EDPS SUPERVISORY OPINION ON A PRIOR CONSULTATION REQUESTED BY EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL) ON THE PROCESS OF AUTOMATING THE PROCESSING OF DATA ORIGINATING FROM THE UNITED STATES NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN (NCMEC) FOR FURTHER DISSEMINATION TO EUROPEAN UNION MEMBER STATES (Case 2023-0142)

1 PROCEEDINGS

(1) On 3 February 2023, the European Union Agency for law enforcement cooperation ('Europol') submitted via its Data Protection Officer ('DPO') to the European Data Protection Supervisor ('EDPS') a request for prior consultation regarding the process of automating the processing of data originating from the United States National Center for Missing and Exploited Children ('NCMEC') for further dissemination to European Union Member States ('EU MS'). This request was submitted under Article 90 of Regulation (EU) 2018/1725 ('EUDPR')[1] read in conjunction with Article 39 of Regulation (EU) 2016/794 as amended ('Europol Regulation)[2].

[1] Regulation (EU) 2018/1725 of the European Parliament and of 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 (Text with EEA relevance.), PE/31/2018/REV/1, OJ L 295, 21.11.2018, p. 39–98.

[2] 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.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

(2) The request for prior consultation sent by Europol contained:

- The Data Protection Impact Assessment ('DPIA')[3].

(3) Attached to the request for prior consultation were the following supporting documents:

- The prior consultation request signed by the DPO[4];
- The NCMEC Data Flows Solution Blueprint[5];
- The General Description of Envisaged Processing Operation and related risks and mitigating measures(additional information)[6];
- Supplemental information - Online Service Providers Platform - EDPS[7];
- The EDPS Opinion regarding a new Online Service Provider Referral System (EDPS Case 2019-0850)[8];
- Global Response Against Child Exploitation ('GRACE'), D2.1 - Use Cases, Process and Data Flows Refinement (Deliverable)[9];
- Global Response Against Child Exploitation ('GRACE'), D2.7 - Definition of Standardised Taxonomy and Information Exchange Formats (Deliverable)[10];
- Global Response Against Child Exploitation ('GRACE'), D10.6 Stakeholder and policy recommendations for addressing online CSEM V1[11];
- The Article 39 Europol Regulation - Prior Consultation Form on the Cross Domain Solution[12].

(4) On 2 March 2023, a meeting took place between the EDPS and Europol to clarify the scope of the consultation request and several aspects of the DPIA, including the description of the processing operations envisaged, the workflows, and the risks to the rights and freedoms of data subjects.

(5) Further to this meeting, Europol submitted the following supporting documents:

- A power point presentation regarding the NCMEC Data Flows;
- The NCMEC - NEO mapping; and
- A sample cross-match report.

(6) In response to additional questions posed by the EDPS on 7 March 2023, Europol provided further clarifications on 9 March 2023.[13]

---

3 EDOC # 1252943 v4.

4 Letter of 2 February 2023;

5 EDOC # 1257710 v5A.

6 EDOC # 1085203v2.

7 EDOC #1098381 v2.

8 EDOC # 1103737.

9 EDOC # 115396 v1.

10 EDOC # 115397 v1.

11 EDOC # 115399 v1.

12 EDOC # 1106488 v6.

13 Email of Europol to the EDPS of 9 March 2023.

(7) According to Article 90 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 a month.

(8) Taking into account the complexity of the intended processing and for the reasons explained in detail in the email that the Head of the Supervision and Enforcement Unit addressed to Europol's DPO on 3 March 2023, the EDPS informed Europol that the deadline would be extended by one month. The EDPS is thus **to render his Opinion by 20 April 2023**.

2 DESCRIPTION OF THE PROCESSING

2.1 Current Europol NCMEC report processing and dissemination service

(9) The current processing operation involves the downloading, processing and dissemination of Child Sexual Abuse Material ('CSAM') referrals by Europol. These referrals are originally reported by Online Service Providers ('OSPs') based in the United States of America ('US'). These companies are obliged by US law to report what they assess as potential child sexual abuse or exploitation material disseminated through their platforms. These referrals are then received by the US based non-governmental organisation, NCMEC, who structures them, assesses the likely concerned countries (including EU Member States) and makes them available to law enforcement (including Europol) [redacted].

(10) These referrals contain textual and media information concerning a potential child sexual abuse related offence, [redacted] reported by online service providers. These reports usually contain information about the allegedly criminal activity (data about suspects, victims, recipients of the material, and the CSAM itself) in addition to supplementary information provided by the analysts of the online service provider (e.g. subscriber information, transactional data, etc.) and by NCMEC (so called 'open source intelligence').

(11) The information contained in a significant proportion of the reports include categories of data subjects referred to in Article 30(1) of the Europol Regulation (e.g. victims, minors). The information processed may occasionally as well include, in cases of misreported referrals, special categories of data such as information on sex life as defined in Article 30(2) ER.

(12) The US Immigration and Customs Enforcement ('ICE') [redacted] sends the SIENA messages indicating the amount of referrals to be downloaded [redacted]

(13) Technically, the **current NCMEC dissemination service** operates as follows:

a. [redacted]

[redacted]

[redacted]

(14) The current Europol NCMEC report processing and dissemination service however presents a series of shortcomings that according to Europol will only be aggravated by the continuous increase in the amount of reports of suspected child sexual abuse criminal activity by the online service providers, namely[14]:

- Delay in the processing of the referrals as they are polled and processed only once per week, which in turn delays the transmission of information to Member States

[14] NCMEC Data Flows Solution Blueprint – EDOC 1257710.

and third associated countries (referred to in the Solution Blueprint as the Associated Countries.[15]

- Delays created by the performance of several manual steps to facilitate the flow of information to all required Europol systems. High-volumes of data processed increase these delays.
- Data retention: All reports received from NCMEC and sent to Associated Countries are stored as duplicates in the system (the original download which was sent and the wave package that is processed under the relevant country folder), with two negative consequences: a) additional complexity from a data retention perspective for the data and b) increasing demands of storage space in the systems.
- Security: [redacted]

These shortcomings prevent national investigators to promptly act on the compiled reports that should be treated as a priority. The investigators in the countries need to be able to prioritise quickly the referrals based on the information reported by NCMEC and the OSPs, but also based on the intelligence provided by Europol.

2.2 New Europol NCMEC report processing and dissemination service

(15) In order to address these shortcomings, Europol proposes a new architectural solution for the improvement of the current processing, called 'Solution Blueprint on NCMEC Data flows analyses'. The new capabilities offered with the proposed solution will include as mentioned above, the ability for Europol to support continuous and automated data acquisition from NCMEC.

(16) As a first step, Europol proposes some changes in the process primarily intended to improve the quality of the intelligence compilation process, by modifying some of the existing components and services and introducing a few new set of components and services aiming at:

a. Improving the automation as an end-to-end process with standardised, near-real time processing of the NCMEC referrals, minimum manual intervention and by leveraging existing ICT capabilities and processes at Europol. Past referrals will be able to be acquired by report ID, which will remove to need to store this data for extended periods and helps handle error cases. The referrals will be processed as and when they are made available by NCMEC. The services are thus expected to minimise data storage and retention needs and capture audit log of user actions.

b. Increasing the security and the data quality controls by:

   i. introducing analysis of referral meta-data to assess potential data quality issues early in the process. Data quality issues will be checked

[15] Member States and Third countries that can receive personal data from Europol as per Article 25.1 a, b, c and 4a of the Europol Regulation, for which Europol currently offers the NCMEC referral dissemination service. These countries are associated to AP Twins.

and will enable in the future to introduce new controls and remedies in the process. Europol will be able to better monitor the process for successful executions [redacted] and collect process statistics so that data volume trends can be monitored for the scaling of infrastructure resources proactively. An automated cross-checking against EAS will be available with the new service. The services will provide the ability [redacted] analysts to dedicate more time to the operational analysis of this dataset using the current and future analytical tools and methods, saving significant amount of time due to automation of routine tasks.

ii. [redacted]

iii. ensuring the systematic collection and analysis of process statistics to scale the solution, as necessary. Europol will be able to collect statistics from the data content for strategic analysis.

(17) The proposed new architectural solution will include two main business services and products:

1. Referral Dissemination Service: This business service delivers the NCMEC referrals to all Member States and Associated Countries. [redacted]
2. Data Compilation Service: This service compiles other relevant information such as the automated cross-match reports that include the results of searches against the EAS. The product in this case is the cross-match report(s) that are included in the packages. If needed, an Associated Country could request from the AP Twins a more detailed report on certain cases.

(18) The above business services will be supported with the following specific IT Services[16] and products:

[redacted]

(19) The **main changes** in this context are briefly outlined below:

[16] Details provided in Solution Blueprint #EDOC 1257710

a. Regarding **security** of the process:

[redacted]

b. Regarding **compilation service and other new functionalities**:

The enriched data that Europol can provide to the countries' investigators will not be limited anymore to hits [redacted]

c. Regarding **Automation**:

Parsing of referrals' [redacted] will extract and automatically import into the Europol Data Environment the main entities (suspect, victim, email, telephone, etc.), removing the need for manual extraction and import of these entities. As the next step, these entities will be automatically cross-checked against the Europol Analysis System using the existing mechanisms in order to enrich [redacted] the information in the

referral. [redacted]

3 LEGAL AND TECHNICAL ASSESSMENT

3.1 Need for prior consultation pursuant to Article 90 EUDPR

(20) Under the threshold for prior consultation in Article 90 EUDPR, the EDPS is to be prior consulted by Europol for processing operations 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.

(21) The EDPS notes that Europol did not indicate under which basis the prior consultation is submitted.

(22) As already highlighted in a previous prior consultation Opinion[17], Article 90 EUDPR has a broader scope of application than Article 40 EUDPR and subjects to prior consultation either those 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 cannot be mitigated by reasonable means) (Article 90))1)(a) EUDPR), or those types of processing that, by nature, include a high risk to the rights and freedoms of data subjects (Article 90)(1)(b) EUDPR).

(23) Regarding Article 90)(1)(b) EUDPR, the EDPS notes that it constitutes 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 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

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

processing in and of itself involves high risks and qualifies for prior consultation with the EDPS under Article 90(1)(b) Regulation 2018/1725.

(24) The indicative wording of the provision '*in particular, where using new technologies, mechanisms or procedures*' provides for some relevant factors for this exercise. However, in line with this indicative wording, 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.

(25) In case the outcome of assessing Article 90(1)(b) EUDPR 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 Article 90(1)(a) EUDPR. 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[18] provide indicative criteria that should be taken into account for this threshold assessment.

(26) The EDPS understands that Europol carried out a threshold assessment in order to confirm the necessity of carrying out a DPIA under Article 89 EUDPR and came to the conclusion that the process of automating the processing of data originating from NCMEC for further dissemination to EU MS is likely to result in high risks for the data subjects[19]. The EDPS also understands that on basis of the risks identified in the DPIA, Europol considered that the abovementioned processing operation indeed results in high risks for the data subjects in the absence of mitigation measures and therefore decided to consult the EDPS under Article 90 EUDPR but without specifying if this assessment was based on Article 90(1)(a) or 90(1)(b) EUDPR. The EDPS notes that no explicit assessment of Article 90(1)(b) EUDPR was expressly included by Europol, neither in nor as part of the information accompanying the DPIA that was shared with the EDPS.

(27) The EDPS considers that the envisaged processing operation leads to a processing which will form part of a new filing system as it involves new processes that aim at improving the automation in the processing of data originating from NCMEC for further dissemination to EU MS and third associated countries under the respective country folders. Such processing involves high risk to the rights and freedoms of data subjects as it will entail the automated processing of large volumes of data of a highly sensitive nature, with a significant proportion of reports expected to contain personal data concerning categories of vulnerable data subjects (victims, minors). The EDPS considers therefore that this processing operation falls under the scope of Article 90(1)(b) which makes the prior consultation of the EDPS mandatory.

In view of the above, the EDPS **considers** that the process of automating the processing of data originating from NCMEC for further dissemination to EU MS and third associated countries is subject to prior consultation in accordance with Article 90(1)(b) EUDPR.
The EDPS **recommends** that for future prior consultations based on Article 90 EUDPR, any threshold assessment carried out by Europol should *always* include, as

[18] https://edps.europa.eu/sites/edp/files/publication/19-07-16_edps_dpia_list_en.pdf .

[19] EDOC # 1252943 v4, p. 9.

first step, an explicit assessment of whether 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 (Article 90(1)(b) EUDPR). Only when the outcome of the assessment is negative, should Europol analyse whether the processing at stake falls under Article 90(1)(a) EUDPR.

3.2 Scope of the Opinion

(28) **The Opinion** of the EDPS on this prior consultation **concerns the DPIA included in the prior consultation** request of 3 February 2023 and further clarified in a meeting between the EDPS and Europol on 2 March 2023.

(29) The opinion focuses on the automation of the NCMEC dissemination service as described in the DPIA submitted to the EDPS, constituting the first stage towards an overall new OSP Referral System architecture already prior consulted with the EDPS on its conceptual phase[20]. The new architecture and solution as proposed by Europol aims to improve specific aspects of the current processes and services for the NCMEC data flows. The new architecture improves current services and incorporates new ones that from technical perspective are tools that will automate manual steps and will enhance security features.

(30) The EDPS notes that any subsequent development stages that would entail new risks for the rights and freedoms of data subjects [redacted] are not addressed in this opinion. The EDPS should be consulted on substantial modifications of the processing operations that significantly change the (or add) risks for the data subjects (e.g. development and use of machine learning models).

3.3 Legal basis of the processing

(31) The processing of incoming OSP reports from third countries (including enrichment and distribution) relate primarily to the task laid down in Article 4(1) (y) ER: '*Europol shall perform the following tasks in order to achieve the objectives set out in Article 3: … y) support Member States' actions in addressing the online dissemination of online child sexual abuse material'*. The tasks provided in Article 4(1)(a) and (b) ER '*(a) collect, store, process, analyse and exchange information, including criminal intelligence*; (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;'* can be considered as instrumental for Europol to carry out the task entrusted to them under indent (y).

(32) As regards the purpose of this processing under Article 18 ER, the EDPS considers that as Europol enriches incoming OSP reports[21] from third countries or analyses reports on request of the Member State or on its own initiative, these

[20] EDPS Opinion of 12 March 2020 regarding a new Online Service Provider Referral System, EDPS Case 2019-0850.

[21] [redacted]

activities fall within the primary purpose of 18(2)(c) ER. While Europol does not clearly indicate for which of the purposes provided in Article 18 ER this processing takes place, it appears to the EDPS that the analysis carried out in the context of AP Twins and in particular enriching OSP reports with Europol operational data comes under the heading of 'operational analysis'.

(33) As regards the dissemination of the enriched reports (referrals and cross-match results) to the Member States and third associated countries, the EDPS notes that Europol is required to notify Member States of any information concerning them under Article 22(1) ER. In the new service, the referrals, along with the enriched data will be disseminated to the countries through the LFE on a near real-time basis, [redacted]. This part of the process falls as well under the purpose of Article 18(2)(c) ER.

Given the above, the processing of information, including personal data, in the context of the development and operation of the new NECMEC dissemination service falls within Europol's tasks provided in Article 4. Furthermore the enrichment of incoming OSP reports from third countries or the analyses of reports on request of the Member States or Europol's own initiative falls under the purpose of Article 18(2)(c) as well as the dissemination of the enriched reports (referrals and cross-match results) to the Member States and third associated countries.

3.4 Assessment of the risks to data subjects from the process of automating the processing of data originating from NCMEC for further dissemination to EU MS

3.4.1 Risks identified by Europol

(34) In accordance with Article 90(3) EUDPR, the controller shall provide the European Data Protection Supervisor with the DPIA referred to in Article 89 in order to allow the latter to make an assessment of the compliance of the processing and in particular of the risks for the protection of operational personal data of the data subject and of the related safeguards. Article 89 EUDPR provides that the DPIA shall contain at least

- a general description of the envisaged processing operations;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address those risks;
- safeguards, security measures and mechanisms to ensure the protection of operational personal data and to demonstrate compliance with data protection rules, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

(35) These four elements have been defined by the legislator as prerequisites for the EDPS, as well as for the data controller itself, to be able to assess the compliance of the processing and in particular the risks for the protection of operational personal data of the data subject and of the related safeguards.

(36) The risk assessment table included in Europol's prior consultation form on the automation of the NCMEC dissemination service includes five risks:

1. Incorrect data reported by NCMEC;
2. Incorrect cross-match reports associated with a referral;
3. Unauthorised access by the system administrators;
4. Unauthorised access by LEA members; and
5. Data is disseminated to the wrong Member State.

(37) The EDPS notes that in the risk assessment section of the DPIA Europol identifies and assesses mostly risks (risk 3, 4 and 5) that are inextricably linked to *any* IT system.

(38) The EDPS considers that although Europol identified risks stemming from the potential inaccuracy of the data included in the received reports, they failed to fully assess the risks linked to or amplified by the substantial changes brought to the current process by its automation as well as to identify appropriate mitigation measures for these risks.

(39) The EDPS is thus of the opinion that in case the risks (as described below) are not appropriately assessed and mitigated this could lead to the infringement of Article 29 of the Europol Regulation on the assessment of reliability of information (in particular paragraphs 3, 4 and 5 on the obligations of Europol), as well as of the principle of accuracy laid out in Article 71(1)(d) EUDPR and Article 38(2)(b) of the Europol Regulation.

3.4.2 Assessment of risk 1 in Europol's risk assessment table: the risks of incorrect data reported by NCMEC

Origin of the risk to the data subject

(40) Europol has listed five areas of risk in its risk assessment table. In its internal ranking, it has emphasised the further processing of inaccurate reports by NCMEC and/or incorrect matches made by Europol's systems on the data as the largest risks related to the proposed automation of the NCMEC referral process. The EDPS agrees with Europol that these scenarios represent extremely grave risks to the data subject, as being incorrectly marked as a distributor or owner of child sexual abuse material in a law enforcement database (Europol's Analysis System, and then further disseminated to Member States competent authorities, with the associated potential for such data to be used for purposes of operational analysis, development of intelligence products and pursuit of criminal investigations) can have severe consequences for that individual, including potentially irreparable damage to private and professional relationships.

(41) The EDPS notes that these possible negative effects to the data subject stem from the uncertain nature of the underlying OSP reports themselves. Some risk level is always 'inherent' to any processing of OSP reports, including the current manual treatment. This is also clearly acknowledged by Europol in the risk assessment

exercise, '*they contain information from NCMEC for which Europol cannot assess reliability and thus the information should be used with precaution'*[22].

(42) [redacted] The EDPS therefore considers that the automation that is at the heart of the current prior consultation amplifies existing risks by enabling ever higher volumes of referrals to be processed ([redacted] disseminated to Member States) and by removing [redacted] manual intervention in the process which may, under the existing system, have allowed for inaccurate reports to be identified upon extraction.[24]

How this risk can materialise at Europol

(43) In light of the potential inaccuracy of reports, Europol has clearly identified the responsibility that Member States need to take when they receive the 'end products' from Europol. As a mitigation measure for this risk, it proposes to include [redacted] to keep them alerted to this possibility.

(44) However, these reports are also further processed as operational analysis contributions under Article 18(2)(c) of the Europol Regulation. In these situations, Europol itself is also faced by the risks that these potential inaccurate reports bring. Indeed, it appears to the EDPS from the documentation provided, that ingested entities and (at least non-media) files will be [redacted] for further future analytical work under Article 18(2)(c) of the Europol Regulation. This conclusion stems directly from the DPIA[25], where Europol provides that '*the textual part of the NCMEC referrals are available* [redacted] from the solution blueprint. [redacted]

(45) This can be seen as the first 'area' where Europol did not appropriately assess the risks linked to or amplified by the substantial changes brought to the processing

---

22 EDOC# 1252943v6, p. 28.

23 Something referenced by NCMEC for 'sextortion cases': '*In many cases, the blackmailers may have stolen or taken images of another person and they are communicating through a fake account'* (see: https://www.missingkids.org/theissues/sextortion)*'*.

24 The EDPS notes that the previous prior consultation of an OSP referral system solution foresaw manual checking as part of the intake process '*to ensure data quality and fulfil Europol's obligation in the ER in relation to review of Third Party data*'. See Notification to the EDPS regarding new type of processing operation 'Online Service Providers (OSP) Referral System' EDOC#1061855v4, p. 8.

25 EDOC-#1252943-v6, p. 17, answer to Q7-4.

26 EDOC -#1257710-v5A-NCMEC Data Flows - Solution Blueprint, p. 12.

27 [redacted]

28 [redacted].

of NCMEC reports, namely: the further processing in the EAS of potentially inaccurate information as part of Europol's normal, internal operation.

(46) Europol does not propose any specific mitigation measure to address the risk of inaccurate data stemming from NCMEC reports being ingested into Europol's data environment, beyond [redacted] Europol does state in its DPIA, in reference to the intended processing operation, that '*in the future, improvements concerning data quality and standardisation as well as further improvements to the cross-matching reports may be added*'.

(47) The EDPS recalls that Article 29 ER obliges the data provider or Europol where the data provider has not done so, to assess the reliability and accuracy of the information provided by applying source and information evaluation codes. Europol does not however provide any information on how they will comply with this obligation in that context.

(48) The EDPS notes that while no information has been provided by Europol to the EDPS concerning the source reliability/accuracy code assigned to NCMEC data under the 4X4 evaluation system, Europol could consider setting a standardised code to be applied to all NCMEC data indicating a low level of reliability (i.e. 'X' indicating that the reliability of the source cannot be assessed and '4' indicating information not known personally to the source and which cannot be corroborated). These codes could be applied by default to NCMEC data unless and until feedback from Member States or operational analysis by analysts in AP Twins can indicate otherwise.

> In light of the above, the EDPS **deems necessary** that Europol consider which **additional mitigation measures** would be necessary to indicate the mixed reliability of reports, already during the intake and ingestion process, to control for the risk of inaccurate data being automatically extracted and imported into Europol's data environment. For example, by marking the data derived from NCMEC reports in a manner that would reflect the unreliable or unverified nature of that information ([redacted] via a specific flagging or labelling functionality or by relying on an appropriate attribution of source and evaluation codes in accordance with Article 29 ER.

Appraising this risk in light of current and future developments in how Europol data is accessed

(49) Since the last NCMEC-related prior consultation that was submitted by Europol in 2019, a number of developments have taken place that increase the accessibility of data held in Europol's systems to authorities external to Europol. One such development is the planned entry into operation [redacted]

[29] EDOC # 1252943 v4, p. 21.

[redacted] Europol has specified (in response to additional clarifications requested by the EDPS), that [redacted] will not allow for searching NCMEC data. The EDPS is reassured to note the application of this restriction in view of the risks of making unverified and potentially unreliable personal data provided through NCMEC referrals searchable via [redacted] and considers it important that such a safeguard be maintained.

Evaluating the risk and finding appropriate risk treatment options

(50) The EDPS reiterates that these risks stem from the nature of OSP reports. The manual intervention of the analyst at different steps of the processing, including during the intake process, served at least as a partial mitigation measure. The now full automation of the processing operation, coupled with the changing processing landscape for Europol, and the increasing volumes of NCMEC referrals expected[30] amplifies those risks and call for different mitigation measures.

The EDPS therefore **deems necessary** that Europol undertake the following (if it has not done so already):

- to scope the risk of stolen/inaccurate identifiers and mis-categorisation of information as child sexual abuse material. As the severity of the risk to the data subject in the view of the EDPS would likely be maximal, given the extreme impact on their personal life that this may generate, the main area of investigation would then be the frequency of this risk occurring.

- to assess whether further mitigating measures, such as those proposed above, can and should be put in place.

Importance of feedback from the Member States

(51) The EDPS considers, that there is an absolutely vital role to be played in the feedback mechanism from Member States and third associated countries to Europol, to both purge reports that are proven to be inaccurate or false, so that they are no longer stored in the EAS, but also to be able to continuously update its own estimation of how frequently inaccurate or false reports are processed (which as mentioned above affects the risk level of all related processing operations).[31]

In view of the above, the EDPS **deems necessary** that Europol consider and propose **technical solutions** that allow for quicker, more frequent and more efficient

[30] EDOC # 1252943 v4, p. 10.

[31] This was the EDPS position in the previous prior consultation of an OSP referral system solution. [redacted]

feedback from the Member States.

3.4.3 Assessment of risk 2 in Europol's risk assessment table: the risk of incorrect cross-match reports associated with a referral

(52) Europol identifies as a second risk area that the automated extraction, ingestion and cross-matching of files ([redacted]) could result in incorrect cross-match reports that may wrongfully link a data subject to a criminal investigation. Europol assesses the residual likelihood of such a risk materialising as very low (rating of 1). The EDPS notes that the tools that will be used for automatic extraction and ingestion will need to be tested thoroughly before their use and Europol should continuously monitor their performance and trace potential errors.

(53) However, the EDPS notes the removal in the proposed processing of the [redacted] The EDPS also underlines that, regardless of the low likelihood, the impact of an erroneous cross-match on a data subject, should it materialise, would be severe, with grave consequences for an individual's rights and freedoms, including significant and irreparable reputational damage as this could lead to an individual being erroneously linked to a crime (child sexual exploitation) of a particularly serious nature.

(54) In light of the severity of this risk, the EDPS finds that the mitigation measure proposed by Europol as a control for this risk may be insufficient. [redacted]

(55) However, such a measure places the burden of responsibility solely on the Member States to exercise sufficient precaution vis-a-vis the material provided. [redacted]

(56) Europol should consider whether other types of organisational or technical safeguards could be integrated into the proposed processing operation workflow, in order to more effectively mitigate such a risk.

In view of the above, the EDPS considers that Europol has not considered all the types of organisation or technical safeguards that could more effectively mitigate the risk that the automated extraction, ingestion and cross-matching of files could result in incorrect cross-match reports that may wrongfully link a data subject to a criminal investigation.
The EDPS thus **deems necessary** that Europol further assess other mitigation measures, examples of which could include:

a. Detailed acceptance tests of the extraction and ingestion tools to eliminate potential errors and monitoring of their performance with monthly reports.

b. Manual spot checks of the system conducted at intervals, overseen by the Data Quality Control Coordinator, to control for inaccurate cross-match reports;

c. An automated system flag could be developed to alert Europol analysts in case of anomalies, e.g. sudden spikes or disproportionate rates of cross-matches;

d. The above-described under point 3.4.2. feedback mechanism allowing Member States to report errors in the information provided by Europol, could not only serve as an important mitigation measure for Risk 1 but also enable Member States to flag to Europol any inaccuracies in cross-match reports and thereby alert Europol to any potential technical issues affecting the components enabling automation.

4 CONCLUSION

(57) As indicated above, in order to ensure compliance of the processing with Article 29 of the Europol Regulation as well as with Article 71(1)(d) EUDPR and Article 38(2)(b) of the Europol Regulation, the EDPS **deems necessary** that Europol:

1. Regarding the risks stemming from potentially inaccurate OSP reports,:

   a. Consider which **additional mitigation measures** would be necessary to indicate the mixed reliability of reports, already during the intake and ingestion process, to control for the risk of inaccurate data being automatically extracted and imported into Europol's data environment. For example, by marking the data derived from NCMEC reports in a manner that would reflect the unreliable or unverified nature of that information [redacted] via a **specific flagging or labelling** functionality or by relying on an **appropriate attribution of source and evaluation codes** in accordance with Article 29 ER.

   b. Undertake (if it has not done so already), to **scope the risk** of stolen/inaccurate identifiers and mis-categorisation of information as child sexual abuse material. As the severity of the risk to the data subject in the view of the EDPS would likely be maximal, given the extreme impact on their personal life that this may generate, the main area of investigation would then be the frequency of this risk occurring.

   c. Consider and propose **technical solutions** that allow for quicker, more frequent and more efficient **feedback** from the Member States,

2. Assess further **mitigation measures** regarding the **risk** that the automated extraction, ingestion and cross-matching of files could result in **incorrect cross-match reports** that may wrongfully link a data subject to a criminal investigation, examples of which could include:

   a. Detailed acceptance tests of the extraction and ingestion tools to eliminate potential errors and monitoring of their performance with monthly reports.

b. Manual spot checks of the system conducted at intervals, overseen by the Data Quality Control Coordinator, to control for inaccurate cross-match reports;

c. An automated system flag that could be developed to alert Europol analysts in case of anomalies, e.g. sudden spikes or disproportionate rates of cross-matches;

d. The feedback mechanism (mentioned under §57(1)(c) of this Opinion) allowing Member States to report errors in the information provided by Europol.

The EDPS expects Europol **to implement** the above actions accordingly and to **provide documentary evidence** of this implementation before the processing operation under prior consultation becomes operational.

(58) Moreover, the EDPS **recommends** that for future prior consultations by Europol based on Article 90 EUDPR, any threshold assessment carried out by Europol should always include, as first step, an explicit assessment of whether 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 (Article 90(1)(b) EUDPR). Only when the assessment is negative should Europol analyse whether the processing at stake falls under Article 90(1)(a) EUDPR.

In light of the accountability principle laid down in Article 71(4) EUDPR, the EDPS has decided to **close the prior consultation case**.

Done at Brussels on 20 April 2023

[e-signed]

Wojciech Rafał WIEWIÓROWSKI