EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS SUPERVISORY OPINION ON A PRIOR CONSULTATION REQUESTED BY THE EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)

on a Face Recognition Solution (Case 2023-1104)

1. PROCEEDINGS

On 16 October 2023, the EDPS received a request for prior consultation from Europol under Article 90 of Regulation (EU) 2018/1725 (the 'EUDPR') as further detailed in Article 39 of Regulation (EU) 2016/794 ('the Europol Regulation' or 'ER' abbreviated), regarding a Face Recognition Solution.

The request for prior consultation sent by Europol contained:

- a Data Protection Assessment form[1], which in turn included:
    - a Threshold Assessment (TA), assessing whether a DPIA had to be carried out,
    - the subsequent Data Protection Impact Assessment (DPIA), and
    - an assessment of whether the EDPS must be prior consulted for this processing operation; as well as
- a cover letter from Europol's data protection officer[2].

Europol attached the following internal supporting documents to the request for prior consultation:

[redacted]

[redacted]

[redacted]

Europol also provided the following external documentation as attachments to the prior consultation:

- NEC NeoFace Watch – Data Protection & NEC algorithm Equitability[12];
- Facial recognition technology in law enforcement (equitability study)[13];
- NIST 2019 Face Recognition Vendor Test Part 3: Demographic Effects[14];
- Report on the Evaluation of 2D Still-Image Face Recognition Algorithms[15];

On 16 November 2023, the EDPS held a staff-level meeting with Europol to further clarify the prior consultation package as regards the input sources to the Face Recognition Solution, its temporary storage locations, access rights management and human review of the output.

According to Article 90(4) of the EUDPR, the EDPS is to issue his Opinion within a period of up to six weeks of receipt of the request for consultation, with a possible extension by one month.

As an extension was **deemed necessary** in this case, the deadline within which the EDPS shall issue his Opinion in this case is **28 December 2023**. The extension of the deadline, together with the justification, was communicated to Europol on 10 November 2023.

[redacted]

[12] Commercial documentation provided by NEC.

[13] T. Mansfield, National Physics Laboratory (NPL) Report MS 43, final report dated March 2023.

[14] Grother, P. , Ngan, M. and Hanaoka, K. (2019), Face Recognition Vendor Test Part 3: Demographic Effects, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8280.

[15] P. Grother, G.W. Quinn and P.J. Phillips. Report on the Evaluation of 2D Still-Image Face Recognition Algorithms (NIST Interagency Report 7709). August 2011. Available at www.nist.gov/manuscript-publication-search.cfm?pub_id=905968 . Released June 3, 2014.

2. DESCRIPTION OF THE PROCESSING

2.1. Overview

In 2016, Europol developed a facial recognition system ('FACE') to combat terrorism, organised crime, and child sexual exploitation. The system aimed to generate leads for identifying unknown criminals and entities falling under Europol's mandate. However, Europol considers that the system has become inadequate due to the evolving needs of Europol's stakeholders, and is unable to handle the rising volume of requests for criminal identification. Europol's internal solution is not seen as capable of expanding to meet the growing demands, which 'includes the future expansion of Europol's operations related to the interoperability of systems in the area of Justice and Home affairs' (however this last element is not further expanded on)[16].

According to Europol, it carried out market research in 2021 and concluded that a commercial solution would better fit these operational needs compared to its existing in-house tool. In the prior consultation package, Europol did not provide details on the way the market research was carried out.[17]

[redacted]

The facial recognition solution provided by NEC is based on a machine learning model, which is trained, tested and integrated in the product by NEC. The facial recognition model on which the NEC product was built was evaluated by the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce[18]. Europol does not carry out any kind of model training of the NFW tool. The solution purchased by Europol does not include the machine learning capabilities itself.

Detection phase

[redacted] [redacted]

[17] During the meeting of 16 November 2023, Europol explained that different candidate tools were scored on factors such as user-friendliness and accuracy, after which these scores were submitted to the NEO steering committee.

[18] NIST carries out periodical Face Recognition Vendor Tests (FRVTs), through which NIST evaluates the performance of face recognition technologies. To the understanding of the EDPS, these tests are conducted on the underlying facial recognition model, meaning that while the specific product that Europol has purchased may not have been tested, this product is based on an iteration of this tested model (either the same model or a more recent version).

[redacted]

[redacted]

[redacted]

[redacted]

If the reviewer decides that the images are suitable for facial recognition processing, the ingestion and cross-checking phase starts.

If the reviewer decides that the images are not suitable for facial recognition processing, the rejected faces are removed from Bioman UI without saving. [redacted]

[redacted] [redacted]

[20] 'Biometrics Manager UI', developed in-house by Europol.

[redacted] [redacted]

[redacted] [redacted]

[redacted]

For videos, the images of each video frame are first processed in a temporary video processing instance to extract faces and identify the highest quality facial image between the different frames[23].The three highest quality images of each data subject are retained and presented to the reviewer. From this point onwards, the same process is followed.

<u>Ingestion and matching phase</u>

[redacted]

According to Europol, Biographical data will not be stored in NFW since details such as name, gender and age, if displayed with images, might influence match adjudication[25].

The newly enrolled images are then compared against the existing stored facial images. These existing stored templates of facial images are stored in the NFW application, with no separation per case or Analysis Project (AP) and although the product offers the functionality to search in other databases[26], this functionality will not be used for the moment in Europol.

[redacted]

A reviewer verifies or excludes each match. This first-line reviewer is an analyst [redacted] who has undergone training in performing face comparisons. They are however not dedicated biometric specialists (and have not been hired as such); they perform these duties together with their normal operational analysis tasks.

If the first-line reviewer concludes that there are positive matches (referred to as likely candidates), a facial recognition expert from the Biometrics team ([redacted], verifies the results (peer-review). These facial recognition experts were (and will be) hired in this capacity by Europol and have a formal biometrics background. Additional contextual information (case information) is technically accessible at either stage by going through the properties of the possible matches.[27] Europol operational emails are used as a channel to notify the team of

[redacted]

[redacted]

[redacted]

[redacted]

[27] This information was provided by Europol during the meeting of 16 November.

biometric experts that a confirmatory review is necessary. For these second-line reviews, the facial recognition experts are not aware of which image the first analyst considered to be a match, and the full list of matches is presented again to the reviewer to analyse.

In case of agreement of the two experts, the results are shared[28] with the respective parties (provider of the image stored and provider of the image that triggered the match). These results are shared as being 'likely candidates' or 'leads' that might assist in the identification of data subjects.

In case of disagreement a third opinion will be sought[29], by assigning the list of matches to a third reviewer (also in the biometrics team). The same procedure is followed in this case as for the second-line review. The final establishment of a match is done via majority decision (2 to 1).

3. LEGAL AND TECHNICAL ASSESSMENT

3.1. Need for prior consultation pursuant to Article 90 of the EUDPR

Article 90 of the Regulation[30] provides that the controller shall consult the EDPS prior to processing which will form part of a new filing system to be created, where:

(a) a data protection impact assessment under Article 89 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

As to whether the Face Recognition Solution will form part of a 'filing system', the EDPS reminds that a filing system is 'any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.'[31] [redacted]

[28] Subject to any sharing restrictions (in particular handling codes) put in place by either party.

[redacted] [redacted]

[30] Chapter IX of the EUDPR is applicable as this concerns the processing of operational personal data by a Union body, office or agency carrying out activities that fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU (Article 2(2) EUDPR).

[31] Article 3(7) of the EUDPR.

[redacted]

As already highlighted in a previous prior consultation Opinion[32], Article 90 EUDPR has a broader scope of application than Article 40 EUDPR. It subjects to prior consultation processing operations for which a DPIA indicates that they would result in a high risk in the absence of mitigation measures (irrespective of whether the controller considers that these risks have been mitigated or cannot be mitigated by reasonable means) (Article 90(1)(a) EUDPR). It also requires prior consultation for types of processing that, by nature, include a high risk to the rights and freedoms of data subjects (Article 90)(1)(b) EUDPR).

The EDPS notes that Europol has submitted the prior consultation on the Face Recognition Solution on the basis of Article 90(1)(b) of the EUDPR, meaning that Europol deems this operation to include, by nature, high risks to the rights and freedoms of data subjects.

As part of its assessment, the EDPS considers the recently released Guidance by the European Data Protection Board (EDPB) on the use of facial recognition by law enforcement[33]. In this guidance, the EDPB confirms that "*pursuant to Article 28 LED, the controller or processor has to consult the supervisory authority prior to processing, where: (a) a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or (b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects. As already explained in point 2.3. of these guidelines, the EDPB considers that most cases of deployment and use of FRT contain intrinsic high risk to the rights and freedoms of data subjects. Therefore, in addition to the DPIA, the authority deploying the FRT should consult the competent supervisory authority, prior to the deployment of the system.*"

Taking into account that Article 28 LED as interpreted by the EDPB contains the national equivalent of Article 90 EUDPR, and that the practical implementation of Europol's proposed facial image processing will impact large sections of Europol's activities (thus not amounting to an exception to the usual intrinsic 'high risk' of these systems), the EDPS deems that the processing indeed requires prior consultation of the EDPS under Article 90(1)(b) EUDPR.

[32] EDPS Opinion of 21 October 2022 on a prior consultation on Europol's biometric queries of SIS II, Case 2022-0904.

[33] See EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0, Adopted on 12 May 2022, available on the website of the EDPB: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

The EDPS deems that the processing is correctly qualified as requiring prior consultation under Article 90(1)(b) of the Europol Regulation.

3.2. Scope of the Opinion

The Opinion of the EDPS on this prior consultation **concerns the implementation of the Face Recognition Solution as described in the notification** of 16 October 2023 and appended documentation.

This Opinion will focus on key aspects that raise issues of compliance with the applicable data protection legal framework or otherwise merit further analysis. The EDPS notes that some of the technical documentation mentions the possibility to query external systems (such as those hosted by eu-LISA) with facial images and provide a first flowchart of how this query would function[34], however the main DPIA does not mention the possibility and related risks. While the possibility to query external systems or to open Europol's database to external queries considerably increases the impact of the processing on data subject's rights and freedoms. As such risks are not addressed by the DPIA submitted for prior consultation, the EDPS considers it to fall out of scope. Therefore, the EDPS has not examined it as part of this prior consultation opinion.

In any case, the EDPS expects to be consulted on any significant update of the DPIA as a result of a substantial modification of the personal data processing operations at stake. This may occur in particular in cases where high risks to the rights and freedoms of data subjects would be created or modified due to significant new tools being added to the Face Recognition Solution, new input sources into the Face Recognition Solution, or other structural changes to how the Face Recognition Solution stores and further processes personal data (including as mentioned due to queries by external systems).

3.3. Lawfulness of the processing

3.3.1. Legal basis for the proposed processing operation

Europol has indicated that it would perform the processing in the Face Recognition Solution as part of the following tasks under Article 4 ER:

> (a) collect, store, process, analyse and exchange information, including criminal intelligence

[redacted] [redacted]

> (b) notify the Member States, via the national units established or designated pursuant to Article 7(2), without delay of any information and connections between criminal offences concerning them;
> (e) provide information and analytical support to Member States in connection with major international events;
> (h) support Member States' cross- border information exchange activities, operations and investigations, as well as joint investigation teams, including by providing operational, technical and financial support;
> (r) support Member States in identifying persons whose criminal activities fall within the forms of crime listed in Annex I and who constitute a high risk for security;

Out of these listed tasks, the EDPS pays particular attention to the ground under point (e) of Article 4(1) ER.

For Article 4(1)(e) ER, which describes the support task of Europol following major international events, this legal basis raises the contentious issue of (retrospective) facial recognition in public places. Indeed, the EDPS recalls that in Europol's 2019-2020 programming document, the topic of support to major international events was mentioned in particular regarding the expert group on the implementation of the UEFA 2020 coordination centre.[35] Depending on the use-case, the use of facial recognition for this task could thus clearly involve the processing of large amounts of non-DSC data[36]. The EDPS warns that a too wide use of this legal basis to store images of events in the watchlist could amount to general surveillance, which must be safeguarded against. One of these clear safeguards that has been introduced by Europol is the explicit prohibition to use non-DSC data as part of the NFW processing. The various proposed safeguards by the EDPS' throughout this document (in particular as regards purpose limitation) should also be read in in light of the risks posed by this legal basis.

3.3.2. Purposes under Article 18 ER for which facial images would be processed

The use of the facial recognition tool will entail a processing of biometric data, which is qualified as special category of personal data under Article 30 ER and subject to stricter requirements, in particular in terms of necessity and proportionality of their processing. Necessity and proportionality should be assessed in light of the purpose of the processing. It

[redacted]

[36] 'Non-DSC data' refers to personal data which has not undergone the data classification process as provided for in the Europol Regulation (the so-called 'data subjects categorisation' or 'DSC'), in order to establish to which data categories and/or data subject categories in Annex II ER the personal data belongs.

follows that compliance with Article 18 ER, which outlines the potential purposes for processing personal data by Europol, must be read together with the specific provisions outlined in Article 30(2) ER. Therefore, any proposed purpose for which Europol intends to use biometric data requires a prior, thorough justification, to ensure that Europol does not process biometric data for purposes for which this processing would not be strictly necessary or proportionate.

Without this careful consideration and justification, there exists a real risk of non-compliance with Article 30(2) of the Europol Regulation.

3.3.2.1. Strict necessity and proportionality requirements under Article 30(2) ER

The recent amendments to the Europol Regulation, particularly Article 30, have clarified the status of biometric data, and specifically facial images, within Europol's processing activities. With the inclusion of 'biometric data *for the purpose of uniquely identifying a natural person*' as a special category of personal data, the EDPS considers that the co-legislators meant specifically to address facial recognition systems. While traditional biometric data such as fingerprints and DNA data are virtually only used for biometric identification and authentication, facial images are commonly processed in a variety of contexts, beyond pure biometric identification systems. Recital 46 of the amended Europol Regulation further explains the inclusion of facial images as a form of biometrics in Article 30, emphasising that the processing of photographs should not automatically be considered as handling special categories of personal data unless processed through specific technical means enabling unique identification.

It is clear however that the proposed development of a facial recognition system by Europol, falls within the scope outlined in the amended Article 30(2) of the Europol Regulation. Consequently, the requirements of strict necessity and proportionality fully apply to the proposed processing of facial images.

Strict necessity

The Court of Justice of the European Union (CJEU) clarified the requirement of strict necessity in case C-205/21, primarily in the context of Article 10 of Directive (EU) 2016/680. This article deals with the processing of special categories of personal data by national competent authorities, including biometric and genetic data. Notably this provision does not discuss 'strict proportionality', which was included in Article 30(2) ER, therefore making Europol's conditions stricter than those that apply at the national level.

As regards strict necessity, the CJEU emphasises that this requirement establishes strengthened conditions for lawful processing of biometric data, requiring a particularly rigorous assessment of its necessity[37]. Through this, the court underlines that the processing of biometric information should be considered necessary only in a limited number of cases and thus cannot form a default part of processing of personal data by an authority[38].

The requirement that the processing of sensitive data be "strictly necessary" is a specific implementation of the principles set out in Articles 4 and 8 of Directive 2016/680. In particular, the Court pointed to the application of the purpose limitation principle (which is defined for Europol through Article 18 ER) and the principle of data minimisation[39].

The CJEU details that the assessment of whether the collection of biometric and genetic data is "strictly necessary" must consider the purpose of the collection, which should be "specified, explicit and legitimate". Additionally, the collection should be adequate, relevant, and limited to what is necessary for the purposes for which they are processed[40].

The EDPS also points to the European Data Protection Board's guidance on facial recognition in the law enforcement context, which also emphasises that processing special categories of data, such as biometric data, can only be deemed "strictly necessary" (Art. 10 of the law enforcement directive) if the interference with the protection of personal data and its limitations are restricted to what is absolutely essential—indispensable—and precludes any processing of a general or systematic nature[41].

Strict proportionality

While the CJEU has not yet expressed itself on the meaning of strict proportionality, which as stated before is not present in the Law Enforcement Directive’s provision on the processing of biometric data, it has frequently expressed itself on proportionality as such. Much of this case law has been summarised by the EDPS in its ‘proportionality toolkit’.[42]

For a measure to respect the principle of proportionality enshrined in Article 52(1) of the Charter, the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of fundamental rights. It

[37] Paras. 115-118.

[38] Para. 118.

[39] Paras. 121-122.

[40] Paras. 122-125.

[41] See para 73 of the EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, available at https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

[42] EDPS, “Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data”, 25 February 2019, available at https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

therefore "restricts the authorities in the exercise of their powers by **requiring a balance to be struck between the means used and the intended aim (or result reached)**".[43]

This concept of a balancing exercise lies at the core of the notion of proportionality and is performed by weighing up of the intensity of the interference vs the importance ('legitimacy', using the wording of the case-law) of the objective achieved in the given context.

As stated by the CJEU, it is essential to point out that proportionality is an assessment in concreto (case by case): "*It is for the referring court to take account, in accordance with the principle of proportionality,* ***of all the circumstances of the case before it****, in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed*"[44]. In other words, the proportionality analysis is always contextual: this analysis cannot take place without first identifying the context of the measure under scrutiny (for instance, does the controller share or provide access to the information on the person concerned? with whom and for what purpose?).

Applying to the conditions laid out by the CJEU as regards necessity *mutatis mutandis* to proportionality, the criterion of **strict** proportionality would require a particularly rigorous assessment. This would involve, for each of the purposes defined by Europol, examining how facial recognition technology would be concretely applied to assess whether both a less intrusive method is available and whether the impact of the interference to the individual does not outweigh the potential benefit of the FRT processing.

3.3.2.2. Assessment of necessity and proportionality requirements for each of the intended purposes of the processing

As to the different purposes that the Face Recognition Solution would serve under Article 18 ER, the notification mentions:

- cross-checking under Article 18(2)(a) ER;
- operational analysis under Article 18(2)(c) ER; and
- temporary processing to determine the relevance of personal data to Europol's tasks, under Article 18(6) ER.

[43] K. Lenaerts, P. Van Nuffel, European Union Law, Sweet and Maxwell, 3rd edition, London, 2011, p. 141 (case C-343/09, Afton Chemical, para. 45; joined cases C-92/09 and C-93/09, Volker und Markus Schecke and Hartmut Eifert, ECLI:EU:C:2010:662, para. 74; cases C-581/10 and C-629/10, Nelson and Others, para. 71; case C-283/11, Sky Österreich, para. 50; and case C-101/12, Schaible, para. 29).

[44] CJEU, case C-101/01, Linqvist, ECLI:EU:C:2003:596, para. 89.

The EDPS notes that Europol only provides a clear description and justification for the use of facial recognition for the purposes of Article 18(2)(c) ER. The need to use this tool for the purposes of cross-checking (Art. 18(2)(a) ER) and for determining whether personal data are relevant to Europol's tasks (Article 18(6) ER) is unclear from the documentation provided.

Processing for the purpose of operational analysis (Article 18(2)(c) ER)

As regards **Article 18(2)(c) ER**, i.e. processing personal data for operational analysis, the EDPS notes that the European co-legislators prescribed a specific framework for this type of processing - namely the matrix of Europol operational Analysis Projects, each with their respective scope of activities and data processing needs, in Article 18(3) ER.

As the basis of the facial recognition for the purpose of Article 18(2)(c) ER will be the facial images processed in these APs, the scope of the APs and the types of data subjects on whom each AP will process facial images will be crucial to determine the impact that processing under article 18(2)(c) ER has on these data subjects.

[redacted]. The EDPS however notes that this version of the AP Portfolio did not yet include any changes as regards this newly introduced special category of personal data[46]. Such changes were however shared with the EDPS for information on 3 November 2023.[47] The EDPS provided comments at staff level on 27 November 2023.

The EDPS would like to reiterate that as facial recognition becomes more and more part of policing, it is essential to establish a clear framework, in particular for the images that can be used as probe images or as part of 'watchlists' for facial recognition applications.

The **EDPS therefore considers it necessary for Europol** to specify the categories of individuals for whom facial recognition will be used in Europol's AP portfolio and provide concise use cases justifying its application. Not doing creates risks of non-compliance with the principle of purpose limitation as laid out in Article 71(1)(b) of the EUDPR and further specified in article 18(2)(c) and (3) ER.

Processing for the purpose of cross-checking (Article 18(2)(a) ER)

[redacted] [redacted]

[46] The submitted version of the AP Portfolio only refers to genetic data as a specific form of biometric data processed within some of the APs.

[47] As was already informally commented on in EDPS case 2023-1194 regarding the amendment of the AP Portfolio.

As regards **Article 18(2)(a) ER**, the EDPS considers that this provision was designed to facilitate direct personal data cross-checking among Member States. Article 18(2)(a) ER allows Member States to access and review a shared pool of personal data without being restricted to a hit-no hit system.[48] To off-set this direct access to personal data, Annex II of the Europol Regulation lays down a much more restrictive list of personal data (and data subject categories) that may be processed for this purpose. At the moment of the adoption of the Europol Regulation, this provision was clearly targeted at the operation of the Europol Information System (EIS).

After reviewing the submitted DPIA and attached documentation, the EDPS has not seen a clear indication that Europol actually intends to use the system in connection with the EIS[49] or in another way wishes plans to use it for the purpose laid out in Article 18(2)(a) ER.

As Europol has insufficiently described how this purpose would be implemented, the EDPS cannot provide a reasoned opinion on whether the intended processing is strictly necessary and proportionate for this purpose as required under Article 30 of the Europol Regulation or would in any other way infringe the Europol Regulation or the EUDPR, in particular whether Europol has insufficiently identified or mitigated any risk, created by the facial recognition solution for the purpose of Article 18(2)(a) ER.

Given the requirements of "strict necessity" and "strict proportionality," the **EDPS considers it necessary,** prior to any processing of facial images for the purpose of Article 18(2)(a) ER, to both describe the proposed implementation and perform an assessment of the necessity and proportionality of this proposed processing. Not doing so would a risk of incompliance with the conditions of strict necessity and proportionality laid out in Article 30(2) ER.

Processing for the purpose of determining whether personal data are relevant for Europol's tasks (Article 18(6) ER)

Finally, as regards **Article 18(6) ER,** the EDPS notes that this provision permits only temporary processing to determine whether personal data are relevant to Europol's tasks. This type of processing implies that the relevance of data at the initial contribution stage is uncertain. The EDPS highlights the importance of strict necessity and proportionality in processing biometric data under Article 30 ER, as outlined in section 3.3.2.1. of this Opinion.

[48] See Article 20(1) ER.

[redacted]

Despite this uncertain relevance of the data, no distinction is made in the DPIA between how this data will be processed by Europol compared to the facial images that will be processed for the purpose of Article 18(2)(c) ER.

In particular, no mention is made of how Europol arrived at the conclusion that the processing for this purpose using FRT can take place under the same conditions (including ingestion into the NFW watchlist) as for Article 18(2)(c) ER, and how this is considered strictly proportionate.

Given the requirements of "strict necessity" and "strict proportionality," the **EDPS considers it necessary,** prior to any processing of facial images for the purpose of Article 18(6) ER, to both describe its proposed implementation and perform an assessment of the necessity and proportionality of this proposed processing. Not doing so would a risk of incompliance with the conditions of strict necessity and proportionality laid out in Article 30(2) ER.

3.4. Assessment of the risks to data subjects and proposed mitigation measures

In its DPIA, Europol outlined five key risk areas for the planned FRT processing. These risks were evaluated using a 5x5 matrix, combining the likelihood and impact of each risk. Consequently, the total risk score could range from 1 (indicating an extremely low likelihood with minimal impact) to 25 (signifying a high probability of occurrence with severe consequences for the data subject). Out of these five areas, the initial (pre-mitigation) risk levels were assessed as medium in three areas and high in the remaining two. However, post-mitigation assessments by Europol suggest an almost negligible risk (scoring 1 or 2 out of 25) across all areas. This suggests a significant reduction in both the probability of risks occurring and their potential impacts.

[redacted]

For this prior consultation Opinion, the EDPS will specifically address risks 1 and 5 of the DPIA. The EDPS notes that risks 1 to 3 are risks that more specifically stem from the proposed processing operation (rather than risks 4 and 5, which are cross-cutting across all of Europol's processing operations).

In addition, the EDPS has identified two specific further specific risks which may lead to the infringement of the Europol Regulation and for which it proposes mitigating measures:

- risk of lower accuracy processing for the faces of minors (as a form of bias); and
- the risk of incoherent processing by operating parallel systems (the existing FACE and the new NFW tool).

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

The EDPS **deems necessary** that a 'pilot' approach in handling facial images through the new facial recognition tool is adopted in order to ensure that the processing of facial images, as a special category of personal data under Article 30 ER, remains proportionate. This approach should lead to an evaluation after a six-month period.

The evaluation should allow Europol to determine what matching score confidence threshold and which rank capping would be appropriate to minimise the risks stemming from false candidates. Concerning the rank capping, it should establish the degree to which the results should be limited by a numerical cap, for instance after 20 results. While the system technically allows the display of up to 50 candidates, this should not be automatically taken as the appropriate number of results, given the potential impact on data subjects.

The lack of a matching threshold and the lack of a cap on the display of the results creates a risk of non-compliance with the strict proportionality requirement for the processing of biometric data under Article 30(2) ER.

As this pilot project approach requires measuring the performance of the tool over time (both as what the score of the selected image is and its ranking), Europol should ensure that for each search conducted, it is capable to capture these performance metrics over the duration of the pilot project. For each search, Europol should record if the search resulted in a lead (or several) or not, as well as the rank of each positive result (position in the list), the confidence scoring provided by the system for that (or those) positive results as well as the average confidence score for the set of 50 results and the standard deviation of the results list. As Europol is the controller in charge of the tool, the EDPS considers that it is best placed to propose the best way to record this information and then upon analysis provide a proposal of a ranking cap and matching score confidence threshold (for instance if the resulting functions for both variables could be modelled as a normal distribution, taking the average plus a number of standard deviations will allow to establish the desired confidence interval).

Europol should report to the EDPS the outcome of this analysis with supporting information, the proposed ranking cap and matching score confidence threshold including statistics from all searches performed during the pilot and the analysis supporting the proposal.

3.4.2. Risk of exceeding data retention by soft deletion of facial images.

[redacted] This reference will also serve as the main point for identification of data retention time expiration. The EDPS welcomes that Europol aims to develop a process to automate deletion of images when the relative case is also deleted from SIENA and expects this is in place by the end of the "pilot" period.

However, the EDPS understands that the result of this automatic deletion is a **soft deletion** of images, meaning that these will not be viewable and processed by the application, but they will not be deleted from the background file storage. Europol has provided information that a separate task needs to be activated for the actual deletion ([redacted] that would slow down the system.

The EDPS **recommends** Europol to ensure that hard deletion of facial images takes place as soon as possible to reduce the possibility of facial images being further processed after they have already been marked for deletion.

The time interval during which data are only soft deleted should also be aligned with Europol's upcoming operational data retention policy.

3.4.3. Other data protection risks

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

The EDPS **deems necessary** that Europol provides further evidence on the accuracy of the algorithm on minors under 12, before enrolling these minors in the use of the facial recognition system.

In case Europol cannot provide evidence on the potential bias of the system for these minors, then the processing of minors under 12 years old should be excluded from the system. Not doing so creates a risk of non-compliance with Article 71(1)(d) EUDPR ('accuracy').

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

The EDPS **deems necessary** that Europol define and implement a plan to migrate the facial images to the new system, following the same quality standards set for ingestion of new facial images and (if any) clarify the cases where the existing 'FACE' solution would be maintained and used as the only biometric tool processing facial images.

Not doing so risks incoherent processing (including accuracy levels) between different data subjects and therefore creates a risk of non-compliance with Article 71(1)(d) EUDPR ('accuracy').

Europol should define and start implementation of this plan by the end of the pilot project period.

4. CONCLUSION

The EDPS conducted its review of this prior consultation with a particular focus on Article 30(2) of the Europol Regulation, which was recently amended to include "biometric data for the purpose of uniquely identifying a natural person". As explained in this Opinion, the EDPS views this addition as clearly targeted at the application of facial recognition by Europol[54] and thus considers that Article 30(2) ER must be rigorously applied to this proposed processing operation.

In order to assess if the conditions of strict necessity and proportionality have been met in the proposed FRT solution, the EDPS examined both the different purposes for which data would be processed in the FRT solution and the technical conditions under which it would stored and analysed within this solution. The EDPS considers that both these factors play a

[54] In particular when read in light of Recital 46 of Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation PE/8/2022/REV/1 OJ L 169, 27.6.2022, p. 1–42 (stating that "photographs are covered by the definition of biometric data under Article 3, point (18), of Regulation (EU) 2018/1725 only when processed through a specific technical means allowing the unique identification or authentication of a natural person)".

crucial role in concluding whether FRT processing takes place in a way that can be considered strictly necessary and proportionate.

[redacted]

[redacted]

[redacted]

Recommendation 1. The **EDPS therefore deems it necessary**, prior to any processing of facial images for these two purposes using the proposed FRT solution, to:

a. describe the proposed implementation of each of these two purposes specifically;

b. perform an assessment of the necessity and proportionality of this proposed processing for each of these two purposes. This assessment must be documented in light of Europol's accountability requirements.

Not doing so would create a risk of non-compliance with Article 30(2) ER.

[redacted]

Recommendation 2. The **EDPS therefore deems it necessary for Europol** to specify the categories of individuals for whom facial recognition will be used in Europol's AP portfolio and provide concise use cases justifying its application. Not doing creates risks of non-compliance with the principle of purpose limitation as laid out in Article 71(1)(b) of the EUDPR and further specified in article 18(2)(c) and (3) ER.

As to the technical conditions for the processing, the EDPS formulates several recommendations to ensure the compliance of the processing with the Europol Regulation.

Recommendation 3. The EDPS **deems necessary** that Europol implements a 'pilot' approach in handling facial images through the new facial recognition tool in order to ensure that the processing of facial images, as a special category of personal data under Article 30(2) ER, remains strictly proportionate. This pilot should allow evidence-driven decision-making on which matching threshold and/or a numerical cap would further reduce the risks to data subjects while allowing the Agency to meet its intended purpose for the facial recognition solution. This approach should lead to an evaluation after a six-month period. Furthermore:

- Europol should ensure that it is capable to capture adequate performance metrics over the duration of the pilot project, including for each search: the matching confidence scoring of the lead(s) (if any) among the returned results and their rank, as well as the average matching confidence score of the whole search result set (regardless whether it resulted in a lead or not) and its standard deviation;

- Europol should report to the EDPS with the outcome of this analysis, including supporting information.

The lack of a matching threshold and the display of the maximum number of results in all cases creates a risk of non-compliance with the strict proportionality requirement for the processing of biometric data under Article 30(2) ER.

Recommendation 4. The EDPS **deems necessary** that Europol provides further evidence on the accuracy of the algorithm on minors under 12, before enrolling these minors in the use of the facial recognition system. In case Europol cannot provide evidence on the potential bias of the system for these minors, then the processing of minors under 12 years old should be excluded from the system. Not doing so creates a risk of non-compliance with Article 71(1)(d) EUDPR (‘accuracy’).

Recommendation 5. The EDPS **deems necessary** that Europol define and implement a plan to migrate the facial images to the new system, following the same quality standards set for ingestion of new facial images and (if any) clarify the cases where the existing ‘FACE’ solution would be maintained and used as the only biometric tool processing facial images. Not doing so risks incoherent processing (including accuracy levels) between different data subjects and therefore creates a risk of non-compliance with Article 71(1)(d) EUDPR (‘accuracy’).

Recommendation 6. The EDPS **recommends** Europol to ensure that hard deletion of facial images takes place as soon as possible to reduce the possibility of facial images being further processed after they have already been marked for deletion.

Done at Brussels on 20 December 2023

[e-signed]

Wojciech Rafał WIEWIÓROWSKI