the other hand, forbids the further processing by the Agency of retained personal data for different purposes than those of Article 31(1). This is a clear reference to the purpose limitation principle⁴⁶.

64. The EDPS welcomes that Article 32(1) exhaustively lists the categories of personal data collected or transmitted to the Agency in the context of providing operational and technical assistance to Member States and that Article 32(2) further specifies the cases in which these data could be processed.

65. The EDPS also welcomes that Article 32(3) imposes on the Agency the strict deletion of personal data *"as soon as they have been transmitted to the European Agency for the Management of Operational Cooperation at the External Borders of the Member States or used for information analysis on the situation of asylum"* and sets in any event a maximum data retention period of three months. In this regard, Recital 40 further explains that *"A longer storage period is not necessary for the purposes for which the Agency processes personal data within the framework of this Regulation"*. This is in compliance with the data protection principles according to which, personal data shall not be kept longer than is necessary for the purpose for which they were collected.

d) The information system to be developed by the Agency and technical means to be used by the Agency

66. Pursuant to Article 29 (2), the proposed Agency will develop and operate an information system capable of exchanging classified information as well as personal data referred to in Articles 31 and 32. **The EDPS recalls that such a system should be designed in compliance with the principle of data protection by design and that appropriate technical and organisational measures must be implemented in order to maintain the security of the system and prevent unauthorised data processing⁴⁷.**

67. Article 23 of the Proposal aims at enabling the Agency to acquire or lease technical equipment (possibly fingerprinting equipment) that the Agency may deploy to Member States to the extent needed to serve the asylum support teams and to complement equipment already made available by Member States or other EU agencies. The EDPS has concerns as regards the security of the technical equipment and, by extension, of the personal data processed through the use of this equipment. As technical equipment changes hands between the Agency and Member States and between members of the teams, it is important to ensure a level of security appropriate to the risks involved throughout the duration of the operations. **Thus, the EDPS recommends clarifying the responsibilities for ensuring the security of the equipment used which should be defined at all steps of the lifecycle of the equipment, namely from its acquisition, throughout its storage and use, and ending with its disposal.**

IV. CONCLUSION

68. The EDPS welcome the efforts in terms of data protection in the different texts. He can see that the culture of data protection is becoming part of the legislative process and can also be observed in the drafting of the proposals.

69. In full respect for the role of the legislator in assessing the necessity and the proportionality of the proposed measures, the EDPS, in his advisory role, provides in this Opinion some recommendations in terms of data protection and privacy with regard to the three proposals examined.

70. Regarding the Dublin Proposal, the EDPS expresses concerns about the fact that the unique identifier might be used for other purposes, for example for identifying the individuals in other databases, making the comparison of databases easy and simple. The EDPS recommends specifying that any other use of the identifier should be prohibited.

71. Regarding the Eurodac recast Proposal, the EDPS considers that extension of the scope of Eurodac raises concern regarding the respect of the purpose limitation principle as enshrined in Article 7 of the Charter of Fundamental Rights of the EU. The EDPS also recommends further specifying the types of measures other than removal and repatriation that could be taken by the Member States on the basis of the Eurodac data. The EDPS recommends that the Commission make available a full data protection and privacy impact assessment of the Eurodac recast 2016 in order to measure the privacy impact of the text proposed.

72. The EDPS is also concerned about the inclusion of facial images: the Regulation does not refer to any assessment of the need to collect and use the facial images of the categories of persons addressed in the Eurodac recast Proposal. Moreover, the EDPS considers that Proposal should clarify the cases in which a comparison of fingerprints and/or facial images shall take place, since the drafting of the recast Proposal seems to imply that such a comparison should take place systematically.

73. The EDPS also recommends that a detailed assessment is made available with regard to the situation of minors, the balance between the risks and harms of such procedure for the minors and the advantages they can benefit from, in addition to the Explanatory Memorandum. In this context, the regulation should further define (*i.e.* in a recital) the meaning of taking the fingerprints of minors in a child-friendly manner.

74. Concerning the retention period, which will be in principle of five years, the EDPS recommends giving more details and explanation why and how a data retention period of five years was considered as necessary in this context to achieve the new purposes of the Eurodac database. Moreover, the EDPS recommends reducing the retention period to the actual length of the entry ban upon a specific individual. Finally, the EDPS recommends specifying in the Proposal that the starting point of the retention period will be the date of the first fingerprinting processed by a Member State.

75. Finally, the EDPS recommends blocking of all data for law enforcement purposes after three years, and stop making a difference between different categories of non-EU individuals with this respect.

76. In addition of the main shortcomings identified above, the recommendations of the EDPS in the present Opinion concern the following aspects:

- regarding the Eurodac recast proposal,

- The EDPS recommends specifying in the text of the Proposal that the final responsibility of the processing of personal data will be with the Member States which will be considered as controllers within the meaning of the Directive 95/46/EC.
- Article 37 should be redrafted to clarify in which case an international transfer is allowed or prohibited, and specifically concerning the transfer to the applicant's country of origin.
- Article 38 (1) should specify that only the data strictly necessary for the purpose of return can be transferred by the Member States.
- Coercion should not be allowed to obtain fingerprints of individuals. This should be specified in the Eurodac Regulation.
- In this context, the EDPS recommends clarifying that detention should not be considered as a sanction for non-compliance with the obligation to provide fingerprints.
- The use of real data by eu-LISA for testing purposes raises a serious concern and should not be allowed by the Eurodac Regulation. The alternative of using non real data should be considered and assessed by the legislator, considering the risk for the privacy of the concerned individuals. In any case, the text should not consider that biometric data can be anonymised, since they will always relate to an individual and therefore be considered as personal data.
- Regarding the processing of information by eu-LISA, the EDPS recommends specifying that appropriate safeguards regarding the access to the data by external contractors must be put in place.
- Finally, the EDPS welcomes the efforts to make sure that access by law enforcement authorities is assessed by an independent body. However, designated authorities and verifying authorities should not be part of the same organisation, in order to preserve the independence of the verifying authority.

- regarding the EUAA Proposal,

- The EDPS recommends specifying that the experts of the Agency should only be allowed to access databases in compliance with the legal acts governing these databases and data protection rules.
- The EDPS recommends further specifying what is meant by administrative purposes in Article 30 (3), since any purpose pursued by an administration could qualify under this term.

- The EDPS recommends clarifying the responsibilities for ensuring the security of the equipment used by the Agency which should be defined at all steps of the lifecycle of the equipment, namely from its acquisition, throughout its storage and use, and ending with its disposal.

Brussels, 21 September 2016

(signed)

Giovanni BUTTARELLI
European Data Protection Supervisor

NOTES

¹ COM (2016) 197 final.

² COM (2016) 270 final.

³ COM (2016) 271 final.

⁴ COM (2016) 272 final.

⁵ See Article 22, 23, 44 and 45 of the Proposal.

⁶ See Article 23 (2) of the Dublin Proposal.

⁷ COM (2016) 205 final.

⁸ This could be done, for example, in a Recital.

⁹ Opinion of the EDPS of 18 February 2009 on the Proposal for a Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...][establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person] (COM(2008)825) of 18 February 2009;

Opinion of the EDPS of 7 October 2009 on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (.../...) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes;

Opinion of the EDPS of 30 September 2010 on the Communication on "Overview of information management in the area of freedom, security and justice";

Opinion of the EDPS of 12 September 2012 on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [.....] (Recast version).

¹⁰ Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions- Communication on migration, 7 July 2011, § 17.

¹¹ Page 8 of the Proposal.

¹² Page 9 of the Proposal.

¹³ In this context, see Article 35 of the General Data Protection Regulation 2016/679; see also Opinion of the EDPS 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, § 15.

¹⁴ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A European Agenda on Migration (COM(2015) 240 final.

¹⁵ Explanatory memorandum, Pages 5 and 13.

¹⁶ One can even doubt about the opportunity to issue such a policy where some documents established by the Commission seems to indicate that the case of damaged fingerprint is quite isolated (see i.e. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/border/588_emn_ahq_eurodac_fingerprinting_en.pdf, and in particular the answer from Belgium; see also Summary of EMN Ad-Hoc Query No. 588, Eurodac Fingerprints, available at <http://statewatch.org/news/2015/mar/eu-com-compulsory-fingerprinting-asylum-applicants-ms-responses-summary.pdf>, and Eurodac Supervision Coordination Group, *Report on the coordinated inspection on unreadable fingerprints*, May 2013, available at https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med_20130705_report_escg_unreadable_fingerprints.pdf).

¹⁷ Fingerprint Recognition for Children, technical report by the Joint Research Centre, 2013, available at <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20%28pdf%29.pdf>.

¹⁸ Page 10 of the Memorandum.

¹⁹ Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in member states for returning illegally staying third-country nationals.

²⁰ 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).

²¹ Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) 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, COM(2016) 194 final.

²² See Article 6 (1)(e) of 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.

²³ According to Article 17 of the Eurodac recast Proposal.

²⁴ According to Article 13 of the Eurodac recast Proposal.

²⁵ See Article 14 of the Eurodac recast Proposal.

²⁶ See Article 19 of the regulation.

²⁷ Part on detailed explanation of the specific provisions in the proposal.

²⁸ See Article 18 of the recast Proposal.

²⁹ The categories addressed by Article 13(2) and 14(3) of the recast Proposal.

³⁰ See Article 19 (2) second paragraph, and the reference to the purposes of Article 1(1)(c).

³¹ See Article 19(4) and the reference to the purposes of Article 1(1)(b).

³² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

³³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

³⁴ Except that the first paragraph refers to the data obtained by a Member States or Europol, and not the information created by them. However, it seems that this paragraph should not be read in a restrictive manner and should receive a broad interpretation, and a broad scope, including all data processed pursuant to the Eurodac Regulation, wherever they are coming from.

³⁵ The same is true regarding Article 38.2.

³⁶ As mentioned in Article 3(3) of the Eurodac Proposal.

³⁷ Commission Staff Working document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints, SWD (2015) 150 final, referred to in the Explanatory Memorandum.

³⁸ Directive 2013/33/EU of the European parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection (recast).

³⁹ Eurodac Supervision Coordination Group, *Report on the coordinated inspection on unreadable fingerprints*, May 2013, available at:

[https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/13-06-](https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/13-06-10_Report_unreadable_fingerprints_EN.pdf)

[10_Report_unreadable_fingerprints_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/13-06-10_Report_unreadable_fingerprints_EN.pdf). The Report of the Coordinated Group also stated that “The procedures should clarify that unreadable fingerprints as such are not to be used against applicants, but that any adverse consequences for applicants need to be justified by sufficient evidence.

⁴⁰ See Article 7 (c) of Directive 95/46.

⁴¹ See EDPS [Opinion](#) of 25 November 2015 on a notification for prior checking for the Operational Management of large-IT systems in the area of freedom, security, and justice (eu-LISA) related to the Eurodac MSI/Optical Scan tests Study, available at

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2015/15-11-25_Eurodac_MSI_Optical_Scan_Test_Study_euLISA_EN.pdf.

⁴² See page 16 of the Explanatory Memorandum: “When it has come to testing the EURODAC Central System, eu-LISA has been restricted to using 'dummy data' for the test environment and to test new technologies, which has failed to yield good test results because of the data used. The proposal allows for the use of real personal data when testing the Central System for diagnostics and repair, as well as the use of new technologies and techniques, subject to stringent conditions and on the basis that the data is anonymised for the testing purposes and cannot be used for individual identification”.

⁴³ For the same reasoning, see §86 of the EDPS Opinion 6/2016 on the Second EU Smart Borders Package.

⁴⁴ According to Article 4(1)(b) of Regulation (EC) 45/2001 and Article 6(1)(b) of Directive 95/46/EC, personal data must be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”.

⁴⁵ Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 december2000 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.

⁴⁶ See above, §16.

⁴⁷ See Article 25 of the General Data Protection Regulation (Regulation 2016/679) and Article 22 of Regulation 45/2001.