EUROPEAN DATA PROTECTION SUPERVISOR

SECOND EDPS SUPERVISORY OPINION ON EU-LISA'S SHARED BIOMETRIC MATCHING SERVICE ('sBMS') DPIA

(Case 2021-0757)

1. INTRODUCTION

This Supervisory Opinion relates to the follow-up information provided by eu-LISA to the EDPS on the use of biometric matching technologies in the Shared Biometric Matching Service ('sBMS') and the Entry Exit System ('EES'). It follows a previous Opinion of the EDPS under the Prior Consultation procedure under Article 40(1) of Regulation (EU) 2018/1725 ('the Regulation') [1], issued on 4 November 2021.

The EDPS issues this Supervisory Opinion in accordance with Article 57(1)(g) and Article 58(3)(c) of the Regulation.

2. PROCEEDINGS

On 28 July 2021, the EDPS received a request from eu-LISA on the high risk stemming from the use of biometric matching technologies in the EES and the sBMS and related measures to mitigate it. The EDPS issued an opinion on 4 November 2021, recommending improvements in the sBMS and EES Data Protection Impact Assessments ('DPIA's), as well as a series of additional measures for the accuracy measurement process, to be performed prior to entry in to operation. These included considering the risks stemming from bias (e.g. age, gender and ethnic origin), performance degradation and un-synchronicity between the

[1] Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, L 295, 21.11.2018, pp. 39-98.

different systems, as well as demonstrating the necessity and proportionality for the use of real facial images and the minimum necessary amount of such data, for the accuracy measurements.

As a follow-up to the EPDS Opinion, eu-LISA has provided on 04 February 2022 updated versions of the relative DPIAs:

- Annex_I_sBMS Data Protection Impact Assessment_v1
- Annex_II_sBMS Data Protection Impact Assessment for Accuracy Measurement Preparation_v1
- Annex_III_EES Data Protection Impact Assessment_v1.

On 03 June 2022 a staff-level meeting between eu-LISA and EDPS took place for clarifications on the provided updated documents and as a result, the EDPS received on 22 June 2022 the document "Response to EDPS – June 2022: sBMS Data Protection Impact Assessment for Accuracy Measurement" (eu-LISA Answer to EDPSv01 00 00).

The EDPS analysed the above provided documents, in order to verify that recommendations were implemented so as to authorise eu-LISA to proceed with the foreseen accuracy measurement procedure.

3. ASSESSMENT OF THE UPDATED DPIAs

3.1. Recommendation 01

Description

The EDPS recommends eu - LISA to review the list of risks, distinguish the risks explicitly related to the sBMS and ensure that risks related to its use are included in the DPIAs of the systems/processes using sBMS[2]

[2] As explained in section 4.1.1 of the EDPS Opinion of 4/11/2021, some of the identified risks for sBMS stem from the use of the system by other systems (e.g. the EES), and any mitigation measures, e.g. human intervention should be place in the risks assessment of these systems.

As regards the changes to the sBMS DPIA

Implementation actions

Eu-LISA adjusted both the DPIA of the sBMS and the EES DPIA. For the sBMS DPIA, the primary action was to expand subsection 9.3 'Specific risks inferred from EES and VIS', which previously contained risks 95-100 (as an example, risk 95 in the previous version of the DPIA discussed the possibility that EES/VIS access may be abused by the national authorities to obtain biometric matching for illegitimate purposes).

EuLISA has enhanced section 9.3 of the sBMS DPIA (specific risks inferred from EES and VIS). The new section 9.3 of the sBMS contains risks 90-99, with the additional new risks being:

- "failure to maintain auditable usage logs",
- "data processing operation decreases the likelihood that people exercise their fundamental rights",
- "processing personal data when it is not necessary for the purpose prescribed by the Regulation or for unspecified purposes or for purposes which are incompatible with those originally declared" and
- "due to the lack of actual EES data, an erroneous accuracy measurement may be undertaken" .

Implementation status

The EDPS takes note of the introduced changes and provides specific comments for the introduced risks.

For the risk identified regarding the exercise of data subject rights (risk 97), this risk is generally not very clearly defined (the current description of the risk 'Impact on fundamental rights' is not descriptive), which means that the EDPS cannot draw any conclusions on where it should have been integrated (either in the general risks section or in the 9.3 inferred risks section). Respectively, in section 10.3 (mitigation measures), there is no further description of the risk, however a set of dedicated mitigating measures is listed (dedicated awareness training for staff regarding how to deal with data subject rights being among them). The responsible entity for the implementation of the mitigating measures is marked as the Member States). As risk 97 matches Risk 13 of the EES DPIA, please refer to the EDPS' Recommendations on R13 and 19 in the below part for the EES DPIA.

For the risk failure to create auditable logs (Risk 96), understood by the EDPS as referring to both internal and external audits, the auditable usage logs is attributed to the EES and the VIS since these logs are generated in those systems rather than the sBMS itself. Similarly, the purposes for the biometric matching are defined in the respective legal frameworks of the access points (VIS and EES) rather than sBMS. However, general requirements for the logs of the sBMS service are mentioned as a mitigation, with no direct mention on the logs kept in EES.

The EDPS thus recommends eu-LISA revisit the above risks and provide clarifications/modifications as to the above comments.

Furthermore, the EDPS reminds that the chapter on risks from/to other systems should be revised every time a new system is connected to sBMS.

As regards the changes to the EES DPIA

Implementation actions

Following EDPS recommendations , euLISA enhanced Section 9.4. (risk assessment) of the EES DPIA taking into account risks inherited to sBMS. The EDPS notes that the risks and treatment table is similar in terms of layout (but not identical) to the one in sBMS.

The EDPS notes that Risk 97 of the sBMS DPIA "EES data processing could decrease the likelihood that people exercise their fundamental rights" corresponds to Risk 19 of the EES DPIA, which again can be considered as a very broad risk description. The EDPS notes that within the same risk treatment section of the EES DPIA, there is also Risk 13 (inability to respond to requests for subject access, correction or deletion of data in a timely and satisfying manner (TpH13 Table 16) could result in a very high risk for Third-Country Nationals (TCNs) but also for the involved authorities with consequences like reputation, economic and social harm). There seems to be an overlap between Risks 13 and 19 within the EES DPIA, and potentially R13 provides a clearer wording of what is meant i
n R19.

The risks related to purpose limitation (risk 90 and 98 of the sBMS DPIA) are addressed in R1 and R2 of the EES DPIA.

The EDPS however could not trace a clear reference to the risk regarding failure to maintain auditable usage logs.

Implementation status

The EDPS recommends to revisit the risk of "not maintaining audit logs" as well as the risk of "low-accuracy due to no pre-existing data set for EES" to ensure they have been properly included into the EES DPIA as well.

In addition, the EDPS recommends to revisit Risks 13 and 19 touching on the exercise of data subject rights and further explain their difference. Alternatively, eu-LISA may consider merging both risks, by expanding on Risk 13 and introducing the non-overlapping mitigating measures from Risk 19.

3.2. Recommendation 02

Description

Eu-LISA identifies a risk of using personal data for unspecified purposes of for purposes which are incompatible with those originally declared.

The EDPS expects eu-LISA to provide access only to necessary services to each controller, in alignment with the legal framework allowing for such access and to simultaneously log and audit the use of sBMS by other systems.

As regards the changes to the sBMS DPIA

Implementation Actions

As regards the sBMS DPIA, eu-LISA rephrased the risks regarding secondary uses of sBMS data (initially risk 52 and 57) into "Processing personal data when it is not necessary for the purpose prescribed by the Regulation or for unspecified purposes or for purposes which are incompatible with those originally declared". Eu-LISA has also moved this risk to section 9.3 "Specific risks inferred from EES and VIS" (Risk 98) and revised mitigation measures, resulting in the reduction of the residual risk.

Implementation status

The EDPS welcomes the editorial changes to the title and location of this risk, however notes that under risk 98 in section 10.3, **there is no direct mention of the EPDS recommendation of ensuring that only the necessary services have access to the system**. The EDPS notes that there is a similar measure in the proposed mitigation measures for risk 90 (Ensure the Access right matrix is kept up to date and allow only authorised EU information system) and proposes to add it to the mitigation measures.

As regards the changes to the EES DPIA

Implementation actions

Under R16 of section 9.4 of the updated EES DPIA, a risk is mentioned which is similar to the risk of incompatible further processing described in risk 98 of the sBMS DPIA. For the EES DPIA, this risk of incompatible processing is alternatively described as "the EES CS, by using the sBMS, could allow the data collection for secondary purpose that is incompatible with the original purpose (TpH16 Table 16)".

The mitigating measures for this risk include training activities by the involved authorities to the staff who will perform the data processing and the provision of proper information to TCNs on the data processing purpose, purpose limitation and exercise of the data subject rights. In addition, the access to data and all the data processing operations shall be recorded and audit activities should be put in place to check the data processing operations. Eu-LISA also, describes as a mitigation measure the existence of a suitable access control system to prevent the possibility that data could be accessed by unauthorised entities (DPR #013)[3].

Implementation status:

The EDPS considers this recommendation implemented, as both mitigation measures related to purpose limitation and access controls are applied.

3.3. Recommendation 03

Description

The EDPS recommends that:

-Eu-LISA includes, assesses and treats the risk of data subjects not being able to exercise their right to human intervention (Article 24 of the Regulation), and the risk of not having meaningful human intervention, due to automation bias.

-Eu-LISA ensures controllers of other systems/processes using the sBMS are adequately informed of these risks so they can include them in their DPIAs and take adequate mitigation measures, such as relevant user manuals for any steps of human intervention (e.g. second line of border checks). In case the design of sBMS allows, the confidence score of the sBMS match could be displayed to the end users of the other systems, along with the matching result.

[3] The definition of 'end-user' (page 11 of the EES DPIA) already mentions access controls: 'the Access Control for End-Users is role-based and under the responsibility of the Users (see the User).' Users are the administrative authority (i.e. MS or a European body) connected to the EES and/or to the VIS.

- Eu-LISA provides training material to the controllers so that end users learn the capacities and limitations of the sBMS and can critically challenge its outcome.

As regards the changes to the sBMS DPIA

Implementation actions

Eu-LISA has added new baseline controls, primarily reference to the Multi Biometric Search Services (MBSS) personal data protection statement (Annex H) and the Bias results from NIST test (Annex I in section 17.9), which apply for both risks 54 and 57 (risk 59 in the first DPIA version) "Automated decision-making with possible relevant consequences for individuals".

In section 10.1, eu-LISA has expanded the list of mitigation measures to ensure controllers are adequately informed about risks related to automated decisions and possess relevant knowledge and skills on how to provide meaningful human intervention at their end. Extended mitigation measures include measures such as awareness trainings, learning materials to the Member States on the use of new technologies, trainings on the sBMS capacities and limitations with user manuals, provision of trainings regarding interpretation of the matching results to enable Member States to challenge the results if needed.

The design of the sBMS will provide the matching confidence score to the Member States' users and this has been described in the sBMS ICD document. This has also been included in the mitigation section for this risk.

Also, in section 7.3 "Interaction with other processes", the explanatory paragraph regarding matching threshold has been added to demonstrate sBMS' function on receiving feedback on the matching results from the Member States. Due to the application of extended mitigation measures, the risk has been reduced.

Implementation status

EDPS takes note of the updated list of mitigation measures for risks 54 and 57 and considers Eu-LISA has implemented the recommendation. **The EDPS welcomes the fact that eu-LISA has updated the design of the sBMS to its users the confidence score of each match (included in the list of mitigation measures of section 10.1).** Furthermore, the EDPS notes that the annex describing the NIST bias test results on the algorithms is not related to automation bias and thus does not contribute to the mitigation of this risk.

As regards the changes to the EES DPIA

Implementation actions

Eu-LISA has included the risks 17 and 18 related to data subjects' rights right for human intervention and providing meaningful human intervention. As mitigation measures, eu-LISA introduced training material for the controllers (MS), in order to allow the end users to learn the capabilities and the limitations of the results of the sBMS and can critically challenge its outcomes'.

Implementation status

The EDPS notes that although the respective part of the sBMS DPIA was updated to present as a mitigation measure the provision of the confidence score for the match (this would be mentioned in the sBMS Interface Control Document (ICD)), **in the EES DPIA, there is no clear reference to the use of this information as to support meaningful human intervention. It is thus not clear that the user interface will present the user with the confidence score.**

Furthermore, the EDPS asks to include in the sBMS DPIA a clear definition of all involved terms, such as system accuracy and matching confidence score to ensure there is common understanding of the terms among all involved stakeholders.

3.4. Recommendation 04

Description:

The EDPS recommends eu-LISA revisit, clarify and reassess the risks to decrease the likelihood that people exercise their fundamental rights, such as respect for private and family life, protection of personal data and non-discrimination (Risks 38, 53, 58, 63, and 68).

As regards the changes to the SBMS DPIA

Implementation actions

Eu-LISA has moved the risks related to the decrease in the likelihood that people exercise their fundamental rights (Risks 38, 53, 58, 63, and 68) to section 9.3 (related to specific risks from EES and VIS). A new risk "Data processing operation decreases the likelihood that people exercise their fundamental rights (e.g. respect for private and family life, protection of personal data and non-discrimination)" has been added to this section. In addition, several additional mitigation measures have been added, such as providing a dedicated mention to the sBMS processing activities within the information given to the data subjects and provide

awareness trainings and training material to Member States on how to ensure human intervention.

Implementation status

The scope of this risk is still too general and not clear. The EDPS recommends eu-LISA to rephrase this risk as to be more clear and concise (a case example would be helpful for the readers) and re-assess whether it should be kept in the sBMS DPIA or if its inclusion to the EES (and other IT systems using the sBMS in the future) would be sufficient.

As regards the changes to the EES DPIA

Implementation actions

Eu-LISA has added Risk 19 (The EES data processing operation using of personal data and biometric data could decrease the likelihood that people exercise their fundamental rights (e.g. respect for private and family life, protection of personal data and non-discrimination).

Mitigation measures for this risk include providing information to data subjects for the fact that EES processes biometric data, policies to ensure access rights of the data subjects are implemented as well as learning material for end users learn the capacities and limitations of the sBMS and can critically challenge its outcome.

Implementation status

The scope of this risk is still too general and not clear. The EDPS recommends eu-LISA to rephrase this risk as to be more clear and concise (a case example would be helpful for the readers), so that the proposed mitigation measures can be evaluated.

3.5. Recommendation 05

Description

The EDPS asks eu-LISA to clarify and reassess the risk of 'Reliance on low confidence outputs.' (Risk 92)

As regards the changes to the sBMS DPIA

Implementation actions

In the initial version of the sBMS DPIA, the risk was described as “impossible to use the results regarding their reliability level” and was considered as limited (p.180). Eu-LISA has added a relative, rephrased risk (Risk 86) under risks related to machine learning, namely

"Controllers relying on low confidence outputs and making wrong conclusions about individuals" and described as "Making wrong conclusions about individuals based on provided confidence threshold level and not understanding how to interpret it".

Eu-LISA has proposed two mitigation measures, namely amending the sBMS Interface Control Document (ICD) document and the provision of trainings to Member States.

Implementation status

The EDPS welcomes the rephrasing of this risk, which now is understood as the risk of end users to misinterpret the provided confidence score. **While the EDPS agrees with the proposed mitigations measures, it is not clear which the implied relation is between confidence score, the matching threshold and the overall system performance as used in the document (see for instance section 7.3 p.80) and asks for more explanations**. Furthermore, the EDPS **recommends explaining the difference between this risk and risk 24** (related to human intervention).

3.6. Recommendation 06

Description:

In the sBMS DPIA, although eu-LISA proposes several mitigation measures, these measures have no effect in reducing the risk to the data subjects (neither the likelihood or the impact of the risk has been assessed as lower).

The EDPS recommends for such cases thorough re-assessment of the likelihood and impact of the risk and where the residual risk remains the same even after the application of proposed mitigation measures, to explain verbally the effect of such measures.

Implementation actions

In the initial version, the risks for which the effect of the proposed measures on the risk mitigation was not evident were: Risks 56, 61, 66, 71, 76 identified as "Malfunction of the matching system causing false positives or false negatives" (risks 56, 59, 62, 65, 68 in the new version) and Risk 83 about "whitebox inference" (risk 77 in the new version). For the above risks eu-LISA has updated the risk analysis and introduced additional mitigation measures, resulting in reduction of the residual risks.

Risks related to the malfunction of the system (risks 56, 59, 62, 65, 68) have been reduced from maximum to limited after additional mitigation measures including mechanisms to assess quality of fingerprint data prior to processing, mechanisms to receive feedback on the matching algorithms' false outputs and trigger fixing error procedures and trainings to raise

awareness on how to perform meaningful human intervention and interpretation of confidence level scores.

Also, risk on whitebox inference (risk 77) has been reduced from significant to limited after the additional mitigation measures, including network separation, installation of Intrusion Detection Systems and application TLS encryption which contributes towards authenticity of the request originating entity. See also comments on recommendation 08 (further below).

Implementation status

The EDPS notes that it is still not clear whether the initial measures had an impact on reducing the risks, however **considers the recommendation as implemented given that the mitigation measures are implemented**.

3.7. Recommendation 7

Description:

The EDPS recommends that eu-LISA:

-Introduce in all processes / systems using the sBMS mitigation measures to ensure alternative means of identification to challenge any false result (e.g. manual identification by a border guard) and minimise the impact to the data subject and

-Introduce procedures and mechanisms to provide feedback on the matching algorithms' false outputs in order to trigger the procedures of fixing errors in sBMS.

-Implement recommendations on Accuracy measurement Procedure (section 4.4).

As regards the changes to the sBMS DPIA

Implementation actions

The EDPS notes that eu-LISA updated the sBMS DPIA. In the original DPIA, the affected risks were Risk 56, 61, 66, 71 and 76, described as 'Malfunction of the matching system causing false positives or false negatives'. In the updated DPIA the risks are Risk 56, 59, 62, 65 and 68.

As regards the risk of malfunction of the matching system causing false positives or false negatives, a list of mitigation measures have been proposed and a supporting Annex I: Bias results from NIST test (section 17.9) have been added to this DPIA describing the demographic effects in the performance of the sBMS algorithm (i.e. demographic bias) in the NIST's facial recognition vendor test . In addition to the introduced mitigation measures

applied (such as having mechanisms and tools to receive feedback on the matching algorithms, periodical audit of accuracy measurement, provision of awareness trainings etc.), the accompanying paragraph describing the calculation of matching thresholds in sBMS functionality has been added in section 7.3 and explanatory footnotes have been added in section 7.2.2 and 7.2.3.

Implementation status

The EDPS considers this recommendation implemented, as regards the part of Introducing procedures and mechanisms to provide feedback on the matching algorithms' false outputs in order to trigger the procedures of fixing errors in sBMS.

As regards the changes to the EES DPIA

Implementation actions

Eu-LISA has introduced mitigation measures for human intervention and challenge of the sBMS matching results, by updating DRP#004 (to include in policies and procedures alternative means of identification to challenge any false result and minimize the impact to the data subject) and also by introducing two additional measures, namely the provision of training material for the end users of the MS (DRP#022) and a Biometric Accuracy Measurement mechanism to provide feedback on the sBMS output (DRP#023). These measures have been proposed as mitigation measures in several risks, such as risk of absence of meaningful human intervention (Risk 18).

Implementation status

The EDPS considers this recommendation has been addressed as regards the introduction of mitigation measures to ensure alternative means of identification to challenge any false result.

As regards the changes to the accuracy measurement procedure

Please refer to comments on implementation of recommendations 12-15 (further below).

3.8. Recommendation 08

Description

Whitebox Inference of training data from examination of model state (e.g. examination of weights (Risk 83) the EDPS considers that this risk can be reduced to limited, provided that mitigation proposed mitigation measures are successfully implemented.

Implementation actions

In sBMS DPIA, risk 83, related to whitebox inference (inference of training data) was updated (new risk number is 77), and mitigation measures such as Intrusion Detection Systems (IDS) and network segregation were introduced to supplement restriction of access from users/systems to only necessary services.

Implementation status

The EDPS notes that in section 10.2, risk 77 has been reduced to limited as proposed, however **considers this recommendation as implemented**.

3.9. Recommendation 09

Description

The EDPS recommends eu-LISA to include in the sBMS DPIA the risks stemming from potential bias, at the very least gender, ethnic origin and age bias.

Implementation actions

Eu-LISA has added risk 87 related to bias (ethnic origin, age etc) and subsequent discrimination on individuals. As part of the mitigation measures, eu-LISA has listed the MBSS software personal data protection statement, Annex H [AN9], as well as the Bias result from NIST test, Annex I [AN10]. The EDPS acknowledges that eu-LISA presented in section 17.9 (annex I) 16.12 (annex II) a study from IDEMIA showing results of a March 2021 NIST FRVT (facial recognition vendor test) in which its algorithm obtained good scores. While the main focus of this test is overall performance of the algorithm, it also includes an evaluation of accuracy variations across demographic groups.

As regards Race and gender bias: According to the latest NIST verification tests (state of the art), IDEMIA's latest algorithm is among the less affected by gender and race. Resulting in a false matching rate (FMR) of 0.001 for white males, of 0.0012 for black males, of 0.008 for black females and of 0.0004 for white females.

As regards Origin: According to the latest NIST verification tests (state of the art), the FMR by country of birth (including samples from different countries, derived from USA, immigration files of USA, applicants for VISA in USA, etc.) ranges from 0.001 to 0.0001, which can be considered acceptable.

As regards age: In the latest NIST verification tests (state of the art) IDEMIA is identified as one of the few vendors whose algorithms show no FMR differentials for age.

In addition, eu-LISA has provided in section 16.13.12 the method on which the selection of the dataset regarding representativeness on age, gender, nationality of origin etc, while section 5 of the additional information received on 22 June 2022 provide clarifications that measurements e.g. for age and gender will be performed, in addition to the overall measurements explained in section 16.13.1.5.

Implementation status

The EDPS welcomes the report on NIST vendor test results on bias and eu-LISA's plan for subsequent measurements to monitor gender, ethnic origin and age bias, after the algorithm has been configured to ensure compliance with legally required performance thresholds[4].

The EPDS understands that ethnicity bias will be based on nationality or country of origin as neither VIS nor the EES process ethnic origin. Eu-LISA pointed out that the minimum dataset necessary to measure the sBMS' overall performance might not be statistically significant with regards to the demographic bias. Having a statistically significant dataset would entail the processing of a much bigger dataset and eu-LISA cannot estimate what the size of such dataset would be.

The EDPS considers that given the available data, eu-LISA has taken sufficient measures to monitor and mitigate the risk of gender, ethnic origin and age bias.

For completeness of the DPIA documentation, eu-LISA has included in 14.2 (annex I) - review of the DPIA and risk 87 (Wrong or undesired discrimination/bias towards an individual leading to wrong conclusions). Mitigation measures include monitoring the accuracy measurement (overall) of the algorithm. From the received documents, it is unclear if the same bias monitoring and mitigation actions will be part of the future accuracy measurements (after the entry into operation of the system). Since eu-LISA has to monitor and mitigate bias before and after the deployment, **the EDPS expects these measures to be included in the post-deployment accuracy measurement process**.

[4] Commission implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES), OJ, L57, 26.02.2019.

3.10. Recommendation 10

Description

The EDPS recommends eu-LISA to include the risk (of non successful accuracy measurements of the matching engine for facial images, due to the lack of EES data and the fact that quality, angle and lighting from the images to be captured in the EES gates is different than the ones in VISA applications' images) and adopt mitigation measures, such as re-measuring the performance when the sBMS goes live.

Implementation actions

The EDPS acknowledges that eu-LISA has added two new risks (Risk 88 -Low performance of the matching algorithms, due to inadequate data used in accuracy measurements and risk 99 -Due to the lack of actual EES data, an erroneous accuracy measurement may be undertaken) with regard to this recommendation. For risk 88, accuracy measurement and provision of information/trainings to MS so that they can ensure effective human intervention are provisioned.

For risk 99, the EDPS did not find a new entry in chapter 14.2. The description of the newly introduced risk prompts to mitigation measure: Monitor accuracy of operations EES after entry into operation using operational EES data. Also the respective footnote to Risk 99 suggests that once EES is operational, and **after some months**, based on the approval of a DPIA for the activity, another Accuracy Measurement can take place using an extraction of EES data. In addition, monitoring of sBMS accuracy during normal operation has been integrated into the design of the system as required by the Regulation.

Implementation status

The EDPS acknowledges the above changes, however asks eu-LISA to re-measure the performance of the matching algorithms to ensure their accuracy for the first time after the sBMS entry into operation, **as soon as the identified necessary number of samples is reached**[5] **or at the latest within 1 month of the sBMS roll-out date**. The latter (at least monthly measurement of biometric accuracy) is also a legal requirement set out in the respective implementing act[6].

[5] According to eu-LISA's study on how large the test dataset needs to be, provided in section 16.13 (see also Recommendation 15).

[6] Section 1.3 of Commission implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES), OJ, L57, 26.02.2019.

3.11. Recommendation 11

Description

The EDPS recommends eu-LISA to include in the sBMS DPIA the risk of non-synchronicity of the databases, meaning data not being deleted or updated at the same time in the original databases and in the sBMS.

Implementation actions

The EDPS notes that Risks 49, 52, 53, 72 and 73 have been added to section 9. These refer to synchronicity issues with other systems such as the EES, during either storage or deletion of personal data in sBMS. They also include a risk related to wrong application of data retention period in sBMS.

The EDPS acknowledges that apart from security baseline measures, eu-LISA has introduced a regular process to detect inconsistencies between data stored in the central systems such as EES with the ones stored in sBMS. The values identifying the record will be compared and any records for which an inconsistency is found will be marked.

Implementation Status

The EDPS welcomes the introduction of a regular process to identify inconsistencies. However, such inconsistencies might signal a lack of legal basis to process (retain) the biometric templates. In such cases, **the result of the process should be the deletion of the biometric template**.

3.12. Recommendation 12

Description:

Given eu-LISA's necessity to comply with its legal tasks to develop the sBMS including the related legal accuracy requirements, the risks for data subjects and eu-LISA of not doing so and the unsuitability of fingerprint synthetic data for ensuring the matching engine's accuracy, the EDPS considers justified eu-LISA's use of sampled VIS production data with the purpose of ensuring the fingerprint matching engine's legal compliance with respect to the ESS accuracy requirements. However, eu-LISA should report to the EDPS about the relevant details (e.g. dates, number of fingerprints used, retention period) and the outcome of the measurement.

However he notes, contrary to the use of fingerprints, for facial images, eu-LISA has failed to demonstrate the necessity and proportionality of this processing, as alternatives such as the use of synthetic data were not assessed. Given the sensitive nature of biometric data, additional

justification for the use of real facial images should be provided. Therefore the EDPS recommends a study on alternatives of using real facial images in this processing.

As regards the measurements report

Implementation actions

As regards, the plan of accuracy measurement, eu-LISA has shared a plan of the accuracy measurements (Annex II, section 16.13) and additional information on further measurements for bias (section 5 of the information received on 22/06/2022). The planned accuracy measurements consist of 3 categories of measurements respective to different EES use cases:

- Verification against probe: Verification (1:1) simulating use cases where 2 biometric samples are input to sBMS to verify if they belong to the same person (e.g pre-enrolment- the border guards need to check if the person that passed the gate was the same that came to border desk). These measurements are performed with either fingerprints or facial images and measure both false matching and false non-matching rates.

- Verification against reference: Verification (1:1) simulating use cases where a biometric sample is input to sBMS, a template is extracted and is compared to a stored biometric template in sBMS (e.g. use of data for verification at the border when creating/updating the EES file, verification within the territory of the Member States). These measurements are performed with either fingerprints or facial images and measure both false matching and false non-matching rates.

- Search by biometric data: Identification (1:n) simulating use cases where a biometric sample is input to sBMS, a template is extracted and is matched against the different stored biometric templates in sBMS related to EES (e.g. access for designated law enforcement authorities). These measurements are performed with either fingerprints, facial images or multimodal data (combination of facial images and fingerprints) and measure both false positive identification rates and false negative identification rates.

The results will also be presented by age, gender and ethnic origin.

Implementation status

The EDPS notes eu-LISA's plan for the accuracy measurements and **reminds that after the tests, he should receive a report about the relevant details (e.g. dates, number of fingerprints used, and retention period) and the outcome of the measurements.**

As regards the necessity to use real facial images

Implementation actions

Eu-LISA has added a new explanatory note in section 16.13 of annex II. This explanatory note is based on ISO 19795-1:2021, explores the potential use of synthetic facial images and concludes that for realistic performance metrics, the use of real biometric data is still necessary.

Implementation status

The EDPS notes that the additional information provided by eu-LISA on the use of synthetic facial images as an alternative to measuring the matching algorithm's performance, complements the information provided during the prior consultation. As a result, **eu-LISA has demonstrated the necessity and proportionality for the processing of real facial images**.

The EPDS welcomes the fact that eu-LISA commits to continue research in the area of AI use to create synthetic biometric samples, so as to use in future tests (eu-LISA has created a research program to explore the use of synthetic biometric samples (based on StyleGAN tool) to replace real biometric samples).

3.13. Recommendation 13

Description

The EDPS recommends eu-LISA to apply the 4-eyes principle to any step including verification from an MS biometric expert.

Implementation actions

As regards, risks 44 and 59 (Make erroneous - and potentially harmful - inferences or conclusions on specific individuals through the use of artificial intelligence techniques, in particular data mining, facial recognition or biometric analysis of any kind), the EDPS gave their own interpretation of the risk in the former opinion and provided a recommendation to apply the 4-eyes principle to all steps of the accuracy measurement process (annex II) including verifications by an MS biometric expert.

Eu-LISA has implemented this recommendation by amending both the respective process steps' description and the related section in the risk assessment. For instance, steps 4 and 5 in the process description of section 6.3.1.1 mention the submission of the matching results to the **two** biometric experts. In addition, the mitigation measures for other risks were enhanced with the 4-eyes principle, whenever human validation by biometric experts was necessary.

Implementation status

The EDPS notes that the risk description and the respective mitigation measures are not modified in the DPIA documents (e.g. in section 10-measures to mitigate identified risks, in section 13 - review of the DPIA and action plan). For this, **the EDPS is not sure eu-LISA confirms the EDPS understanding of the risk, however he notes that the recommendation to apply the 4-eyes principle to all steps where biometric experts are involved is updated.** As a result, the EDPS considers this recommendation is implemented, and **recommends eu-LISA look into this element and update any risk descriptions accordingly, for future reference**.

3.14. Recommendation 14

Description

Eu-LISA has identified a risk of whitebox inference for individuals that were part of the training dataset, from the MS biometric experts that took part in the accuracy measurement procedure. The EDPS understands that the MS biometric experts will sign a binding agreement addressing their exact activities.

The EDPS recommends to reduce this risk to Negligible, provided that:

- *access is restricted only to necessary services in the accuracy testing dedicated environment, and a confidentiality (non-disclosure) clause is included in the binding agreement of the MS biometric experts.*

Implementation actions

Eu-LISA, following the EDPS recommendation, has reduced the risk of whitebox interference (risks 45 and 60) in sections 9 and 10 of the annex II to negligible. In addition, eu-LISA has confirmed the signature of the declaration of confidentiality and non-conflict of interest agreement by the MS biometric experts that will take part in the accuracy measurement process and provided the respective template (16.14).

Implementation status

The EDPS considers **this recommendation is implemented**.

3.15. Recommendation 15

Description

The EDPS recommends eu-LISA to perform a study on the necessary/optimal size of the random VIS dataset to be used to initiate the process and to introduce it as a requirement in the first step of the process, where representativeness is analyzed.

Also, since measurements related to bias measurement are not described for the accuracy measurement process, the EDPS recommends eu-LISA to include additional separate metrics at least per gender, age and ethnicity as part of the measurement protocols to be defined (by MS and JRC).

The EDPS understands that due to lack of actual EES data, the risk of resulting to erroneous accuracy measurement cannot be further mitigated. The EDPS notes that this risk should be clearly described in order to be taken into account in the sBMS DPIA (as proposed in section 4.3.2).

As regards the optimal size of the selected dataset

Implementation actions

Eu-LISA has provided a study of the necessary/optimal size of the random VIS dataset to be used to initiate the accuracy measurement process (section 16.13.1.4 of the accuracy measurement process DPIA and sections 3 and 4 of the additional information provided on 22/06/2022).

The calculation of the minimum necessary testing data considers two aspects. First, it considers the rule of 30, as described in ISO/IEC 19795-1:2021, according to which one can be 90% confident that the error rate will be ±30% of the observed error rate, if there are at least 30 errors. Second, eu-LISA plans to use a ratio 1 (mated pair):10 (non-mated records) and therefore this ratio dictates the total number of non-mated records (unique biometric data) needed as a minimum for the FMR test cases.

Finally, eu-LISA wants to ensure the performance observed during the accuracy measurement by checking if those results extrapolate when using more data than the minimum necessary testing data. This process will involve the use of the real data extracted from VIS and a database of synthetic data equivalent of 3% of the size of the whole sBMS database (9.5 million facial images and 4.5 million fingerprint sets).

Implementation status

The EDPS considers **this recommendation is implemented.**

As regards the bias measurements

Implementation actions

Eu-LISA provided a study on representativeness of the selected datasets in section 16.13.1.6 (based on age and nationality distribution). In the additional information provided on 22/06/2022 (section 5), eu-LISA has provided confirmation that additional measurements will be done, by age, gender etc.

Implementation status

The EDPS considers **this recommendation is implemented.**

As regards the risk of erroneous accuracy measurements (since EES data will be simulated)

Implementation actions

The EDPS notes that risk 75 "Due to the lack of actual EES data, an erroneous accuracy measurement may be undertaken" is introduced with likelihood 2 and impact 4 (section 9.8 and section 10 .8 of annex II). Since this risks cannot be further mitigated before the entry in to operations of the EES, this risk has been accepted by eu-LISA and mitigation measures, namely a process to monitor the performance once the EES starts operating, have been provisioned.

Implementation status

The EDPS considers this recommendation as implemented and reminds eu-LISA of the comments on recommendation 10, as regards the time to re-measure the accuracy of the algorithms for the first time after the sBMS entry into operation date.

4. CONCLUSION

The EDPS has made several recommendations to ensure compliance of the processing with the Regulation.

Based on the provided information, the EDPS considers recommendations related to the sBMS accuracy Measurement DPIA (recommendations 12-15) are implemented and **eu-LISA may proceed with the described process for accuracy measurements**.

The EDPS reminds that after the completion of the measurements, **a report with relevant details (e.g. dates, number of used fingerprints and facial images, retention period) and the outcome of the measurements should be submitted** (recommendation 12).

As regards recommendations on the sBMS DPIA and related changes in the EES DPIA, the EDPS expects eu-LISA implements these recommendations (Recommendations 01, 04, 05, 11) **and provides documentary evidence prior to the entry into operation**.

Furthermore, as regards the procedure for prior consultations, and in order to simplify the process of providing follow-ups, the EDPS recommends for the future to:

- provide a report of implementation per recommendation referencing all actions taken (specific for each DPIA/system) so that a complete view of the mitigation approach is presented to the EDPS.

- Provide a version of the DPIAs with track changes, for the EDPS to easily identify the amendments related to the recommendations.

- Provide a searchable version of the documents (e.g., the annex related to the IDEMIA report on bias was not searchable).

Done at Brussels on 4 August 2022

po

[e-signed]

Wojciech Rafał WIEWIÓROWSKI