



EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

EDPS OPINION ON A PRIOR CONSULTATION ON EUROPOL'S BIOMETRIC QUERIES OF SIS II

(Case 2022-0904)

1. INTRODUCTION

The EDPS issues this Supervisory Opinion in response to a Prior Consultation submitted by Europol to the EDPS on 9 September 2022, regarding Europol's use of the dactyloscopic component of the Schengen Information System II¹ ('SIS II AFIS²').

This Opinion follows a previous Opinion³ of the EDPS in accordance with the prior consultation procedure under ex-Article 39(1) of Regulation (EU) 2016/794⁴ ('the Europol Regulation'), issued on 3 June 2022. In that earlier Opinion, the EDPS concluded that Europol had not sufficiently identified the specific risks related to the inclusion of dactyloscopic searches in its

¹ The SIS II legal framework is composed of: Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third country nationals; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the use of the SIS in the field of border checks; and Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System in the field of police cooperation and judicial cooperation in criminal matters.

² Automated Fingerprint Identification System

³ EDPS Case 2022-0384.

⁴ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53-114.

SIS II workflow. Because of this, the EDPS was unable to determine whether the processing, as described in the data protection impact assessment ('DPIA') and the appended documentation, may involve a breach of any provision of the Europol Regulation, according to Article 39(4) ER.

Europol has now shared an updated DPIA for prior consultation with the EDPS.

The EDPS accounts for the fact that, between the EDPS' earlier prior consultation Opinion and the follow-up information provided by Europol, Regulation (EU) 2022/991⁵ entered into force, amending the Europol Regulation and aligning Europol's prior consultation framework with that applicable to other EU institutions, agencies and bodies under Chapter IX of Regulation (EU) 2018/1725⁶.

Under the threshold for prior consultation in Article 90 of Regulation 2018/1725, the EDPS is now to be prior consulted by Europol where processing which will form part of a new filing system to be created and:

- (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 subject.

This is a change from the wording of the previous Article 39(1) of the Europol Regulation, which required prior consultation for any new type of processing where:

- (a) special categories of data as referred to in Article 30(2) were to be processed; or
- (b) the type of processing, in particular using new technologies, mechanisms or procedures, presented specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.

⁵ 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.

⁶ 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.

Through this change, the provision for prior consultation by Europol is now aligned with the corresponding provision in Article 28(1) of the Law Enforcement Directive⁷. The EDPS finds it important to highlight this aspect. The general data protection regime, under Article 36 of the GDPR and Article 40 of Regulation 2018/1725, only subjects to prior consultation processing where a DPIA indicate that the processing would in the absence of mitigation measures, result in a high risk to the rights and freedoms of data subjects where this risk cannot be mitigated by reasonable means. Article 28 of the Law Enforcement Directive and Article 90 of Regulation 2018/1725 have a broader scope of application and refer to prior consultation processing for which a DPIA indicates that they would result in a high risk in the absence of mitigation measures (irrespective of the fact whether the controller is of the opinion that these risks cannot be mitigated by reasonable means) and types of processing that, by nature, include a high risk to the rights and freedoms of data subjects.

As this is the first prior consultation submitted by Europol under the amended Europol framework, the EDPS will also take this opportunity to clarify a number of aspects which it considers of particular importance to guarantee that both the DPIA process (which is now formalised in Article 89 of Regulation 2018/1725) and the prior consultation process meet the requirements of Regulation 2018/1725.

According to Article 90(4) of the Regulation, the EDPS has to provide its Opinion within a period of up to six weeks of receipt of the request for consultation, with a possible extension by one month. The notification was received on 9 September 2022. As the EDPS has not made use of its possibility to extend the deadline, the EDPS shall thus render its Opinion by 21 October 2022.

2. PROCEEDINGS

On 25 March 2022, the EDPS received a request for prior consultation from Europol under Article 39 of the Europol Regulation on the inclusion of a new type of query of the Schengen Information System ('SIS II'), namely dactyloscopic searches.

⁷ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89-131.

On 3 June 2022, the EDPS issued its Opinion concluding that Europol had insufficiently identified the specific risks related to the inclusion of dactyloscopic searches in its SIS II workflow. Therefore, the EDPS was unable to determine if the notified processing might involve a breach of any provision of the Europol Regulation and was, consequently, unable to make concrete proposals, where appropriate, to avoid such a breach under Article 39(3) of the Regulation to ensure compliance of the envisaged processing with the Europol Regulation.

Nevertheless, the EDPS did consider that specific risks to data subjects could well arise in this process, in particular during the assessment of the matches obtained from the SIS II - in case there would be no tailored strategy to identify the different categories of matches (print-to-print, mark-to-print, mark-to-mark). The EDPS also placed special consideration on the potential specific risks to data subjects stemming from comparisons between lower quality marks at Europol and SIS II.

The EDPS asked Europol to re-evaluate whether specific risks to data subject arise in these two areas, and if so, adopt a tailored mitigation strategy. Finally, the EDPS invited Europol to reassess whether alerts on missing persons should be included by default when comparing fingerprints or palm marks recovered from crime scenes, in light of the data protection principles of necessity and proportionality.

On 9 September 2022, Europol submitted an updated DPIA to the EDPS, addressing the points identified by the EDPS in its first Opinion. The DPIA was accompanied by a letter from Europol's Data Protection Officer ('DPO'). While there was no additional documentation included in the package, the EDPS will, for the purpose of this opinion, also consider the documents provided by Europol in the scope of the previous prior consultation.

In particular, the EDPS will take into account the following documents:

- two copies of the SIS II Interface Control Document⁸, version of 8 October 2021;
- Europol's process description for cross checking data and managing hits⁹, version of 23 March 2021;
- Europol's manual of data review¹⁰, draft version of August 2019;
- a process description for the data review process in Europol Analysis System ('EAS')¹¹, version of 8 December 2017;
- a copy of the EAS manual¹², version of June 2019;

⁸ EDOC#1196887 and EDOC#1196887.2, both documents share a 'version number' of v.4.9.0.12.

⁹ EDOC#1145817v3.

¹⁰ EDOC#969053v8.

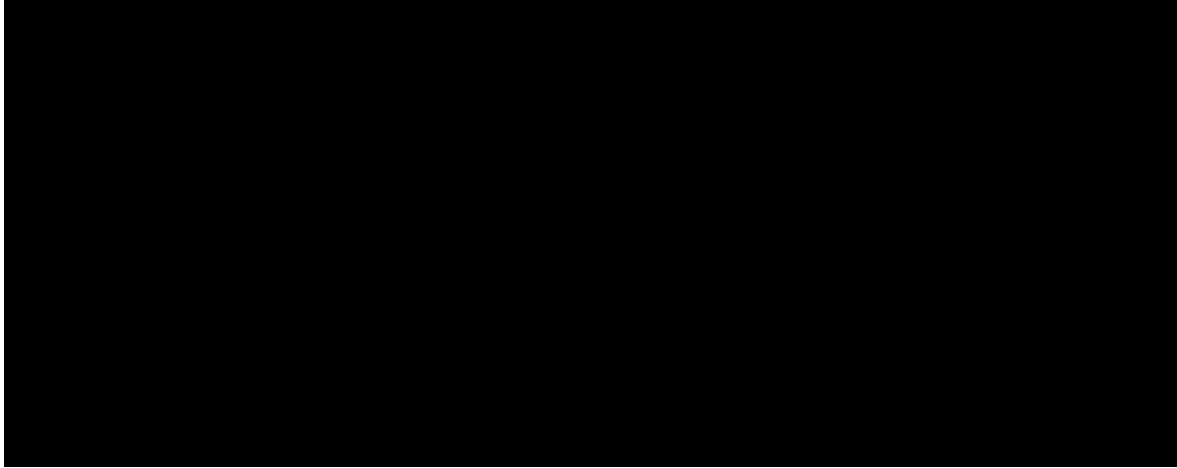
¹¹ EDOC#893701v12.

¹² EDOC#886249v16.

3. DESCRIPTION OF THE PROCESSING

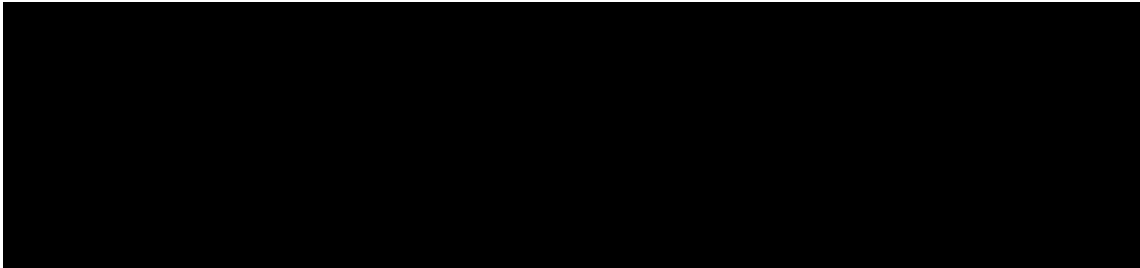
As the process is already described in detail in the EDPS' previous Opinion¹³ on Europol's dactyloscopic searches of SIS II, the EDPS will simply reiterate the main processing under consultation.

Europol plans to perform the following types of dactyloscopic searches in SIS II:



Europol will have a trained fingerprint expert access and validate the matches in SIS II AFIS by comparing the fingerprints sent in the NIST file¹⁴ with the fingerprints returned in the search result.

¹³ EDPS Case 2022-0384.



4. LEGAL AND TECHNICAL ASSESSMENT

4.1. Need for prior consultation pursuant to Article 90 of Regulation 2018/1725

As indicated in the introductory part of this Opinion, the main Article defining the requirements for prior consultation in the amended legal framework that now applies to Europol is Article 90 of Regulation 2018/1725.

Consultation of the EDPS must take place prior to processing which will form part of a new filing system to be created (which is the case here as the foreseen processing involves new processes of receiving, storing and cross-matching dactyloscopic data by Europol against SIS II, in line with the definition of a filing system under Article 3(7) of Regulation 2018/1725)¹⁵ and where one of two scenarios occur:

- (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 subject

This second scenario is an acknowledgement of the high impact that law enforcement processing has on data subjects, and establishes that some law enforcement processing operations should always be subject to prior consultation. This relates in particular to cases where the controller would use new technologies (such as Machine Learning or Artificial Intelligence), mechanisms or procedures, which by themselves pose high risks to the rights and freedoms of data subjects. This also means that Europol should first assess whether the type of processing in and of itself involves high risks and qualify for prior consultation with the EDPS under Article 90(1)(b) Regulation 2018/1725.

While the text of the provision ‘in particular, where using new technologies, mechanisms or procedures’ gives an indication of relevant factors for this exercise, these three elements are not necessarily the only ones that could prompt a prior consultation. Other elements to be taken into account are for instance the processing of special categories of personal data or processing targeted at special categories of individuals such as minors.

¹⁵ For further information refer to EDPS Opinion on a Prior Consultation on conducting dactyloscopic searches in the Schengen Information System (SIS II) of 3 June 2022 (Case 2022-0384), p.6.

The EDPS notes that for future prior consultations, the internal assessment done by Europol should also always include an assessment of the second ground of Article 90 of Regulation 2018/1725. The EDPS notes that this was not expressly included, either in or next to the DPIA that was shared with the EDPS.

In case the outcome of assessing the second ground of Article 90(1) is that the specific type of processing does not involve high risks for the rights and freedoms of the data subjects, Europol should nevertheless assess the first ground provided in the same article. To that end, the list of criteria for assessing whether processing operations are likely to result in high risk contained in Annex 1 of the Decision of the EDPS of 16 July 2019 on DPIA lists issued under Article 39(4) and (5) of Regulation (EU) 2018/1725 provide indicative criteria that should be taken into account for this threshold assessment.

The EDPS understands that Europol, in the context of the risk assessment conducted for the drafting of the DPIA, has come to the conclusion that the cross-matching of biometric data against SIS II database did not involve high risks to data subjects.

However, when assessing the risks for the rights and freedoms of data subjects, the EDPS attributes particular weight to the nature of the data being processed.¹⁶

In this case, the processing is designed to work with biometric data. With the amendments made by Regulation (EU) 2022/991 to the Europol Regulation, Article 30(2) on special categories of personal data was modified to now explicitly mention biometric data as a special category of data. This already demonstrates that the processing of biometric data involves a higher risk for data subjects. This is in part due to the fact that biometric data are permanently and irrevocably linked to a person's identity. Their use thus could be used as a unique identifier to build a complete profile around this person. Any error in the identification process could also lead to disastrous consequences for the enjoyment by this person of his or her rights and freedoms.

In addition, the processing at stake concerns comparisons between data held at Europol and data stored in SIS II, which may not have been initially collected for law enforcement purposes. Most particularly, the processing

¹⁶ See EDPB Guidelines of 4 October 2017 on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, pp.8-12; see also EDPS Guidance of 16 July 2019, Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies.

of biometric data extracted from the SIS database by Europol could imply the re-purposing of biometric data collected for migration management purposes for law enforcement purposes, such as in the cases where an alert has been created for refusal of entry. This re-purposing, even if established by law, inherently involves a high risk for the data subjects, as it has a direct impact on a number of fundamental rights and freedoms enshrined in the EU Charter of Fundamental Rights that may go beyond privacy and data protection, such as freedom of movement.

Finally, the EDPS takes into account the magnitude of the processing at stake as additional risk factor, as the SIS database is a large-scale system which enables the immigration, police, customs and judicial authorities of the Member States to cooperate and exchange information. Europol is giving access to a large databases of fingerprints in that context.

Taking these elements into account, the EDPS concludes that the processing operations described under Chapter 3 of this Opinion, involve a high risk to the rights and freedoms of data subjects and therefore fall within the scope of **Article 90(1)(a) of Regulation 2018/1725**.

4.2. Assessment of the updated DPIA

As already indicated above, the recent amendment of the Europol Regulation has aligned the prior consultation regime of Europol with that of the national EU law enforcement authorities¹⁷, as well as other EU institutions, bodies or agencies subject to Chapter IX of Regulation 2018/1725. As a consequence of this, Article 90 of Regulation 2018/1725 places an increased emphasis on the evaluation of **high risks** to data subjects. The EDPS will examine in this prior consultation Opinion whether Europol has identified and satisfactorily mitigated high risks to data subjects in the proposed processing operation.

The EDPS will therefore first look into whether the risk scoring mechanism, which has so far been applied by Europol for prior consultations under ex-Article 39 of the Europol Regulation, remains fit for purpose in view of the need to objectively (as far as possible) estimate the risk level to data subjects - under Article 90 of Regulation 2018/1725.

Afterwards, the EDPS will examine the additions made by Europol, which have been clearly marked by Europol throughout the document.

¹⁷ Who are subject to the nearly identical Article 28 of the Law Enforcement Directive.

Europol's risk evaluation methodology

Scoring system

The EDPS notes that Europol's risk scoring system relies on three levels ('low', 'medium' and 'high') for the severity and impact level of the initial risks to data subjects. After applying mitigating measures (indicated under recommended controls), the Agency then provides a single score for the overall residual risk level after mitigation.

The EDPS makes the following recommendations to increase the transparency of Europol's risk assessment table, in order to improve the effectiveness of the DPIA and prior consultation procedures:

First, **the EDPS recommends** Europol to include a cover page to its risk assessment table, which clarifies the thresholds for the different levels (regardless of whether Europol continues to use three levels, or decides to move to a different system)¹⁸. For the likelihood, this cover page should include an estimation of what it means that something has e.g. a 'medium' likelihood of occurring. For the severity of the risk to data subject, Europol could provide examples for each of the levels it indicates (e.g. 'death/threat to life for the data subject' for the highest severity level). By doing so, the risk assessment would provide more meaningful and actionable risk information to Europol as the controller.

Second, **the EDPS recommends** Europol to indicate which formula it uses to calculate when a certain likelihood and severity amount to a 'high' risk (i.e. whether a low likelihood and a high severity would qualify as a low, medium or high risk). While the EDPS does not impose any particular scoring methodology, provided that it allows for a clear overview of the effectiveness of mitigating measures, Europol could consider using a numerical system, as is used by several other EU institutions, agencies and bodies - whereby the likelihood and severity levels are multiplied to arrive at the overall risk level.

Third, in order to evaluate the residual risk to data subjects, **the EDPS recommends** Europol to use the same two columns (severity and likelihood) for the residual risk as well. With the current implementation of the table, it is not clear why a certain risk level has been reduced (whether it is because of the reduced likelihood or the reduced severity).

¹⁸ The EDPS however notes that there is a risk that three levels may not allow for sufficient granularity for Europol's assessment purposes.

Mitigating measures

As regards the mitigating measures introduced by Europol to lower the risks it has identified, the EDPS notes the positive work that has been done by Europol to identify appropriate mitigating measures, including additional ones following the previous prior consultation of the EDPS. In particular, the EDPS agrees with Europol that the following measures would contribute to a meaningful lowering of the risks (in particular risks 2, 3 and 9):

- The overall approach by Europol to only query SIS with data from non-Schengen Third Countries, or Member States with no SIS access, to avoid duplication and exclude routine access.
- The planned regular trainings on data security and data protection for the staff authorised to have access to SIS.
- The disclaimer to be displayed in USE to inform authorised staff of possible risks.¹⁹

Given the importance of accurately determining the level of the 'initial risk' to data subjects in order to evaluate the need to launch a prior consultation with the EDPS, it is important to highlight (for the future) that where mitigating measures are part of the essential design of the system (e.g. a certain system is by design only querying select amounts of data), this can and should be included in the calculation of the initial risk (meaning the initial risk would be lowered).

This would for instance be the case if only a very restricted location of data would be included in a querying mechanism at Europol. In this scenario, where risk is assessed in the context of a DPIA leading to a prior consultation under 90(1)(a), the fact that only limited information (by design) is being processed by the system would lower the initial risk, meaning that a prior consultation may not be necessary. The DPIA exercise and (where appropriate) subsequent prior consultation of the EDPS are designed to be practical tools to be used by a controller in a concrete scenario, meaning there would not be a need to consider 'in abstract' what the risk to data subjects would be if the purpose of the system would be fundamentally different.

While Europol has accurately placed its mitigating measures for this prior consultation, the EDPS would nonetheless take this opportunity to already

¹⁹ The EDPS notes that, while not indicated under R9 (risk that a false negative result could entail for Print to Mark searches), a disclaimer may potentially mitigate the risks to data subjects to some extent, even where Europol cannot control the automated steps in external systems hosted by eu-LISA.

provide guidance on this point, as this has been a recurring issue in prior consultations received from multiple European Institutions, Bodies and Agencies. Given that this is the first prior consultation received by the EDPS under Chapter IX of Regulation 2018/1725, which has the 'initial high risk' threshold that is also used by other EUIs in this domain, the EDPS wants to proactively communicate its advice on this matter.

As another point which should be taken into account for the DPIA and prior consultation exercise, **the EDPS would like to highlight** that any references to Europol's legal framework cannot be seen as an additional mitigating measure, as indicated under risk 4 on page 25 of Europol's DPIA. Here, Europol defines as a mitigating measure that 'matches on information contained in SIS will only be processed to the extent that it is proportionate and required to prevent or investigate a crime that falls under Europol's mandate.' Adherence to the Europol Regulation is a non-optional requirement for any system to be created by Europol and should always be complied with for the design of the initial system.

4.3. Specific EDPS comments on the risks identified and changes made by Europol

Previously identified risks

Risk 1

The first risk which is identified by Europol is the following: 'Disclosure of information, the relevance of which for the prevention and combatting of serious crimes and terrorism, may not always be evident'. This risk was scored by Europol with an initial impact level of 'medium' and an initial likelihood of 'low'. After applying mitigating measures, the residual risk level identified by Europol is low. This is marked as a general risk applying to all types of dactyloscopic queries, and indeed, it has been historically included in many (if not most) of Europol's risk assessments.

The EDPS notes that, at least from the recommended controls, Europol foresees two separate ways in which the risk for the 'disclosure of non-relevant data' may occur. The first way is that an incorrect match is generated within SIS AFIS, meaning that the wrong person's fingerprints are returned. The control that Europol has put in place here is to have an assessment of the list of matches (potential hits) returned by SIS AFIS, by the Europol Fingerprint specialist for verification, and therefore to determine whether such data is relevant to a particular case.

The second way in which a non-relevant disclosure may occur, is by further processing information in Europol's systems (and potentially disclosing it to the Third Party who submitted the dactyloscopic data in the first place), without the consent of the issuing Schengen State. Here Europol's mitigating measure is to always ask for consent of the issuing authority prior to further processing within Europol's systems (which the EDPS notes is a legal obligation under e.g. Article 48(4) of Regulation (EU) 2018/1862). While it has not been included in this prior consultation, the EDPS also recalls from a previous prior consultation on Europol's access to SIS II using biographical data, that Europol's default *modus operandi* is to have the issuing Member State contact any third party. As such, Europol will only play the role of interlocutor when asked to do so, or otherwise explicitly confirmed by the Member State.


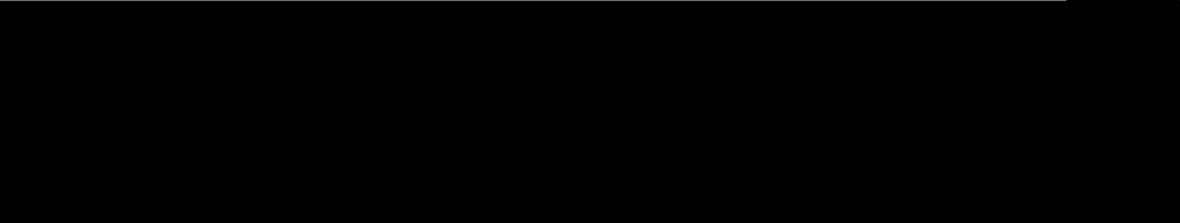
The EDPS refers back to earlier in this Opinion, where the EDPS discussed exactly the issue of using a legal obligation as a mitigating measure. In this case, it is a legal obligation of Europol under the SIS II framework to always obtain the issuing Member State's consent prior to further processing SIS II data (whether or not dactyloscopic). However, as Europol put the legal obligation as a mitigating measure, the EDPS cannot tell whether the initial risk was calculated 'as if this legal obligation did not exist', which would artificially boost the initial risk. Of course, Europol should comply with the legal obligations of the SIS II framework, and should clearly mention that it is under this legal obligation, but it should not use this as a mitigating measure but as part of the process description.

Otherwise, the EDPS is satisfied with the controls for the risks that have been identified. However, the EDPS does recommend to connect the mitigating measures more clearly to the risk that they are supposed to mitigate (as in this case, two separate risks/mitigating measure sets are bundled into one). The **EDPS also recalls its previous concerns over the onward communication of SIS II data, and the need to promote that the status of data subjects in third party systems accurately reflects their status in the SIS II**, in particular where the SIS II alert is changed to the benefit of the data subject, and Europol itself has been asked to share personal data with third parties. Situations should be avoided where the data subject of an SIS II alert continues to be subject to measures abroad, based on previous information included in an SIS II alert²⁰ that is no longer valid, such as where it has been amended or erased in the meantime.

²⁰ Underlying which of course is a national investigation.

Risk 2

The second risk identified by Europol is the risk of 'unauthorised access to SIS AFIS', which is another risk that exists in one form or another for all of its systems. The mitigating measures proposed by Europol are to



As the current prior consultation concerns an 'update' of the general regime for SIS II access for Europol, to include dactyloscopic searches of SIS AFIS, Europol could generally refer back to its overall access management regime for SIS II, and focus on emphasising the novel verification step (and how it has implemented access management for this step).

The EDPS recommends Europol to verify whether the mitigating measures that it has identified (required training on SIS II and appropriate knowledge about data security and data protection rules) are also applied to Europol's fingerprint expert. In any case, it should be documented how access management is handled for the fingerprint expert (even if this boils down to an acknowledgement that the same rules apply). Also, the limitation of access to SIS "only to duly empowered staff who have a need to know" should be supported by an access control policy envisaging procedures to ensure timely updates from human resource management.

Risk 3

The third risk mentioned by Europol is referred to as the 'risk of indiscriminate access'. The EDPS considers that this risk is formulated too vaguely, and should be further specified for future prior consultations.

From the recommended controls section on page 25, the EDPS can deduce that the risk Europol is referring to is of *'Europol searching SIS AFIS in scenario where it would not need to, because either the personal data was contributed by a Schengen country (so they simply could have made the search themselves), by an entity who has not yet searched their own fingerprint database (which may give them the results without having to search SIS II)'*. This risk was scored by Europol with an initial impact level

of 'medium' and an initial likelihood of 'low'. After applying mitigating measures, the residual risk level identified by Europol is low.

In case the understanding of the EDPS of risk 3 is correctly derived from the recommended controls, the EDPS is glad to note the multiple steps that will be undertaken by Europol to avoid unnecessary dactyloscopic searches of SIS AFIS. The EDPS was already aware, from the previous prior consultation on SIS II biographical access, that Europol generally only searches SIS for contributions by entities that do not have SIS II access themselves, which the EDPS believes is an excellent strategy to avoid duplication. The EDPS also supports Europol's use of a set of established criteria, [REDACTED] to perform a case-by-case assessment of whether the dactyloscopic data should be used to query SIS AFIS. As part of this, the EDPS follows Europol's approach that marks should be searched in a contributor's own fingerprint database first.

The EDPS is therefore satisfied that Europol has undertaken multiple steps to further reduce the risk to data subjects from unnecessary searches, which may indeed have reduced the risk level to a relatively 'low' level.

Risk 4

Europol has also identified a risk concerning the 'unnecessary storage of data' throughout the processing lifecycle of SIS II data. While the risk is not further expanded upon, Europol proposes four mitigating measures. Two of these are related to logging, with Europol stating that 'all data processing operations related to accessing SIS data by Europol are logged for the purposes of checking the admissibility of the request' (which is a legal obligation under Article 48(7) and that these logs will be integrated with Europol's Unified Auditing Solution (UAS).

Europol also reiterates two previous mitigating measures, which are both legal obligations stemming from the SIS II framework, namely:

- Europol will store and use SIS data in accordance with the ER only after receiving consent from the MS concerned.
- Europol will delete information containing personal data at the latest one year after the related alerts have been deleted in SISII (unless Europol has information in its databases on a case to which the supplementary information is related and has duly informed and provided justification to the relevant parties).

The EDPS notes that the only 'optional' measure that Europol has taken in this field, is to integrate the logs with the Unified Audit Solution. The EDPS supports this decision by Europol, as it can facilitate the monitoring of the accesses to SIS, allowing Europol to detect and correct excessive or abusive accesses to the platform.

As the other three measures are mandatory under the SIS II framework, they would need to be considered as part of the initial risk assessment. **The EDPS therefore asks Europol** to consider what the impact of the integration of the logs in the UAS would be on the risk of 'unauthorised storage of data' that was identified by Europol with a severity score of medium and a likelihood of low (and what this means for the residual risk).

Additional risks identified by Europol depending on the query type

Risk 5, 8 & 10 (risk of false positives for print-to-print, print-to-mark and mark-to-print/mark searches)

As regards the risk of false positives for searches of SIS AFIS, Europol discusses the risk in three different query types, namely:

- the risk of false positives in [REDACTED] in risk 5;
- the risk of false positives in [REDACTED] in risk 8;
- the risk of false positives in [REDACTED] in risk 10.

Europol clarifies that false positive results occur in occasions of erroneous matching of fingerprints that did not originate from the same source.

Europol mentions that generally, false positive and negative results could occur both when a search is run against SIS AFIS fingerprints and finger and palm marks, as the matching accuracy is direct proportional with the amount of information and quality of the fingerprints templates searched or present in SIS AFIS database [REDACTED]

The EDPS will discuss these risks, and the corresponding mitigating measures, in the same chronological order as they were presented by Europol (5, 8, 10) as it appears that for each step, additional safeguards are being put in place by Europol, owing to the gradually increasing uncertain nature of the three types of searches [REDACTED]

To mitigate the risk of false positives for [REDACTED] (risk 5), Europol proposes to put in place three measures.

First, all matched fingerprint results returned by SIS AFIS will be verified and validated by Europol's fingerprint expert.

Secondly, Europol mentions the following 'Europol will not implement a fully automated "lights-out" approach, since the results are not as accurate as if they are confirmed by fingerprint specialist conducted comparison'. Europol does not explain anywhere what it means by 'lights-out' approach, leaving it unclear to the EDPS what the additional mitigating effect of this second sentence is.

[REDACTED]

The EDPS considers that these are core issues, which are likely to be tackled in the SIS AFIS incident management procedure. However, this document should comply not only with the requirements of the SIS II framework but also with the Europol Regulation. **The EDPS requests to be provided with this document as soon as it becomes available to Europol, in order to be able to verify how it proposes to mitigate the risk of false positives over time.**

The EDPS notes that for [REDACTED] (risk 8), Europol applies the same two first mitigating measures, while adjusting the third mitigating measure as follows: [REDACTED]

As in this case, the risk concerns [REDACTED] it appears that this mitigating measure has been misplaced by Europol.²¹ Indeed, in the [REDACTED] mode, a maximum number of candidates would be returned based on a threshold [REDACTED]²², as Europol proceeds to indicate

²¹ The EDPS reminds that in the processing description given by Europol earlier in the DPIA, [REDACTED] (which in the SIS II technical documentation is referred to as [REDACTED])

²² See page 244 of EDOC#1196887 (SISII-ICD-v4.9.0.12.)

under risk 10. **The EDPS ask Europol to adjust this mitigating measure and align it with the correct corresponding risk.**

For **risk 10**, Europol groups the risk of false positives for [REDACTED] [REDACTED] Aside from the previously mentioned mitigating measures, the EDPS is glad to note that Europol will follow eu-LISA's recommendation [REDACTED] [REDACTED]²³), and that for its searches it will use marks that are previously encoded by the finger specialist.

Risk 6, 9 & 11 (risk of false negatives for print-to-print, print-to-mark and mark-to-print/mark)

As regards the risk of false negatives for searches of SIS AFIS, Europol equally discusses the risk in three different query types, namely:

- the risk of false negatives in [REDACTED] in risk 6;
- the risk of false negatives in [REDACTED] in risk 9;
- the risk of false negatives in either [REDACTED] [REDACTED] in risk 11.

As a first mitigating measure that Europol will apply to mitigate **risk 6**

[REDACTED]

The EDPS understands that the extended report function refers to the optional [REDACTED] functionality [REDACTED]

[REDACTED]

[REDACTED] Particularly for false negatives, **the EDPS is satisfied** that this would indeed increase the likelihood that the matching person would be found through the search mechanism.

This risk also includes, as a mitigating measure, [REDACTED]

[REDACTED]

[REDACTED]

²⁴ EDOC#1196887.

[REDACTED]

The EDPS recalls its earlier comments on this mitigating measure, however for clarity, the EDPS advises Europol not to repeat this measure here under risk 6, as it does not address this risk.

Risk 11 [REDACTED] of the updated DPIA refers that [REDACTED]

[REDACTED]

The EDPS takes note that there is a default number of matched candidates returned by SIS II queries, and that the only means to adjust the number of results from client side is through adjusting the minimum accuracy score.

Taking into account the principle of data minimisation, the number of candidate matches should be adjusted to the needs of Europol while bearing in mind that a larger number of candidate matches with lower level of similarity will, most likely, result in a larger amount of false positive results.

This measure would also address risk 12 (unnecessary access to data), in the way that the quality of the marks is a decisive factor to determine the level of accuracy of the query.

The EDPS recommends Europol to define user procedures specifying the minimum level of accuracy required during the searches, to better adjust the number of candidate matches returned by SIS II. The definition of the minimum threshold should depend on the quality of the existing fingerprint, or palm print, mark and other features that Europol might deem relevant. This mitigating measure would be relevant for risk 10, and 12 as well.

Risk 13

The risk assessment indicates that [REDACTED]

[REDACTED]

²⁵ Risk assessment, risk R11, footnote 12.

[REDACTED]

It is unclear to the EDPS if having only one available position [REDACTED] derives from a decision from the Europol management or from any other kind of limitation. It is also unclear whether [REDACTED] can be assured by more than one element of Europol.

Given the responsibility of the task, **the EDPS recommends** Europol to ensure that the fingerprint evaluation is carried by, at least, [REDACTED]

5. CONCLUSION

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

1. to ensure compliance with Article 20(4) of the Europol Regulation on access to information as well as the principles of purpose limitation and security under Articles 71(1)(b) and (f) EUDPR:
 - to verify whether the mitigating measures that Europol has identified for biographic searches (required training on SIS II and appropriate knowledge about data security and data protection rules) are also applied to Europol's fingerprint expert and to document how access management is handled for the fingerprint expert (even if this boils down to an acknowledgement that the same rules apply);
 - To ensure that the limitation of access to SIS "only to duly empowered staff who have a need to know" is supported by an access control policy envisaging procedures to ensure timely updates from human resource management.
2. to ensure compliance with the principle of data accuracy under Article 71(1)(d) EUDPR:
 - to verify and document that the SIS AFIS incident management procedure for false positives complies with the requirements of both the SIS II and Europol frameworks; The EDPS also requests to be provided with this document as soon as it becomes

available to Europol, in order for the EDPS to be able to verify how it proposes to mitigate the risk of false positives over time.

- for [REDACTED] to define user procedures specifying the minimum level of accuracy required during the searches, to better adjust the number of candidate matches returned by SIS II. The definition of the minimum threshold should depend on the quality of the existing fingerprint, or palm print, mark and other features that Europol might deem relevant
- to ensure that the fingerprint evaluation is carried by, at least, [REDACTED]

In addition, as this is the first prior consultation submitted by Europol under the amended Europol framework, the EDPS has also taken this opportunity to make further recommendations to guarantee that Europol's DPIA process (under Article 89 of Regulation 2018/1725) and prior consultation process (under Article 90 of Regulation 2018/1725) meet the requirements of these provisions, and to increase the overall utility and transparency of these processes. These recommendations are:

3. to include a cover page to its risk assessment table, which clarifies the thresholds for the different levels (regardless of whether Europol continues to use three levels, or decides to move to a different system)²⁶. For the likelihood, this cover page should include an estimation of what it means that something has e.g. a 'medium' likelihood of occurring. For the severity of the risk to data subject, Europol could provide examples for each of the levels it indicates (e.g. 'death/threat to life for the data subject' for the highest severity level). By doing so, the risk assessment would provide more meaningful and actionable risk information to Europol as the controller.

4. to indicate which formula it uses to calculate when a certain likelihood and severity amount to a 'high' risk (i.e. whether a low likelihood and a high severity would qualify as a low, medium or high risk). While the EDPS does not impose any particular scoring methodology, provided that it allows for a clear overview of the effectiveness of mitigating measures, Europol could consider using a numerical system, as is used by several other EU institutions, agencies and bodies - whereby the likelihood and severity levels are multiplied to arrive at the overall risk level.

²⁶ The EDPS however notes that there is a risk that three levels may not allow for sufficient granularity for Europol's assessment purposes.

5. in order to evaluate the residual risk to data subjects, to use the same columns (in this case, two columns for severity and likelihood) for the residual risk as well. With the current implementation of the table, it is not clear why a certain risk level has been reduced (whether it is because of the reduced likelihood or the reduced severity).

6. not to include legal obligations (such as those in the SIS II framework), as a mitigating measure but as part of the process description. Legal obligations are non-optional requirement for any system to be created by Europol and should always be complied with for the design of the initial system.

7. to consider what the impact of the integration of the logs in the UAS would be on the risk of 'unauthorised storage of data' that was identified by Europol with a severity score of medium and a likelihood of low (and what this means for the residual risk).

8. to (only) align mitigating measures with the correct corresponding risk. For instance where a measure addresses false positives, but is located in the false negatives section.

Done at Brussels on XX October 2022

Wojciech Rafał WIEWIÓROWSKI
(e-signed)