EDPS OPINION ON EUROPOL'S PROCEDURE TO HANDLE DATA SUBJECT ACCESS REQUESTS (Case 2019-0570)

1. INTRODUCTION

- This Opinion relates to Europol's handling of data subject access requests under Article 36 & 37 of Regulation (EU) 2016/794[1] ('the Europol Regulation', or 'ER' abbreviated).

- The EDPS was consulted by Europol's Data Protection Function ('DPF') on 15 May 2019. As the consultation partially covers the inquiry on Computer Forensic Network ('CFN'), the case was suspended until the EDPS rendered its Decision in case 2019-0370, which it did on 17 September 2020.

- The EDPS issues the present Opinion in accordance with Article 43(2)(d) ER.

2. BACKGROUND

Under Article 36 ER, any data subject may ask Europol whether the organisation processes any personal data relating to him or her. Since the entry into force of the Europol Regulation, data subjects have made frequent use of this possibility. In fact, the amount of data subject access requests ('DSARs') spiked in 2020, based on preliminary reporting from Europol's DPF.[2] At the same time, Europol is processing growing amounts of personal data, in various formats, across its databases.[3] It is against this background that the DPF has consulted the EDPS on the practical implementation of the right of access at Europol going forward.

---

1 *Regulation 2016/794 of the European Parliament and 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, 24.05.2016.*

2 *This preliminary reported number follows a decrease of reports between 2018 and 2019. However since 2017 the amount of DSARs has never dropped below 300, see EDOC#1060458v5.*

3 *Further detailed in the aforementioned EDPS case 2019-0370.*

[redacted]

Europol further consulted the EDPS on how to handle search results that cannot be attributed to the data subject with full certainty (so-called 'partial hits'). Europol provided the example where a search on the name of a data subject returns a 'hit', however there is no '*additional information available to enable an exact match of the requester and the person in Europol's system*'. Such additional information would be for example the date of birth.

In order to assist Europol in implementing the right of access in an efficient and effective way, this Opinion includes guidance on:

1. Situations where data cannot be conclusively matched to the person requesting access ('the requester');
2. The scope of the searches to be conducted in Europol's various systems, which, the EDPS already notes, principally excludes external databases such as SIS II.

3. LEGAL ANALYSIS AND RECOMMENDATIONS

The right of access to one's own personal data is a cornerstone of the right to data protection. It is explicitly granted by Article 8 (2) of the European Charter of Fundamental Rights (the 'Charter') and enables data subjects to check both whether their personal data are correct and whether they are being lawfully processed. Through the right of access, data subjects can also monitor whether central data protection principles such as data minimisation, purpose limitation and storage limitation are being complied with. Finally, the right of access acts as a precondition for the exercise of other rights, such as the rights of rectification, erasure and restriction, as reflected in Article 37 and Recital 46 of the Europol Regulation.[5]

Considering the above, Europol should in principle not refuse requests for access or otherwise restrict the information to be provided under Article 36(2) ER. In certain circumstances, Article 36(6) of the Europol Regulation allows for some or all of the

[4] *Europol letter to the EDPS of 15 May 2019 requesting consultation on 'Data Subject Access Requests Article 37 and 37 Europol Regulation', ref. 1038265-19.*

[5] *See also CJEU, C-553/07, Rotterdam v. Rijkeboer: §51.*

information to be withheld from the data subject. However, this possibility must be carefully applied by Europol, and be based on a detailed, case-specific assessment and clear justification. In order to safeguard the rights of the data subject it should never become a baseline scenario.

Aside from this explicit exception in Article 36(6) ER, the EDPS acknowledges that the right of access can be restricted in scenarios where the access request would be manifestly unfounded or excessive, for instance because of its very repetitive nature. Article 36(1) ER mentions that data subject access requests should be posed 'at reasonable intervals' and recital 40 of the Law Enforcement Directive further clarifies that a request could be considered as excessive or manifestly unfounded where "*the data subject unreasonably and repetitiously requests information or where the data subject abuses his or her right to receive information, for example, by providing false or misleading information when making the request.*" [6]

The EDPS considers that Europol, as any other controller, should not be compelled to respond to manifestly unfounded or excessive requests. However, the burden of proof remains with Europol as regards the excessive or manifestly unfounded nature of the requests. A similar provision to Article 14(5), second sentence of the EUDPR can be found in Article 14(3) of the European Code of Good Administrative Behaviour: "*No acknowledgement of receipt and no reply need be sent in cases where letters or complaints are abusive because of their excessive number or because of their repetitive or pointless character.*" Insofar, the European Ombudsman has highlighted that "*any decision reaching the conclusion that correspondence sent by a citizen is improper, for example, because it is repetitive, abusive and/or pointless, must be based on an individual and substantive assessment of a citizen's correspondence*".[7] In the case of Europol, Article 36(7) ER also requires Europol to include these grounds for refusal in its response to the data subject.

The EDPS has provided additional guidance on the interpretation of 'reasonable intervals' and the assessment of unreasonably repetitious requests under Article 36(1) ER in its Opinion of 13 July 2021 (case 2021-0364.)

[6] *Directive (EU) 2016/680 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.*

[7] *European Ombudsman, The European Code of Good Administrative Behaviour, 2002: https://www.ombudsman.europa.eu/en/publication/en/3510#/page/5.*

3.1. Regarding the conclusive matching of Europol data to the requester

The EDPS acknowledges that personal data processed at Europol is subject to certain specificities. As it supports criminal investigations, data held by Europol can be incomplete or may not be conclusively linkable to the data subject. Indeed, identities are frequently uncovered gradually throughout the investigative process, which has a practical impact on the right of access as well.

The EDPS emphasises that the correct identification of the data subject is paramount, not only to provide requesting data subjects with an accurate response to their DSAR, but also to avoid interference into the rights and freedoms of others. Under the Law Enforcement Directive[8] and the EUDPR[9], the protection from interference into other data subjects' rights and freedoms has been explicitly included into the text of the articles on the right of access. While the Europol Regulation does not contain a similar provision, it should be recalled that the principle has been recognised by the Charter in Article 52 (1) as a general ground for the limitation of the right to data protection. Such limitation has been applied in several cases by the CJEU.[10]

Because of the volume of data subjects in Europol's systems, occasionally search results may turn up following a data subject access request that seemingly match the requester, while actually belonging to someone else. For example, when dealing with a DSAR from 'John Smith', Europol may find that a 'John Smith' indeed exists within its systems, however given how common this combination of first name and surname is, a match (or 'hit') does not necessarily mean that the data can be conclusively attributed to the requester.

In cases of doubt, Europol must make reasonable efforts to clarify whether the personal data belong to the requester. In this respect, the EDPS recognises that Europol has developed a robust procedure in the past, which includes cooperating with the contributing entity to verify the potential match. **However, Europol should apply the principle of data minimisation and not gather further information from the requester on its own initiative either by using OSINT** (publicly available information),

---

[8] *Article 13(3)(e) of Directive (EU) 2016/680 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, OJ L 119, 4.5.2016, p. 89–131.*

[9] *Article 17(4) of Regulation (EU) 2018/1725 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, OJ L 295, 21.11.2018, p. 39–98.*

[10] *See for example joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, para. 50: "Moreover, Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others."*

or by requesting additional identifiers from the data subject - other than those present on standard identity documents.

In this sense, the EDPS points to Article 11 of the GDPR and Article 12 of the EUPR which state that "*If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.*" As further specified by Recital 52 of the GDPR and (Recital 32 of the EUDPR), "*If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights.*"

The EDPS further reminds that, based on the principle of purpose limitation, the personal data thus obtained can only be used to verify the requestor's identity; they cannot be processed for any other purpose, for example purposes of operational analysis. The retention period for the copy of an identification document should be limited to the period required to establish the identity of the requestor, including for cases of doubt.

Where Europol is not able to determine with certainty that the personal data in its systems match the requester, the EDPS supports Europol's current approach: that it should not provide this data to the requester. Incorrect identifications should be strongly avoided as they can have a deep impact on the requester, as well as the person whose personal data is wrongly disclosed. Among others, the requesters may incorrectly believe that they are being investigated by law enforcement, leading to distress and causing a chilling effect on their future actions.

3.2. Regarding the systems, databases and datasets to be searched in response to the access request

The EDPS notes that Europol processes personal data in a wide variety of formats, for instance on a seized device being forensically extracted at Europol or as part of long lists of personal data provided by law enforcement partners. These circumstances can make performing the checks particularly difficult and burdensome for Europol as a controller.

[redacted]

[redacted]

The EDPS emphasises that **the right of access does not differentiate between any databases or systems for its scope. In principle, all personal data processed at Europol, regardless of where and how it is stored, can be subject to a DSAR under Article 36 ER**.[11]

[redacted]

The Europol Regulation places a high expectation on Europol to provide information in response to a DSAR, therefore **no (parts) of Europol's systems should be *a priori* excluded from the search. However**, the EDPS has upheld in various guidance documents that **the burden of the task for the controller has to be kept in mind** when responding to access requests.[13] As indicated previously, it is up to Europol to make reasonable efforts to retrieve and assess the requested information. In principle, data subjects should have access to all the information regarding them that Europol itself can retrieve.

Considering that Europol processes data from a range of data sources, including raw data from seized evidence, the EDPS understands that this can take substantial time and effort when retrieving all personal data that could match the individual, and in some cases none can be attributed clearly.

Nevertheless, the lack of sufficient infrastructure to perform searches when responding to a DSAR is in and of itself not sufficient as a justification to forego searches in such systems of any kind. In line with Article 33 ER on data protection by design, the data controller is under

---

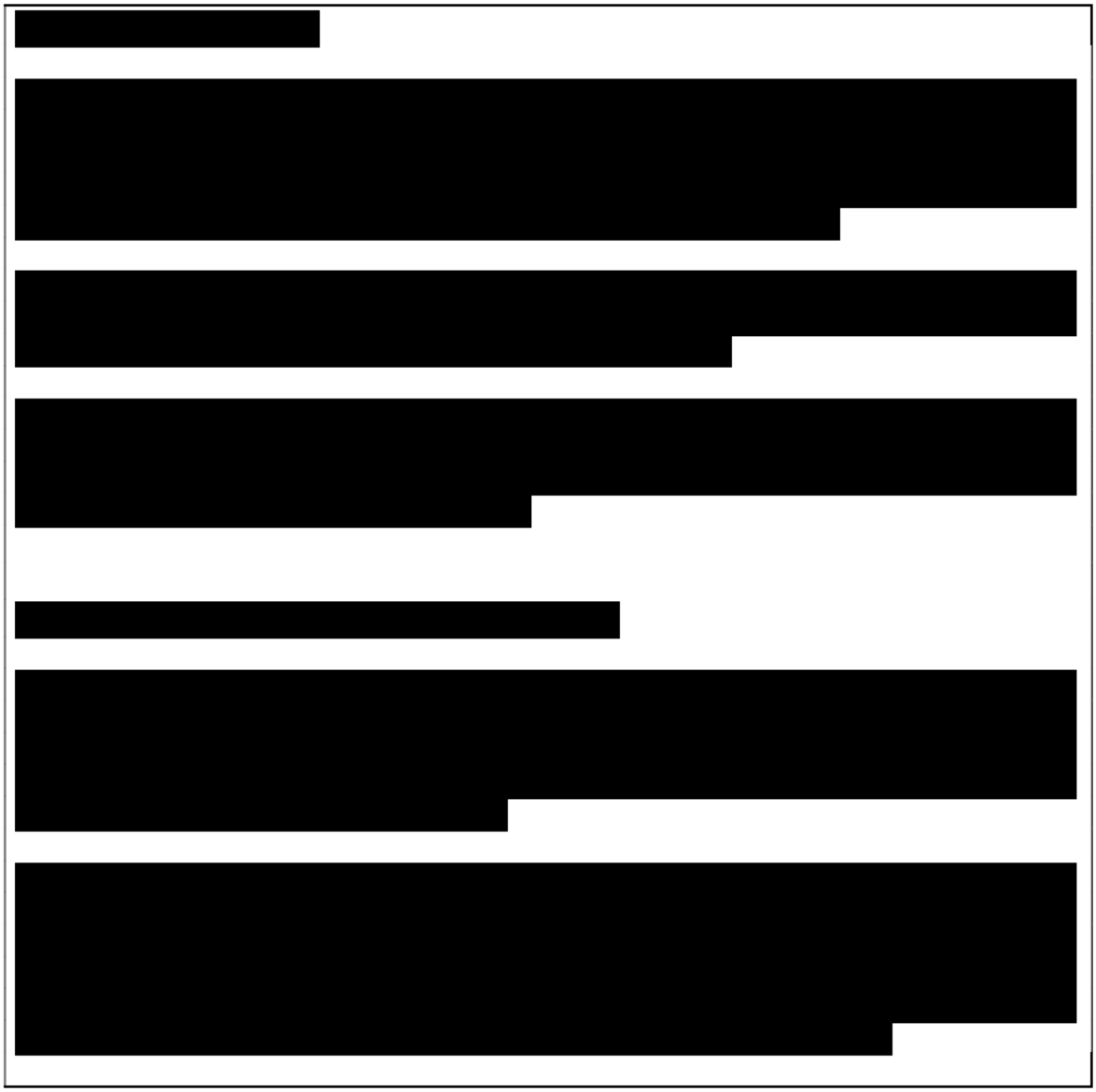
[11] *This concerns operational systems, as access to administrative data is dealt with under Regulation (EU) 2018/1725.*

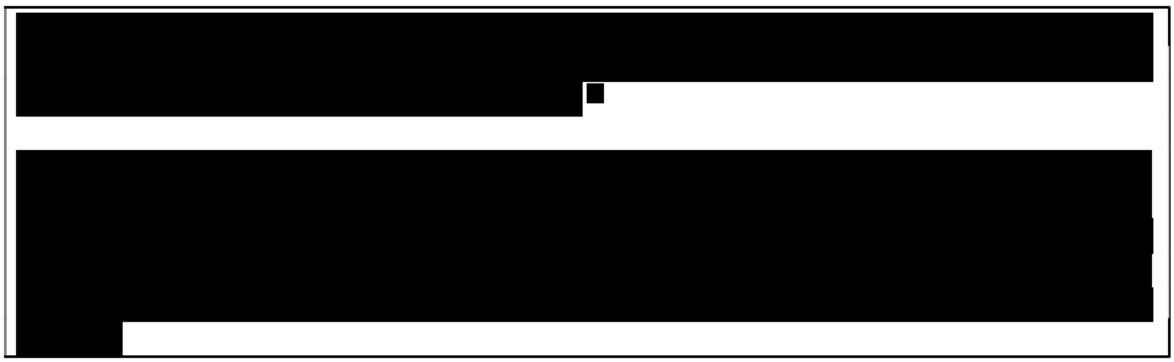
[12] [redacted]

[13] *See page 17 of the "EDPS Guidelines on the Rights of Individuals with regard to the Processing of Personal Data", available at https://edps.europa.eu/sites/edp/files/publication/14-02-25_gl_ds_rights_en.pdf, as well as pages 9-10 of the "EDPS Guidance Paper on Articles 14-16 of the new Regulation 45/2001", available at https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en.pdf.*

an obligation to implement functions enabling the compliance with data subject rights. This means, in this context, that there should be appropriate ways to find and retrieve information regarding a data subject when handling a request for access.

Europol should therefore examine **whether any changes to the tools, structure or policies of the system could be made in order to allow (future) searches in a less burdensome manner**.





3.3. Specific point regarding queries of the Schengen Information System (SIS II)

Europol also asked whether it should conduct searches in SIS II following an access request. **On this point, the EDPS reminds that only Europol's own systems are governed by the right of access as laid down in Article 36 & 37 ER.** SIS II on the other hand is subject to its own specific legal framework[15]. Where a data subject wants to exercise their right of access *vis-a-vis* SIS II, they should therefore go through the regime designated in the SIS II framework, namely via the consulate, the national data protection authorities or the national competent authorities for this system.

Europol could however still perform its own procedural check in SIS II whenever a full hit in Europol's systems indicates that a European Arrest Warrant (EAW) was issued. The aim of the check would then not to grant access to SIS II data to the data subject, but to confirm the status of the EAS in order to assess whether the access must be refused on one of the grounds listed under Article 36(6) ER. A valid EAW could be taken into account for a potential refusal or restriction of the request under Article 36(6)(c) ER, 'to guarantee that any national investigation will not be jeopardised'. Considering that the measure would only serve to verify the accuracy of the alleged EAW already indicated in Europol's system, such a limited check would be compatible with the applicable legal framework. This check should only be conducted by staff qualified and trained to search the SIS.

---

[14] The obligation relates primarily to sanitised data files as opposed to encrypted or untreated data files stored in the CFN as the EDPS understands it would not be technically possible run searches on the latter, as doing so would present a high risk to the security of Europol's systems.

[15] Recently expanded by means of Regulation (EU) 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals; Regulation (EU) 2018/1861 on the establishment, operation and use of the SIS in the field of border checks; and Regulation (EU) 2018/1862 on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

4. CONCLUSIONS

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

As regards 'partial hits', Europol must make reasonable efforts to clarify whether the personal data belong to the requester. The EDPS is satisfied with the current procedure implemented at Europol, whereby Europol contacts the contributing entity in order to attempt to resolve these hits. In addition, the EDPS asks Europol:

- to use only information obtained from the data subject in order to handle data subject requests, and not to further request personal data from the data subject beyond those present on standard identity documents or use OSINT to supplement this information.
- to only provide information on Europol data that can be attributed to the requester with a high degree of certainty.

As regards the systems to be checked as part of the scope of the right of access, the EDPS reiterates that no (part of) Europol's systems should be *a priori* excluded from the search. The EDPS takes into account that systems [redacted], due to the format of files, or unstructured nature of the data concerned, may be particularly complicated or burdensome to search. In this regard, the EDPS asks Europol to:

- Implement all necessary and appropriate technical measures to facilitate the efficient search and retrieval of data subjects in response to a DSAR in forensically extracted datasets [redacted].
- Take into careful consideration the requirements associated with DSARs as part of the ongoing project to develop the architecture and governance of NEO and integrate in new systems the appropriate functionalities to ensure compliance with Articles 36 and 37 ER.

Done at Brussels on 13 December 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI