Opinion on a notification for prior checking received from the Data Protection Officer of the European Union Agency for the Operational Management of Large-scale IT systems in the area of freedom, security and justice (eu-LISA) related to the "Eurodac MSI/Optical Scan Tests Study"

Brussels, 25 November 2015 **(Case 2015-0082)**

1. Proceedings

On 28 January 2015, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer ("DPO") of the European Union Agency for the Operational Management of Large-scale IT systems in the area of freedom, security and justice ("eu-LISA") a notification for prior checking ("the Notification") under Article 27 of Regulation (EC) No 45/2001 ("the Regulation") regarding the "Eurodac MSI/Optical Scan Tests Study".

The following documents were attached to the notification:

- Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice;
- Eurodac MSI/Optical Scan Test Strategy;
- Eu-LISA note (DPO opinion on the processing operation Eurodac MSI/Optical study), dated 28 January 2015;
- Letter of the Norwegian Data Protection Authority (*Datatilsynet*) "Assessment – Test of MSI-scanning of fingerprints – Eurodac", dated 22 December 2014.

By e-mail of 5 March 2015 the EDPS asked eu-LISA information and clarifications on the data processing operations notified for prior checking.
Eu-LISA's DPO replied by e-mail to the EDPS on 26 May 2015. The following documents were attached to this reply: "Annex 1 – The Alternate Approach 1.0"; "MSI/Optical Scan Test Plan 1.0".
In the light of these documents, the EDPS asked further clarification, in particular on the categories of personal data processed, by e-mail of 5 June 2015.
Eu-LISA replied to this by e-mail of 27 August 2015, also including an updated notification form.
On 3 September 2015 the EDPS sent the draft Opinion to the DPO for comments. The latter replied by e-mail of 19 November 2015 providing the risk assessment applied to the processing operations related to the Eurodac MSI/Optical Scan Test Study; and by e-mail of

20 November, specifying that aforesaid risk assessment has been approved by eu-LISA's Security Officer and that eu-LISA had no comments to be made regarding the draft Opinion.

2. Examination of the matter

2.1 The facts

According to the notification, **the purpose of the data processing** is to assess the performance of new devices for the scanning of fingerprints ("Multi-Spectrum Imaging/MSI scans", hence "MSI scans") in order to determine if such devices should be recommended for general use within the scope of application of the Regulation (EU) No. 603/2013 (hence, the "Recast Regulation")[1].

To do this, eu-LISA will test the MSI scans with real fingerprints provided by the competent national authorities of the Member States of the European Economic Area (EEA).

Eu-LISA, acting on a specific mandate given by the Eurodac Advisory Group[2], will coordinate -with the support of the Eurodac Recast ICD sub-group of the Eurodac Advisory Group- tests related to the usage of the MSI scans for 'fingerprints-taking'.

The aim of the tests is to prove that the use of the MSI scans for taking fingerprints does not lead to a deterioration of "Eurodac's results" (for instance, it does not lead to more false hits, to quality degradation) compared to other fingerprint-taking methods in use by the Member States in the Eurodac context.

In practice, the test's objective is to ascertain whether the MSI scans meet quality standards better than the current fingerprint-taking methods (optical scans). To do so, the same fingerprint will be scanned using both techniques, that is both by means of the optical scans and by means of the MSI scans.

Regarding the typology of fingerprints to be scanned by the MSI scans, eu-LISA indicated in the reply provided to the EDPS on 26 May 2015 that: "the test study covers the use of the MSI scans with all *regular, damaged and regenerated* fingerprints".

The notification indicates, as **data controller**, the "Applications Management and Maintenance Unit" of eu-LISA.

Eu-LISA will perform the tests and provide the test result to the to the Eurodac Advisory Group, who will finally issue its advise on whether to accept or not the use of the MSI scans for 'fingerprints-taking' in the Eurodac context.

The **legal basis** relied upon by eu-LISA for the data processing (the 'testing exercise' briefly described above) is:
- Article 4, paragraph 1, of the Recast Regulation, laying down that: "(...) *The Agency shall ensure, in cooperation with the Member States, that at all times the best available and most secure technology and techniques, subject to a cost-benefit analysis, are used for the Central System*" (that is, the "Eurodac Central System");

[1] Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 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-County national or a stateless person.
[2] The Eurodac Advisory Groups consists of representatives of the Member States, the European Commission and eu-LISA.

- Article 8, paragraph 1, of the Regulation establishing eu-LISA[3], according to which: "*The Agency shall monitor the developments in research relevant for the operational management of SIS II, VIS, Eurodac and other large-scale IT systems*." (emphasis added)

As to **the source of the data**, the notification points out that the data contained in the "Eurodac Production Database" will *not* be used for the test. For the purpose of the test the competent national authorities of the Member States will provide fingerprints of non-EU nationals to a 'dedicated/ad hoc database' ("testing environment"). These fingerprints will not be accompanied by any form of reference allowing the trace-back of the applicant ("*no link is to be kept neither at the Central System side nor at the Member States side between the fingerprints and the identity of the person*"[4]).

According to the notification, the **data subjects** concerned are foreign (non-EU) nationals (also referred to as "Eurodac data subjects").

The **personal data** processed (in an automated way) are, as also specified above:

- fingerprint images of non-EU nationals *provided by the competent authority of the Member States participating in the study*. The notification states that "all the test data is anonymised. Except the fingerprints, no other personal identification data is to be used in this test study". While the dedicated test database will also include other data fields, these other fields will be populated with randomly generated data[5].

Eu-LISA also points out that it requires the competent authorities of the Member States wishing to participate in the test (providing the fingerprints to the eu-LISA dedicated database) to check with the respective competent national data protection authority (DPA) the compliance of their own data processing with the domestic law implementing the Directive 95/46/EC, as well as the need for specific authorization and the conditions and limits of the data processing.

The notification clarifies that the competent national authorities will not only provide the fingerprints to eu-LISA dedicated database, but they will also run tests ("Tests Cases") on the accuracy of the results obtained via the MSI scans. For these tests, the national competent authorities will make use of a special database of fingerprints[6].

The assessment of the compatibility of the transfer of the data by the Norwegian competent authority (Norwegian Directorate of Immigration) to eu-LISA under Norwegian data protection law has been conducted by the DPA of Norway[7].

As specified by eu-LISA in its reply to the EDPS of 26 May 2015, at the moment eu-LISA has "no written agreement/MoU with the participants."

---

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

[4] See the notification for prior checking, at point 6.

[5] As clarified by eu-LISA on 27 August 2015.

[6] "NIST Special Database 14", described under point 9 of the notification.

[7] See letter form the Datatilsynet of 22 December 2015, attached to the notification.
In this regard, see the *Datatilsynet* (the Norwegian DPA) letter of 22 December 2014.
By this letter the Norwegian DPA takes note that the right of access to the eu-LISA dedicated 'central' database - in eu-LISA's view- would not be applicable, and remarks that: "*as access requests directed to the data controller of the central database will be governed by this [Regulation (EC) 45/2001] Regulation, the interpretation of said article [article 20(2)] lies outside of the Data Protection Authority's formal competencies, and therefore we have no objections*."

The **recipients** to whom the data may be disclosed are:
- eu-LISA;
- the competent authorities of the Member States participating in the study.

The **storage** of the data is ensured by electronic storage media in a secure eu-LISA's Data Centre. As to the **conservation**, the data will be kept for the lifetime of the study (2 months period, renewable, if needed, for other 2 months)[8].

Concerning the **rights of the data subjects**, Articles 13-16 of the Regulation are considered *not applicable* by eu-LISA on the grounds of Article 20(2) of the Regulation, in particular due to the fact that the processing is carried out for scientific research and data are not used for taking measures or decisions regarding particular individuals.

As regards the **information** to be provided to the data subjects, Article 11 is also considered by eu-LISA *not applicable* (since the data have not been obtained from the data subject); while Article 12(1) is considered not applicable on the basis of Article 12(2), since the processing's aim would be for scientific research and the provision of such information would involve a disproportionate effort by the controller.

On **security measures** eu-LISA reports (in the notification and in the attached document "Eurodac MSI/Optical Scan Test Strategy") that it has put in place security measures concerning physical access; logical security; staff security. In addition to the security measures referred above, eu-LISA has provided –as attached documents to eu-LISA's DPO's e-mail of 26 May 2015- the "Annex I, the Alternate Approach 1.0" and the "MSI/Optical Scan Test Plan 1.0".

2.2 Legal aspects

2.2.1 Prior checking

This prior checking Opinion relates to the processing of personal data by eu-LISA, carried out for the purpose of checking the accuracy of new fingerprints scanning devices (the MSI scans) as compared to the technology currently in use (as described under Section 2.1 of this Opinion).

Applicability of Regulation (EC) 45/2001 (hereinafter "the Regulation"). The notification concerns the processing of "personal data" within the meaning of the Regulation. It has to be noted that -by their very nature- fingerprints (being biometric data) allow 'by themselves' the identification of the data subject.
The data processing is performed "by a European Union body", eu-LISA, in the exercise of activities which fall within the scope of EU law.
Personal data of individuals which are not directly or indirectly identified, but are identifiable [Article 2(a)], will be processed (fingerprints images). In this regard, recital 8 of the Regulation foresees that to determine whether a person is identifiable, account should be taken of all the means likely to be reasonably used either by the controller or by any other person to identify the said person.
The processing therefore falls within the scope of the Regulation.

[8] As specified by eu-LISA DPO's by e-mail of 26 May 2015 "2 months (extendable with another 2 months in case of issues)".

Prior checking. Article 27(1) of the Regulation subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes"*. Eu-LISA considers that the fact that biometric data are the object of the processing operations presents specific risks to the rights and freedoms of the data subjects. These views are mainly based on the nature of biometric data which is highly sensitive, due to some inherent characteristics of this type of data. For example, biometric data changes irrevocably the relation between body and identity, in that they make the characteristics of the human body 'machine-readable' and subject to further use. These risks - in eu-LISA's view - justify the need for prior checking by EDPS of the data processing in question.

Considering the self-assessment made by eu-LISA's DPO and the reasons put forward in this respect, and in line with previous decisions issued by the EDPS whereby the processing activities notified to the EDPS involved the use of biometric data (fingerprints)[9], the EDPS considers that the present case is subject to prior checking.

Ultimately, we take note that the entire test entails:
- data processing at national level (collection, storage and transfer of fingerprints from the competent national authority to the dedicated database maintained by eu-LISA), which falls under the scope of the Member State law implementing Directive 95/46/EC;
- the collection and storage of fingerprints by eu-LISA, to which the Regulation applies.
In this Opinion we will limit our analysis to the facts and legal aspects which are relevant for the application of the Regulation.

2.2.2 Lawfulness of the processing

Personal data may only be processed if legal ground can be found in Article 5 of the Regulation.

As far as the **legal basis** is concerned, the DPO of eu-LISA informed the EDPS of the following EU legislation applicable to eu-LISA and relevant as legal basis for the data processing: Article 4, paragraph 1, of the Recast Regulation; Article 8, paragraph 1, of the Regulation establishing eu-LISA. The testing exercise is considered by eu-LISA as necessary for the fulfilment of the aforesaid task (as falling within the Agency's mandate) carried out in the public interest on the basis of the Treaties establishing the European Union or of the legislation established thereof [pursuant to Article 5, letter a), of the Regulation]. Eu-LISA affirms that the purpose of the data processing (to realise a test with a view to check the reliability of the MSI scans) responds to eu-LISA's mandate/attributions. In this regard, the notification states that the test "*plays a pivotal role for the technical implementation of the Eurodac Recast project in order to provide more accuracy when comparing fingerprints with the new scanning devices and current technologies*".
In the light of the above, the test can therefore be considered as falling within the scope of the 'Eurodac objectives' to be pursued by eu-LISA as institutional task.

On the **necessity** of the processing for the aforesaid purpose, eu-LISA specified in its reply of 26 May 2015 to the EDPS questions that -technically- it could not rely on the fingerprints already taken by means of the MSI scans and stored by certain Member States in the Eurodac Production System since "*there are only some isolated cases of MSI fingerprints in the*

[9] See, among others, case 2011-0209, Opinion on a notification for prior checking received from the Data Protection Officer of the European Commission related to the "fingerprints recognition study of children below the age of 12 years"; and case 2014-0496; see also case 2007-0501 (Iris scan system at the European central Bank) and case 2007-0635 (access control at OLAF).

database" ("less than 0,001%"); moreover, such fingerprints "*are not clearly indicated by the Member State and they were treated as they are Optical fingerprints*". Thus a study/test based on the MSI taken fingerprints already stored by certain Member States "may be inconclusive/impossible".

The EDPS therefore concludes that the data processing notified can be considered as necessary for the performance by eu-LISA of a task carried out in the public interest on the basis of the Treaties establishing the European Union or other legal instruments adopted on the basis thereof pursuant to Article 5(a) of the Regulation.

2.2.3 Data quality

Adequacy, relevance and proportionality. Pursuant to Article 4(1)(c) of the Regulation, personal data must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed.

In analysing whether the processing at point, which involves the processing of biometric data, is in line with this principle, the EDPS notes the following.

The type of data processed (fingerprint images) corresponds to the data required to carry out a thorough and integrated in-depth assessment of the technical feasibility of the adoption of the new fingerprints scanning devices (the MSI scans). From this point of view, the data collected could be considered adequate and relevant for the purposes of the processing.

The EDPS also takes note of the justification given by eu-LISA for the fact that MSI scans will be tested with reference to both 'normal' and 'hard to read' fingerprints: in its reply to the EDPS of 5 June 2015, eu-LISA also specified that the test covers the use of the MSI scans with *all* fingerprints (that is, it would check the reliability of the new technology with reference to regular, damaged and regenerated fingerprints). The technical reason given in this respect by eu-LISA is that a test limited to damaged and regenerated fingerprints would be "extremely expensive and useless", also in view of the fact that "due to slow human body recovery, the collection of such fingerprints [would] last tens of years".

Concerning the data referred to in the document "Eurodac MSI/Optical Scan Test Plan", Section 3.3. "Other Data Fields" (where reference is made to the processing by eu-LISA of a "selection of other data fields", including: "Date and Time of the Fingerprint"; "Gender"; "Place [and date] of the application/apprehension"; "Priority"; "Date of granting international protection" and to "additional descriptive data"), we note that eu-LISA, making reference to Section 2.2 of the same document, clarified that these fields will be populated with randomly generated data.

Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analyzed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to the data subjects and it is therefore further addressed in Section 2.2.7.

Accuracy. According to Article 4(1)(d) of the Regulation, personal data must be *"accurate and, where necessary, kept up to date",* and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified"*.

In this case, the personal data at stake are the biometric data provided by the competent national authorities of the Member States (for example, for Norway, by the Norwegian Directorate of Immigration). The accuracy of the data which are provided is assessed by the competent Data Protection Authority allowing the transfer to eu-LISA.
In this regard, we take note, as a safeguard also as far as it concerns accuracy, that the notification specifies that -unless the national competent authority is authorised by its national DPA- eu-LISA does not accept its participation in the study (and, therefore, it does not collect the data/the fingerprints from such national authority).

2.2.4 Conservation of data

Pursuant to Article 4(1)(e) of the Regulation personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed. According to the notification, the data will be stored by eu-LISA "for the lifetime of the study" (envisaged duration of 2 months, plus a possible extension for two more months). The EDPS has no reason to believe that such data retention period -reflecting (according to eu-LISA) the timing necessary for the carrying out the test- is in breach of the Regulation.

2.2.5 Transfers of data

The EDPS notes that the processing does not foresee transfers of data to third Countries or international organisations.

2.2.6 Right of access and rectification

According to Article 13 of the Regulation, the data subject shall "*have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source*".
Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data.
However, this right may be limited if Article 20 applies.
On the basis of Article 20(2) of the Regulation, Articles 13 to 16 shall "*not apply when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics, provided that there is clearly no risk of breaching the privacy of the data subject and that the controller provides adequate legal safeguards, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals*" (emphasis added).
In the case at stake, the EDPS notes that the conditions for the application of Article 20(2) are met, since the purpose of the 'test' is to provide statistics [the EDPS, in this regard, remarks that the purpose of the test is *not* scientific research since the test aims at verifying the reliability of a technology (the MSI scans) which is already available and in use] and the other conditions foreseen in the aforesaid provision are also fulfilled (in particular, the data are not used for taking measures or decisions affecting individuals).

2.2.7 Information to the data subject

Pursuant to Articles 11 and 12 of the Regulation, EU institutions or bodies are required to inform individuals that their data are being collected and processed. Individuals are further

entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

With reference to the processing operations notified for prior checking, the data are not collected directly from the data subjects. Therefore, Article 11 is not applicable in this case. Article 12 (which relates to information to be supplied where the data have not been obtained from the data subject) is instead applicable.
Article 12(2) of the Regulation, containing an exception to the obligation foreseen under Article 12(1) in case the provision of information to the data subjects would involve a disproportionate effort, **can be relied upon** by eu-LISA. Anyway, the EDPS considers that **eu-LISA should provide the data subjects information on the processing operations (the test)** through a privacy statement to be published on eu-LISA institutional web-site.

2.2.8 Security measures

[...]

3. Conclusion

The proposed processing operation would not appear to involve any breach of the provisions of the Regulation, provided that account is taken of the observations made above.

In particular, eu-LISA should:
• **provide adequate information on the processing operations (the test)**: this could be done in a simplified manner, for example through a privacy statement to be published on eu-LISA institutional web-site;
[...]

Done at Brussels, 25 November 2015

(signed)

Wojciech Rafał WIEWIÓROWSKI
Assistant European Data Protection Supervisor