EUROPEAN DATA PROTECTION SUPERVISOR

Decision of the European Data Protection Supervisor in complaint case 2020-0908 against the European Union Agency for Law Enforcement Cooperation (Europol)

The EDPS,

Having regard to Article 16 TFEU, Article 8 of the Charter of Fundamental Rights of the EU, and Regulation (EU) 2016/794,

Has issued the following decision:

1. Proceedings

1.1. On 6 October 2020, the EDPS received a complaint under Article 47 of Regulation (EU) 2016/794 (the Europol Regulation)[1] against the European Union Agency for Law Enforcement Cooperation (Europol) concerning a request for access of personal data under Article 36(1) of the Europol Regulation. The complaint was registered under case 2020-0908.

1.2. Following receipt of the complaint the EDPS started investigating it, pursuant to Article 43(2)(b) of the Europol Regulation.

1.3. On 20 October 2020 the EDPS sent a written request to Europol, asking for comments on the complaint, including confirmation as to whether processing by Europol of personal data relating to the complainant had taken place and detailed reasons why access was denied.

1.4. On 11 November 2020, the EDPS received a written reply from Europol's Data Protection Function (DPF), confirming that it had been processing personal data on

[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, pp. 53-114.

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

the complainant at the time of receipt of the data subject access request and stating that it had subsequently deleted the personal data concerned. Europol also identified the Netherlands as the contributor of the personal data on the complainant and provided reasons for its decision to refuse access.

1.5. On 23 November 2020 the EDPS sent a request for clarification regarding the timing of Europol's decision to delete the data on the complainant and asked for a screenshot to attest that personal data on the complainant was no longer being processed in Europol's systems.

1.6. On 26 November 2020 Europol provided two print screens from Palantir and iBase as evidence that no personal data on the complainant was processed at the current time by Europol. It also clarified that the decision to delete the complainant's data was taken after receipt of the data subject access request and after having consulted the Netherlands, and before sending its decision to the complainant.

1.7. On 12 January 2021 the EDPS sent a request for cooperation to the Dutch Data Protection Authority (hereafter the Dutch SA), in accordance with Article 44(4) of the Europol Regulation. The EDPS asked the Dutch SA to inform as to (i) whether the data processed on the complainant was lawfully transmitted to Europol and (ii) whether it considered that access to the complainant's personal data as processed by Europol could be granted or whether access should be refused or restricted based on the exemptions foreseen in Article 36 of the Europol Regulation.

1.8. On 12 January 2021 the EDPS also sent a written request to Europol to further substantiate its reasons for refusal of access. In addition, the EDPS, noting the technical possibilities available to Europol for retrieving deleted data, requested to receive a copy of the complainant's personal data processed at the time of receipt of his data subject access request.

1.9. On 17 March 2021, Europol provided a reply to the EDPS' questions. In response to the EDPS request for a copy of the personal data concerned, Europol invited the EDPS to verify any operational information linked to the case at Europol's headquarters.

1.10. On 15 April 2021, the EDPS requested a copy of Europol's internal assessment documenting the applicability and justification for applying an exemption under Article 36(6)(a) on which the decision to refuse access was based. In addition, the EDPS reiterated its request for a copy of the personal data relating to the complainant to be transmitted to the EDPS via a secure channel.

1.11. On 16 April 2021 the EDPS received the reply of the Dutch SA which provided the findings of its consultations with the Dutch competent authority, and its conclusions

on disclosure to the complainant.[2] On 21 April 2021, the EDPS forwarded a copy of the reply of the Dutch SA to Europol, accompanied by additional questions to Europol in light of the information provided by the Dutch SA (including discrepancies between information provided by the Dutch SA and information provided by Europol).

1.12. On 11 May 2021, Europol provided the EDPS with a copy of its internal assessment (EDOC#1114580v1).[3] It also informed the EDPS of its decision not to transmit the requested personal data to the EDPS[4] and reiterated its invitation to verify the personal data at Europol headquarters (should the absence of quarantine requirements for travel between the Netherlands and Belgium allow.)

1.13. On 26 May 2021, the EDPS sent Europol a set of additional requests for clarification based on the information provided in the internal assessment (EDOC#1114580v1) and proposed to schedule an on-site verification of the operational personal data concerned.

1.14. On 26 May 2021, the EDPS forwarded to the Dutch SA the internal assessment (EDOC#1114580v1) and requested the Dutch SA, in the framework of the initial EDPS request for cooperation, to complete its checks on the personal data processed on the complainant. On 3 June 2021, Europol provided additional information to the EDPS which the EDPS forwarded to the Dutch SA on 10 June 2021.

1.15. On 22 June 2021 two Europol staff members visited the EDPS in order to provide access to the requested documents on a secure Europol laptop.[5] During Europol's visit, the EDPS viewed the operational personal data concerning the complainant (SIENA messages and a personal file on the complainant) and correspondence between the DPF, Europol operational units, Liaison Bureau Netherlands (LB NL) and the Dutch Police. The email correspondence was consulted on screen during a secure videoconference call with Europol's DPF during the visit. Minutes of the visit were taken by the EDPS during the visit, finalised and sent to Europol for review and signature .[6]

---

[2] Letter of the Dutch SA of 16 April 2021, "Request for cooperation - Consultation on a complaint against Europol (EDPS Case No 2020-0908)" ref. z2021- 01483.
[3] EDOC#1114580v1 (Europol Briefing note of 4 June 2020, 'Data subject access request - full hit Mr Frank van der Linde').
[4] Europol cited the "absence of an accredited system to process operational personal data in a secure manner owned by the EDPS."
[5] Restrictions linked to the COVID-19 pandemic prevented EDPS travel and access to Europol premises in June 2021.
[6] Minutes of the Visit of Europol to EDPS premises of 22 June 2021 in order to provide access to the documents requested in the context of the investigation of the complaint (2020-0908).

1.16. On 14 September 2021, the EDPS received a letter from the Dutch SA,[7] informing that it had consulted the competent privacy officer of the Netherlands Police's Central Unit and duly assessed all available information, including the additional information provided by Europol, via the EDPS. The Dutch SA provided a new opinion and set of conclusions, deviating from its initial Opinion provided on 16 April 2021.

1.17. On 20 September 2021, the EDPS forwarded the revised Opinion of the Dutch SA to Europol and issued a written request to review, in light of the information contained in that new Opinion, Europol's original decision to refuse access to the complainant to his personal data. The EDPS requested that Europol share its reassessment by 11 October 2021. The EDPS granted an extension of this deadline to 5 November 2021 upon Europol's request. Upon expiry of this deadline, the EDPS sent Europol a series of written reminders on 12 November 2021, 17 January 2022 and 31 January 2022. In response, Europol informed it was waiting for the response of the Dutch police as regards its position on disclosing information to the complainant.

1.18. On 3 February 2022 the complainant informed the EDPS that his lawyer would provide the EDPS with further legal substantiation of his complaint.

1.19. On 11 February 2022, Europol provided the EDPS with the result of its reassessment, together with a proposal for a reply to the complainant.

1.20. On 28 February 2022 the complainant contacted the EDPS to reiterate that his lawyer would provide further information and to indicate that the EDPS should not to issue a Decision on the complaint until it had received and taken into account this additional information. The complainant also submitted a series of questions to the EDPS pertaining to the EDPS' complaints handling procedures, to transparency and the right to be heard of the complainant, and to the mechanisms of redress available to him following the issuance of a decision.

1.21. On 22 March 2022 the EDPS sent a set of replies to the complainant's questions.

1.22. On 7 May 2022 the complainant provided the EDPS with further legal substantiation of his complaint. In addition, he reiterated his request to receive and respond to the position of Europol before the EDPS issues a decision on his complaint. The EDPS responded on 20 May 2022, restating its procedures with regard to the investigation of complaints against Europol that concern refusals of access (and the confidentiality requirements imposed on the EDPS by Article 36(6)).

[7] Letter of the Dutch SA of 14 September 2021, "Request for cooperation - Consultation on a complaint against Europol (EDPS Case No 2020-0908)" ref. z2021- 01483.

2. Facts

2.1. On 29 May 2018, the Netherlands Police Amsterdam Counter-Terrorism Unit (CTER) sent a SIENA message (SIENA 1346846-1-1) to the Federal Criminal Police Office of Germany (BKA), with Europol in copy. The SIENA message informed the German Police that Frank van der Linde (the complainant), a Dutch left-wing activist, would be travelling to Berlin to receive medical treatment, and warned that though the individual had no previous criminal record for violence, he might undertake some form of action against authorities during his stay in Germany. The SIENA message included a personal file on the complainant as an attachment. The personal file contained information on the involvement of the complainant in various social media platforms, protests and initiatives against racism and discrimination.[8]

2.2. On 15 April 2019 the Netherlands sent a cancellation of the SIENA message to Germany but, due to a mistake of the Netherlands SIENA operator, did not cancel the message to Europol.[9]

2.3. On 23 October 2019, following a data subject access request submitted to the Regional Police Unit of Amsterdam, the complainant was provided access to a copy of the SIENA message 1346846-1-1 and personal file sent by the Dutch police on 29 May 2018, with the exception of the handling officer's name.[10]

2.4. On 7 February 2020, in the context of an on-going investigation, the Netherlands provided Europol with a mobile phone [redacted] to obtain Europol's support in extracting data from the device. The information subsequently extracted from the device and stored by Europol included personal data from [redacted] Twitter [redacted] consequently the complainant's Twitter account was stored in a data file in Europol's Analysis System (EAS).[11]

[8] EDOC#1114580v1 (Europol Briefing note of 4 June 2020, 'Data subject access request - full hit Mr Frank van der Linde'); see also Minutes of the Visit of Europol to EDPS premises of 22 June 2021 in order to provide access to the documents requested in the context of the investigation of the complaint (2020-0908).
[9] Email from Europol to the EDPS of 3 June 2021.
[10] Letter of the Dutch SA of 14 September 2021, "Request for cooperation - Consultation on a complaint against Europol (EDPS Case No 2020-0908)" ref. z2021- 01483.
[11] EDOC#1114580v1 (Europol Briefing note of 4 June 2020, 'Data subject access request - full hit Mr Frank van der Linde'). See also Minutes of the Visit of Europol to EDPS premises of 22 June 2021 in order to provide access to the documents requested in the context of the investigation of the complaint (2020-0908).

2.5. On 10 March 2020 Europol received a data subject access request from the complainant via the Dutch Police and confirmed its receipt. Checks performed by the DPF in Europol's systems the same day revealed a "full hit" on the complainant in AP Dolphin[12] with a person implication of suspect.

2.6. On 11 March 2020, Europol's DPF sent a request to Liaison Bureau Netherlands asking whether the Netherlands competent authority would agree to the release of information to the complainant. In the absence of a reply, the DPF followed up with subsequent reminders. Having still received no response, on 25 May 2020, the DPF initiated a videoconference call with Europol operational staff from Analysis Project Dolphin ('AP Dolphin'), who informed the DPF that they would follow up with Liaison Bureau Netherlands regarding their position on disclosure of the personal data. AP Dolphin also provided its opinion to the DPF that information on the complainant should not be released [redacted][13]

2.7. On 25 May 2020, the DPO of the Dutch Police contacted Europol to ask why Europol was still processing personal data on the complainant when the SIENA message had been cancelled. The Netherlands subsequently, on 27 May 2020, sent a SIENA request to Europol to delete all data of the complainant mentioned in SIENA 1346846-1-1 (the SIENA message sent from the Netherlands to Germany) and SIENA 1346846-3-1 (the cancellation message), noting that the pending procedure to consult the Dutch Police on disclosure could be solved if Europol would delete the information from its Analysis System. The Dutch counter-terrorism unit asked Europol to "let them know whether the deletion could be a solution to the problem."[14] On 28 May 2020 the DPF was informed by AP Dolphin that the data in the cancelled SIENA message had been deleted.[15]

2.8. On 3 June 2020, the DPF performed a check in the EAS to verify that no data on the complainant was being processed by Europol. It was then discovered that a second item of personal data, relating to the complainant in the form of the above-mentioned Twitter account, was stored in the Europol Analysis System (EAS). Due to the fact that the DPF could not find the origin and relevance of the information on the complainant's Twitter account, on 4 June 2020 the DPF sent to several APs (AP Hydra, AP Dolphin, AP TFTP and EU IRU) a request as to whether: (i) the data on the Twitter account was relevant from an operational point of view and needed to be stored in the

[12] Analysis Project Dolphin gathers intelligence and information available in EU Member States linked to terrorist groups identified by the Council of the European Union, and other violent extremist groups active in the EU. See: https://www.europol.europa.eu/operations-services-and-innovation/europol-analysis-projects
[13] EDOC#1114580v1.
[14] Exchange described by the DPF in an email to the EDPS on 3 June 2021.
[15] EDOC#1114580v1.

EAS; and (ii) whether information on the storage of the Twitter account could be released to the complainant.[16]

2.9. On 5 June 2020, the European Counter Terrorism Centre (ECTC) at Europol replied stating that the Twitter account was not relevant from an operational point of view and could be deleted from the EAS. On the matter of disclosure, the ECTC stated that it disagreed with the release of information to the data subject due to the fact that (i) the data would be deleted due to its lack of pertinence to the operational analysis and (ii) in order to guarantee that the release of information would not jeopardise a national ongoing investigation. The DPF replied requesting deletion of the data as soon as possible. The same day the ECTC communicated to the DPF that it had deleted the data concerned from the EAS.[17]

2.10. On 5 June 2020 the DPF sent an internal briefing note, informing the Executive Director of a full hit (positive match) in its systems following a data subject access request, the procedures followed in accordance with Article 36 of the Europol Regulation to handle the request, and the assessment and proposed response to the data subject. The briefing note recommended to refuse access on the basis of the exemption provided by Article 36(6)(a) of the Europol Regulation as a measure necessary to enable Europol to fulfil its tasks properly.[18]

2.11. On 11 June 2020 Europol replied to the complainant, stating that: "There are no data concerning you at Europol to which you are entitled to have access in accordance with Article 36 of the Europol Regulation".[19]

Allegations of the complainant

2.12. In his initial complaint filed with the EDPS on 6 October 2020, the complainant alleges that Europol denied it was processing any information relating to him. He asserts that he believes this not to be true and states that he has "the right to know which personal data related to me Europol has stored. Very important because this data might be incorrect, which might [cause] severe danger to me." He requests that Europol disclose which personal data related to him they have stored and that Europol send him a copy of that data.[20]

[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] Letter of Europol of 11 June 2020 to Mr Frank van der Linde, ref. 1114580-20.
[20] EDPS complaint submission form submitted on 6 October 2020.

2.13. In an additional written submission, provided by email to the EDPS on 7 May 2022, the complainant recalls his right to access data concerning him under Article 36(1) of the Europol Regulation and the full list of information that Europol shall provide in accordance with Article 36(2) of the Europol Regulation. He states that the decision of Europol to refuse access to any information is inconsistent with the fact that he has already been provided access to several SIENA messages sent by the Dutch Police to Europol. He therefore alleges that Europol is in breach of Article 36(2) of the Europol Regulation.[21]

Comments of the data controller

Regarding the decision to refuse access and the applicability of the exemption under Article 36(6)(a)

2.14. Europol took the decision to refuse access to the personal data processed about the complainant as a necessary measure in order to enable Europol to fulfil its tasks properly under Article 36(6)(a) of the Europol Regulation. In comments provided to the EDPS on 11 November 2020, Europol explained that the information initially processed about the complainant in Europol's systems (SIENA message 1346846-1-1) [redacted][22] In response to the EDPS' request for further information, the EDPS was informed that "clarification on this matter could be provided to you by the Dutch competent national authorities."[23]

2.15. Regarding the personal data processed by Europol as a result of the extraction of a digital device (the complainant's Twitter account), Europol explained that the extraction and transfer of data to Europol took place in the framework of an on-going investigation. According to Europol, revealing the existence of this data and its subsequent deletion might have jeopardised that on-going national investigation.[24] The internal Europol briefing note on the access request of Mr van der Linde notes that the ECTC cited both the risk to a national investigation and the fact that the

[21] Email of 7 May 2022 of Frank van der Linde to the EDPS, subject: '*Legal substantiation to my complaint.*'
[22] Email of Europol to the EDPS of 11 November 2020.
[23] Email of Europol to the EDPS, 3 June 2021.
[24] Email of Europol to the EDPS of 11 November 2020.

data would be deleted from the EAS due to its lack of operational relevance for the investigation concerned "" as reasons to refuse access to this item of personal data.[25]

Regarding the revised assessment on disclosure of personal data to the complainant

2.16. Following the EDPS' request to Europol to reassess its decision of 11 June 2020 on the basis of the revised opinion of the Dutch SA, on 11 February 2022, Europol informed the EDPS of the results of its reassessment. While it upheld the initial decision-making that led to its decision to refuse access, Europol now, in light of the second opinion of the Dutch SA, "comes to the conclusion that there are no aspects for Europol to divert from the opinion of the NL data protection authority, i.e. that there are no reasons to refuse access to the information with respect to the data subject."[26]

2.17. Nevertheless, Europol also stated that as it had "deleted the remaining information concerning the data subject already on the 5 June 2020... even before the first answer was given to the data subject on 12 June 2020, it is considered appropriate that the data subject is referred to the competent authorities in NL." Europol also stated that it had established that on 7 February 2022, "there is no information on the data subject processed in Europol's operational systems at this moment in time, in line with the procedure agreed with the EDPS."[27]

2.18. Europol consequently proposed to inform the complainant that Europol had reassessed its position as regards the access request, confirm to him that it had been processing data on him originating from the Dutch law enforcement authorities at the time of his request, and inform him that these personal data had been deleted on 5 June 2020. For any further information, Europol proposed to advise the complainant to address the Dutch SA.

Regarding the deletion of the personal data concerning the complainant

2.19. Europol records, in its internal assessment of the access request, that it had deleted the first item of personal data concerning the complainant (SIENA messages and attached personal file) in cooperation with the Netherlands, on 27 May 2020, after determining that Europol was still in possession of the data due to an error. Europol took the decision to delete the second item of personal data concerning the

[25] EDOC#1114580v1 (Europol Briefing note of 4 June 2020, 'Data subject access request - full hit Mr Frank van der Linde').
[26] Email of Europol to the EDPS of 11 February 2022.
[27] Ibid.

complainant on 5 June 2020 after it was assessed by the ECTC to be operationally irrelevant and after the DPF asked it to proceed to deletion as soon as possible.[28]

2.20. During Europol's operational visit to the EDPS on 22 June 2021, Europol explained that despite having deleted the entity concerning the complainant in May 2020 in the Europol Analysis System (EAS), it was still possible to retrieve information on the complainant's Twitter account via a targeted search in the EAS because this personal data was still stored in the raw document extracted from the mobile phone. In addition, despite the SIENA messages relating to the case having been deleted on 27 May 2020 in SIENA, Europol explained that the set of data related to the case will only be deleted when a new data retention functionality ('the EAS SIENA data retention synchronisation') is implemented.[29]

Opinion of the Dutch SA

2.21. In its first letter to the EDPS of 16 April 2021, the Dutch SA informed the EDPS that it had consulted the Central Unit of the Netherlands Police and encountered difficulties in locating the required information (e.g. no record found of Europol's consultation of the Dutch police under Article 36(5) of the Europol Regulation, and no record located of the transmission of personal data on the complainant to Europol by the Dutch competent authorities). In the absence of this information, the Dutch SA could not provide an opinion regarding the lawfulness of transmission of the personal data from the Netherlands to Europol. Regarding the possibility to grant access to the personal data of the complainant, the Dutch SA relayed the position of the Dutch police that "the data shared with Germany on the data subject is of such nature (counter-terrorism information) that it cannot be disclosed to him."[30]

2.22. The revised opinion of the Dutch SA, provided by letter on 14 September 2022, informed that follow-up consultations with the Privacy Officer of the Netherlands Police's Central Unit had located the two items of personal data concerning the complainant and transmitted by the Netherlands competent authority to Europol in 2018 and 2020.

[28] EDOC#1114580v1 (Europol Briefing note of 4 June 2020, 'Data subject access request - full hit Mr Frank van der Linde').
[29] Minutes of the Visit of Europol to EDPS premises of 22 June 2021 in order to provide access to the documents requested in the context of the investigation of the complaint (2020-0908).
[30] Letter of the Dutch SA of 16 April 2021, "Request for cooperation - Consultation on a complaint against Europol (EDPS Case No 2020-0908)" ref. z2021- 01483.

2.23. As regards SIENA message 1346846-1-1, Dutch police records showed that the complainant had already obtained access to a copy of this personal data by the Regional Police Unit of Amsterdam in 2019, with the exception of the handling officer's name. Regarding the lawfulness of the transmission of the information item to Europol, the Dutch SA echoed the privacy officer's assessment that the transmission was lawful and in accordance with Dutch law. Regarding the possibility of disclosure, the Dutch SA informed that "as the complainant already has full knowledge of the information item concerned, the NL police does not see the need for keeping this information from him or calling in restrictions for that matter."[31]

2.24. As regards the second item of personal data, the complainant's Twitter account, the Dutch SA finds that the transmission of the information to Europol was lawful and in accordance with the Dutch law. As regards the decision to refuse access, the Dutch SA informs that it is the position of the Dutch police that: "no restrictions in releasing the information to the complainant are necessary, as in principle it could happen to anyone that his personal data from a social media account turn out to be stored on a device of person who has become a target of interest to law enforcement."

2.25. The Dutch SA concludes that "we can agree with the Netherlands police's assessment that both transmissions were lawful and in neither case the need would occur to refer to refusals or restrictions regarding the complainant's right of access as laid down in Article 36 of the Europol Regulation."[32]

3. Legal Analysis

Formal legality of Europol's Decision

3.1. Article 36(4) of the Europol Regulation requires that Europol respond to a data subject access request within three months of receipt of the request. Europol received the request from the designated competent authority on 10 March 2020 and issued a decision on 11 June 2020. The EDPS notes that the late reply (one day after the legal deadline expired) resulted from difficulties obtaining a reply from the Netherlands in response to Europol's consultation request.

3.2. Article 36(5) of the Europol Regulation states that Europol shall consult the competent authorities of the Member States that provided the personal data on the decision to

[31] Letter of the Dutch SA of 14 September 2021, "Request for cooperation - Consultation on a complaint against Europol (EDPS Case No 2020-0908)" ref. z2021- 01483.
[32] Ibid.

be taken in response to an access request. The provision stipulates that "a decision on access to personal data shall be conditional on close cooperation between Europol and the Member States and the provider of the data directly concerned."

3.3. As regards the decision to refuse access to information relating to SIENA message 1346846-1-1, Europol duly consulted the Dutch competent authorities on a decision to be taken. Europol's attempts to obtain a reply to this consultation request are documented, although no formal response to the request was received from the Dutch competent authority other than a request to delete the data concerned.[33]

3.4. As regards the second item of personal data (Twitter account), Europol did not consult the Dutch competent authorities before issuing a refusal of access. Europol chose to rely only on the internal assessment of Europol's operational staff. While Europol's decision may have been motivated by the requirement to respond to the access request before the expiry of the three month time limit, nevertheless the procedure for reaching the decision to refuse access to this item of personal data is not in compliance with Article 36(5) of the Europol Regulation.

3.5. Article 36(7) of the Europol Regulation requires to inform the data subject of any decision to refuse access and to provide the reasons for such a decision. Europol applied the derogation available under Article 36(7) of the Europol Regulation which permits to only notify the data subject that checks have been carried out without giving any information about whether data concerning him or her are being processed if the provision of such information would deprive the refusal of its effect. Europol therefore informed the complainant that: "There are no data concerning you at Europol to which you are entitled to have access in accordance with Article 36 of the Europol Regulation."[34]

3.6. In accordance with Article 36(7) of the Europol Regulation, the reply provided to the complainant did inform of his right to lodge a complaint with the EDPS and to seek a judicial remedy before the Court of Justice of the European Union.

[33] EDOC#1114580v1 (Europol Briefing note of 4 June 2020, 'Data subject access request - full hit Mr Frank van der Linde'). See also Minutes of the Visit of Europol to EDPS premises of 22 June 2021 in order to provide access to the documents requested in the context of the investigation of the complaint (2020-0908).
[34] Letter of Europol of 11 June 2020 to Mr Frank van der Linde, ref. 1114580-20.

Material legality of Europol's Decision

Legitimacy of Europol's decision of 11 June 2020 to refuse the right of access to the first item on the basis of Article 36(6)(a)

(a) Conditions for a refusal of the right of access under Article 36(6) ER

3.7. According to Article 36(1) of the Europol Regulation, any individual shall have the right to obtain information on whether personal data relating to him or her are processed by Europol.

3.8. Article 36(6) of the Europol Regulation provides that Europol may refuse or restrict access, if such a refusal or restriction constitutes a measure that is necessary to achieve one of the four grounds for exemption listed in that Article. In this case, Europol applied Article 36(6) of the Europol Regulation invoking the ground for exemption to "enable Europol to fulfil its tasks properly" (Article 36(6)(a) of the Europol Regulation). Article 36(6) requires that "*when the applicability of an exemption is assessed, the fundamental rights and interests of the data subject should be taken into account.*"

3.9. Application of an exemption under Article 36(6) of the Europol Regulation constitutes a restriction of an individual's fundamental rights, as granted by Article 8 of the EU Charter of Fundamental Rights (the Charter), and a derogation to the right of access as a general rule provided by Article 36(1) of the Europol Regulation. The grounds for applying a derogation to Article 36(1) must be interpreted narrowly and applied strictly, in accordance with the guidance of the European Data Protection Board,[35] and established case law of the CJEU.[36] The CJEU's condition of strict necessity is a horizontal one, irrespective of the area at issue, including law enforcement.[37]

3.10. Article 52(1) of the Charter requires that any limitation on the exercise of the rights and freedoms recognised by the Charter must respect the essence of those rights and freedoms, be subject to the principle of proportionality, and be made only if they are

[35] The EDPB has established that, in line with the requirements of Article 52 of the Charter, restrictions under Article 23 of the GDPR should be interpreted narrowly, only be applied in specifically provided circumstances and only when certain conditions are met. See EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR.
[36] The case law of the CJEU applies a strict necessity test for any limitations on the exercise of the rights to personal data protection and respect for private life with regard to the processing of personal data: 'derogations and limitations in relation to the protection of personal data (...) must apply only insofar as is strictly necessary'. See CJEU, judgment of 16 December 2008, case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, ECLI:EU:C:2008:727, para 56.
[37] EDPS Guidance of 11 April 2017, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit, p.7.

necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[38] In determining what is "necessary" to justify a limitation of a fundamental right in accordance with Article 52(1) of the Charter, the proposed measure should be supported by evidence describing the problem to be addressed, how it will be addressed by the measure, and why less intrusive measures cannot sufficiently address it.[39] The case law of the CJEU and ECtHR indicates that necessity in data protection law is a facts-based concept, rather than a merely abstract legal notion, and that the concept must be considered in the light of the specific circumstances surrounding the case as well as the concrete purpose it aims to achieve.[40]

3.11. Any decision by Europol to refuse or restrict access to personal data by a data subject must be taken in light of the above legal framework. In this case, it means that the decision to refuse access to the complainant on the basis of Article 36(6)(a) of the Europol Regulation should have been based on a detailed assessment, supported by precise legal and factual reasons, demonstrating that the refusal to grant access to any information to the complainant was necessary to enable Europol to fulfil its tasks properly.[41] The risk, namely which Europol tasks in particular would be affected, and how disclosure would impact them, should be described. The risk should be specific, foreseeable and not merely hypothetical. The assessment, and the legal and factual reasons to support Europol's position must be documented internally.

3.12. A data controller, when applying a refusal or restriction to data subject rights, is not only required to conduct an assessment of the applicability of an exemption but is equally required to document that assessment and to motivate its decision with factual and legal arguments.[42]

3.13. This obligation derives from Article 41 of the Charter of the Fundamental Rights of the European Union, which provides for the right to good administration which has also been recognised as a general principle of EU law. The right to good administration is a procedural fundamental right that aims to fulfil the Union's commitment to the rule of law.

---

[38] Article 52(1), EU Charter of Fundamental Rights.
[39] EDPS Guidance of 11 April 2017, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit, p.8.
[40] Ibid.
[41] Opinion of the Article 29 Data Protection Working Party on some key issues of the Law Enforcement Directive, December 2017.
[42] Opinion of the Article 29 Data Protection Working Party on some key issues of the Law Enforcement Directive, December 2017, p.21; EDPS Guidance on Article 25 of the New Regulation and internal rules, December 2018, paragraph 25.

3.14. Article 41(2)(c) specifically provides that "*this right includes: … (c) the obligation of the administration to give reasons for its decisions*". This obligation is closely linked with the right to effective remedy laid down in Article 47 of the Charter and requires that the reasoning offered by the institutions, offices, bodies and agencies of the Union are sufficiently precise to enable the persons concerned to ascertain the reasons for the measure and the competent Court of the European Union to exercise its power of review. Even in cases where this duty is limited, as it has to be balanced with the obligation for professional secrecy or because of security considerations, the decision to withhold certain information is subject to judicial review and needs to be sufficiently motivated.[43]

3.15. This principle has also been integrated in the European Code of Good Administrative Behaviour in Article 18 (1) which states that "every decision of the institution which may adversely affect the rights or interest of a private person shall state the grounds on which it is based by indicating clearly the relevant facts and the legal basis of the decision".[44]

(b) Legitimacy of Europol's decision of 11 June 2020 to refuse the right of access to the first item (SIENA message 1346846-1-1) on the basis of Article 36(6)(a)

3.16. With regard to the first item of personal data concerning the complainant, SIENA message 1346846-1-1, Europol states in its internal assessment and by way of justification to the EDPS, that: "information in Europol's systems on the requester should not be released [redacted]"[45] Europol does not further clarify why this reasoning necessitated a full refusal of access to the data subject. Nor is it clear how only a partial disclosure of information, together with the notification that the personal data in question had been deleted, [redacted]. Further, Europol does not explain or document how disclosure - including partial disclosure of only certain information - would impact Europol's ability to fulfil its tasks properly.

3.17. The EDPS notes that Europol's reliance on the justification [redacted] appears to originate from internal information held by AP Dolphin. No written documentation was shared with the EDPS during the course of

[43] Kellerbauer et al, The EU Treaties and the Charter of Fundamental Rights : A Commentary, Oxford University Press 2019, p. 2204 - 2207.
[44] https://www.ombudsman.europa.eu/en/publication/en/3510.
[45] EDOC#1114580v1 (Europol Briefing note of 4 June 2020, 'Data subject access request - full hit Mr Frank van der Linde'), p.2.

its investigation indicating that this information came from the Netherlands competent authority. In response to EDPS requests for clarification [redacted] and the necessity for issuing a full refusal of access, Europol replied stating that "in a meeting ...it was stated by [a] Europol operational colleague that the [redacted]." Clarification on this matter could be provided to you by the Dutch competent national authorities that supplied the data to Europol."[46]

3.18. The EDPS reiterates that it is the responsibility of Europol, under Article 36(5) of the Europol Regulation, to ascertain the position of the national competent authority that provided the data prior to taking a decision on an access request. Had the consultation procedure been conducted to its full conclusion, Europol should have received the information that the Dutch police had already disclosed the SIENA message 1346846-1-1, including the personal file in attachment, to the complainant in 2019, which indicates that the Netherlands did not consider disclosure a risk.

3.19. In light of the considerations above, the EDPS finds that the necessity assessment, with regard to applying a full refusal of access to the information pertaining to SIENA message 1346846-1-1 was inadequate: the assessment was not supported by precise legal and factual reasons demonstrating how even a partial disclosure [redacted] and Europol was unable to provide this information to the EDPS during the course of its investigation.

3.20. Furthermore, it is unclear why, in this context, Europol chose to rely on Article 36(6)(a) of the Europol Regulation as a legal ground for applying a limitation to the right of access. Europol has not documented how disclosure (full or partial) would impact its ability to fulfil its tasks properly. It is thus not possible to fully assess the appropriateness of Europol's reliance on Article 36(6)(a).

3.21. In light of the considerations above, the EDPS finds that the obligation to sufficiently motivate the decision to apply an exemption under Article 36(6) of the Europol Regulation and under Article 41 of the EU Charter was not fulfilled. Europol did not document in its internal assessment preceding its decision, how disclosure of information (even partial information) regarding its processing of the personal data contained in SIENA message 1346846-1-1) on the complainant would prevent Europol from fulfilling its tasks properly.

(c) Legitimacy of Europol's decision of 11 June 2020 to refuse the right of access to the second item (Twitter account) on the basis of Article 36(6)(a) of the Europol Regulation

[46] Email of Europol to the EDPS of 3 June 2021.

3.22. Regarding the second item of personal data concerning the complainant (the Twitter account), Europol (ECTC) states in its internal assessment as reasons for non-disclosure: "(i) the fact that the data will be deleted from EAS for its lack of pertinence to the analysis; (ii) to guarantee that the release of information will not jeopardise the national ongoing investigation [redacted]."[47]

3.23. With regard to the first reason for refusal of access, that the information concerning the processing of the Twitter account should not be disclosed because the data would be deleted for its lack of pertinence to the analysis,,the EDPS supports the internal assessment of the DPF of the case,[48] i.e. that this is not a legitimate justification to restrict or refuse access to a data subject. Europol can only refuse access on the basis of one of the grounds listed under Article 36(6) ER of the Europol Regulation. Part of the data processed by the data controller cannot be omitted from the disclosure without a legitimate ground justifying such an omission. When a controller receives a data subject access request, the controller must assess the personal data being processed that falls within the scope of the access request. That assessment must reflect as close as possible the situation when the controller receives an access request and the response should cover all data available at that point in time.[49]

3.24. With regard to the second reason put forward by Europol's ECTC, that disclosure would jeopardise an ongoing investigation, Europol does not further elaborate how disclosure to the complainant that Europol had been processing his Twitter account could jeopardise this investigation.

3.25. The link between the disclosure of this information and the risk described is not evident and not established factually. On the contrary, the Netherlands police observed, in their risk assessment provided to the Dutch SA, that it could happen to anyone that their social media information is stored on the mobile device of a person who becomes the target of interest by law enforcement and therefore concluded that the risk is negligible.

3.26. It is thus not demonstrated that the disclosure of the information requested would jeopardise an ongoing investigation.

3.27. Refusal of access was finally based on Article 36(6)(a) of the Europol Regulation, i.e. to enable Europol to fulfil its tasks properly. However, Europol does not explain or

[47] Ibid, p.3.
[48] EDOC#1114580v1 (Europol Briefing note of 4 June 2020, 'Data subject access request - full hit Mr Frank van der Linde').
[49] EDPB Guidelines 01/2022 on data subject rights - right of access, p.17.

document how disclosure (full or partial) of its processing of the complainant's Twitter account would impact Europol's ability to fulfil its tasks properly.

3.28. In light of the considerations above, the EDPS finds that Europol has not demonstrated the necessity of the limitation applied with regard to issuing a full refusal of access to information with respect to the processing of the Twitter account.

3.29. Therefore, the EDPS finds that the obligation to sufficiently motivate the decision to apply an exemption under Article 36(6) of the Europol Regulation and under Article 41 of the EU Charter was not fulfilled. Europol did not document in its internal assessment preceding its decision, how disclosure of information (even partial information) regarding its processing of the personal data of the Twitter account of the complainant would prevent Europol from fulfilling its tasks properly.

Europol's reassessment of 11 February 2011 and provision of access to the complainant

3.30. Europol states, in its email of 11 February 2022 to the EDPS, that having reviewed its initial decision in light of the information provided by the Dutch SA, it now considers that there are no reasons to refuse access to the information with respect to the data subject. However, due to the Agency having deleted the personal data concerning the complainant "it is considered appropriate that the data subject is referred to the competent authorities in NL" and proposes to refer the complainant to the Dutch SA.

(a) About the entity obliged to grant access under Article 36 of the Europol Regulation

3.31. Article 36 of the Europol Regulation lays down the procedures by which Europol shall receive, consult on and issue a decision in response to a data subject access request. Article 36(2) ER allocates sole responsibility to Europol for providing access ("Europol shall provide the following information to the data subject…"). While Article 36(5) ER requires close cooperation with the competent national authority (as provider of the data) on the decision to be taken, as long as the data subject request was addressed to Europol, the task of granting access should not be re-assigned to the national competent authority, via referral to the national SA.

3.32. Under the data protection legal framework, the controller may not direct the data subject to different sources in response to a data subject request. In line with the transparency principle, data subjects must obtain from the controller the information and personal data required in a way that enables a complete access to the requested

information.[50] The EDPS therefore underlines that it is the obligation of Europol, and no other entity, to grant access to the complainant of his personal data.

(b) Extent of the access to be granted to the complainant under Article 36(2) of the Europol Regulation

3.33. As to the precise form of the access to be granted, access should comprise provision of the full set of information listed under Article 36(2) of the Europol Regulation. Article 36(2) provides that Europol shall, as a rule, provide confirmation as to whether or not data related to the data subject are being processed; communication of the data undergoing processing; a full set of information relating to the processing, as well as the existence of the right to request from Europol rectification, erasure or restriction of processing of personal data concerning the data subject.

3.34. Article 36(2)(c) of the Europol Regulation requires "communication in an intelligible form of the data undergoing processing" to be provided. The Europol Regulation does not specify further the form by which personal data should be disclosed. However, recital 43 of the Law Enforcement Directive indicates that for the right of access to be complied with, personal data should be provided in "a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with this Directive, so that it is possible for him or her to exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing."[51]

3.35. The EDPS recalls that a central component of the right of access is not only to know whether a controller is processing data on a given individual, but also to be able to access and verify these data. The controller is therefore under the obligation to grant access to the fullest extent and ensure that the personal data provided is complete.[52] Ensuring that the personal data provided is complete is essential for the data subject to be able to exercise other data subject rights, including requesting rectification, erasure or restriction,[53] and to verify the lawfulness of the processing.[54] Provision of

[50] EDPB Guidelines 01/2022 on data subject rights - right of access, paragraph 128.
[51] Recital 43 of EU Directive 2016/680 of 27 April 2016 on 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, OJ L 119/89
[52] EDPB Guidelines 01/2022 on data subject rights - right of access, p.12 and p.46.
[53] Case C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, judgment of 7 May 2009, ECLI:EU:C:2009:293.
[54] Case C-434/16, Peter Nowak v Data Protection Commissioner, judgment of 20 December 2017, ECLI:EU:C:2017:994.

personal data in a complete a form as possible is also necessary to enable the data subject to exercise his or her right to effective remedies under Article 47 of the EU Charter.[55]

3.36. Thus, while the applicable data protection framework does not oblige provision of a copy of the personal data, there may be circumstances in which this offers the most effective means of granting access. Analysis of both European and national level case law indicates that, in certain cases, providing an actual copy of the personal data undergoing processing is the only effective means of disclosing the data in line with the requirement to ensure personal data provided is complete.[56]

3.37. In light of the considerations above, taking into account the complainant's explicit written request to receive all information items listed under Article 36(2) of the Europol Regulation and in particular a copy of the personal data processed by Europol concerning him,[57] in accordance with Article 36(2)(c) of the Europol Regulation, and based on the evidence obtained by the EDPS that the complainant has already been granted access to a full copy (excluding the handling officer's name) of the personal data transmitted by the Netherlands to Europol pertaining to SIENA message 1346846-1-1,[58] the EDPS sees no justifiable reason to provide information to a lesser extent. Europol should therefore provide the complainant with all information listed under Article 36(2) of the Europol Regulation, including a copy of his personal data relating to the SIENA message 1346846-1-1 and the personal file attached.

Europol's deletion of the personal data concerning the complainant

3.38. During the handling of the complainant's data subject access request, and while conducting an assessment of the request, Europol deleted both items of personal data, prior to issuing the data subject with a reply.

3.39. The first item of data was deleted in cooperation with the Netherlands, after determining that Europol was still in possession of the data due to an error. The

[55] Case C-362/14, Maximilian Schrems v Data Protection Commissioner, judgment of 6 October 2015, ECLI:EU:C:2015:650.
[56] Case C-434/16, Peter Nowak v Data Protection Commissioner, judgment of 20 December 2017, ECLI:EU:C:2017:994; K.H. and Others v. Slovakia, Application no. 32881/04, Council of Europe: European Court of Human Rights, 28 April 2009; Judgment of the Higher Regional Court of Cologne, OLG Köln, 13.05.2022 - 20 U 295/21.
[57] EDPS complaint submission form submitted on 6 October 2020.
[58] Letter of the Dutch SA of 14 September 2021, "Request for cooperation - Consultation on a complaint against Europol (EDPS Case No 2020-0908)" ref. z2021- 01483.

second item of personal data was deleted as it was assessed not to be operationally relevant.

3.40. According to Article 36(1) and (2) of the Europol Regulation, the assessment of an access request and the data concerned by such request shall reflect the processing at the time the request was received. The response should cover all data available at that point in time. This necessarily includes data that may be unlawful, inaccurate or no longer required by the controller.

3.41. The possibility to know about such data is one of the main objectives of the right of access and has a bearing on the order by which a controller should meet its obligations to both respond to a data subject access request and delete or correct unlawful or inaccurate data. Thus the EDPB in its guidance on the matter, instructs controllers to first reply to data subjects, before preceding to the deletion of unlawful data.[59] When providing access, the controller should at the same time notify the data subject of its intention to delete or rectify the data.

3.42. In this instance, Europol decided to apply an exemption to the right of access, based on Article 36(6) of the Europol Regulation. Europol thus decided not to inform the data subject prior to the deletion. It is therefore necessary to determine whether personal data can be deleted when a controller issues a refusal or restriction of access following a data subject access request, if it assesses that it no longer has a legal basis for retaining the data that has been refused or restricted.

3.43. Article 36(6) of the Europol Regulation is analogous to the restrictions provided under Article 23 of the GDPR,[60] or Article 25 of the EU Data Protection Regulation.[61] Guidance provided by the EDPB on the application of restrictions under Article 23 GDPR underlines that "even in exceptional situations, the protection of personal data cannot be restricted in its entirety. [Restrictions] ...shall respect the general principles of law, the essence of the fundamental rights and freedoms and shall not be irreversible."[62] Data subjects must be in a position to challenge the restriction and have access to a judicial remedy vis-a-vis the processing.

---

[59] EDPB Guidelines 01/2022 on data subject rights - right of access, paragraph 39.
[60] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC.
[61] 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.
[62] EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, paragraph 4.

3.44. In order to ensure that data subjects may exercise their rights with respect to personal data that has been subject to a restriction, controllers are instructed, when establishing the relevant retention periods applied to such personal data, to take into account potential data subject requests, complaints or legal proceedings.[63] The standard retention period should build in the possibility for a data subject to lodge a complaint with the Data Protection Authority, bring an action before the court for alleged data protection infringements or lodge a complaint with other competent administrative authorities (e.g. an ombudsman) for infringements of other rights. [64]

3.45. Article 31(1) of the Europol Regulation requires personal data to be retained only as long as is necessary and proportionate for the purposes for which it is processed. Article 31(6) of the Europol Regulation provides that personal data shall not be erased if this would damage the interests of the data subject; if their accuracy is contested; if they have to be maintained for purposes of proof or for the establishment, exercise or defence of legal claims; or if the data subject opposes their erasure and requests their restriction instead.

3.46. When the retention of personal data processed for operational purposes is assessed as no longer necessary and proportionate, this data should be erased. However, where the continued storage of this data is required for other purposes, such as to protect the legitimate interests of the data subject (or fulfil other objectives under Article 31(6) of the Europol Regulation), then the data should be retained in a restricted form, and only processed for the purposes for which it has been retained.

3.47. The EDPS notes that during the course of the EDPS complaint investigation, upon the EDPS' request, Europol was able to retrieve both items of personal data concerning the complainant. Europol shared a copy of the relevant SIENA messages and a copy of the personal file on the complainant during the operational visit to the EDPS on 22 June 2021. It is therefore unclear to the EDPS why Europol now claims to no longer be in a position to disclose the information to the complainant.

[63] EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR; EDPS Guidance of June 2020 on Article 25 of the Regulation 2018/1725 and internal rules restricting data subjects rights, paragraph 54.
[64] Both the EDPS and the EDPB advise that the retention period be calculated as the duration of the processing operation plus additional time for potential litigation. Refer to EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, paragraph 76. See also EDPS Guidance of June 2020 on Article 25 of the Regulation 2018/1725 and internal rules restricting data subjects rights. See also Case C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, judgment of 7 May 2009, ECLI:EU:C:2009:293; and the decision of the Spanish Data Protection Authority (AEPD) PS/00267/2021.

3.48. Europol states that it established on 7 February 2022 "that there is no information on the data subject processed in Europol's operational systems at this moment in time, in line with the procedure agreed with the EDPS."[65] The EDPS strongly underlines that no such procedure was discussed or agreed with Europol during the complaint investigation with respect to the deletion of the complainant's personal data.

3.49. The EDPS understand that this statement could mean two different situations: (1) the personal data of the complainant have been erased, while they should not have been erased as the request of the data subject triggered application of Article 31(6)) of the Europol Regulation; (2) the personal data of the complainant are simply archived, or as Europol expresses itself 'deleted' (i.e. 'soft deleted', see next section) in which case it should have been considered as existing for the purpose of the complainant's access request.

3.50. The EDPS further underlines that should Europol have erased (permanently deleted) the personal data concerning the complainant, this would constitute a failure to cooperate with the EDPS and a serious infringement of the Europol Regulation. Erasure of personal data that is the subject of an EDPS investigation prior to the conclusion of that investigation amounts to an obstruction of the EDPS' abilities to exercise its duties under Article 43(2)(a) of the Europol Regulation and of its ability to order corrective measures in accordance with Article 43(3)(c) of the Europol Regulation.

Retrieval of personal data deleted by Europol concerning the complainant

3.51. Europol states that it "established on 7 February 2022 that there is no information on the data subject processed in Europol's operational systems at this moment in time..."[66] The EDPS has grounds to understand that even data which is deleted from Europol's operational systems is nevertheless searchable and retrievable by Europol, from its databases, back-up systems or archives.

3.52. EDPS onsite inspections of Europol's data retention and deletion procedures with respect to its IT systems (including SIENA and the EAS) indicate that Europol does not implement a consistent policy of hard deletion, i.e. erasure of personal data.[67] Rather, once Europol assesses that data can no longer be stored under Article 31 of the Europol Regulation (i.e. only for as long as is necessary and proportionate to do so) personal

[65] Email of Europol to the EDPS of 11 February 2022.
[66] Email of Europol to the EDPS of 11 February 2022.
[67] Hard deletion implies the physical deletion of the data, removing them from the database so they cannot be accessed if a back-up copy is not restored.

data is 'soft deleted', meaning that it is marked so that users cannot access them, but nevertheless retained in those databases. [68]

3.53. Findings of EDPS inspection activities indicate that Europol retains soft-deleted data for extended periods of time in SIENA, EAS, and EIS databases.[69] Despite having issued recommendations to remedy this situation and put in place an automated archiving policy, the EDPS understands that this situation persists, and will only be addressed in the context of a significant forthcoming overhaul of Europol's new IT architecture.[70] It is the EDPS' understanding that soft deleted data can be searched and retrieved from Europol's databases by duly authorised Europol staff.

3.54. Furthermore, Europol systems, such as data archives, backups and other infrastructure components, that are not accessible by end-users for operational purposes, may have a longer retention of copies of operational data than the production system if necessary and justified by the purposes of that system, even after data has been deleted from the production system concerned.[71]

3.55. According to Europol's Data Archiving Policy, copies of deleted data are retained and stored in Europol's archives for a period of five years. In principle, all data processed in Europol's production systems are archived before their erasure from the production system. The data is retained, and may only be retrieved, for the purpose of its possible use "in court cases or other exceptional circumstances."[72] Other exceptional circumstances may include the event that data was removed from the production system as a result of a mistake in the review process and which cannot be retrieved from a backup system.[73]

3.56. The EDPS therefore understands that if the personal data of the complainant that has been deleted by Europol on 27 May and 5 June 2021 cannot be restored by any other means, this data can be retrieved from Europol's data archives.

3.57. The EDPS considers that Europol must now retrieve, by any technical means necessary, the personal data concerning the complainant that it has deleted and that is necessary to grant full access to the complainant, in accordance with Europol's revised position on disclosure as set out to the EDPS on 11 February 2022, and in order to comply with its obligations under Article 36 of the Europol Regulation.

---

[68] EDPS Report on Inspection at Europol of 7 May 2018(case 2017-0656), p.41-45.
[69] Ibid, p.42.
[70] Refer to EDPS report 'Recommendations of EDPS Inspection Reports - Follow-up',
[71] EDOC1189145-v9, Data retention and Archiving Policy for Operational Data (draft), 3 May 2022.
[72] EDOC393445, Europol Data Archiving Policy.
[73] EDOC1189145-v9, Data retention and Archiving Policy for Operational Data (draft), 3 May 2022.

Findings of the EDPS

3.58. In light of the above, the EDPS concludes that there has been a breach of Article 36(1) and (2) of the Europol Regulation, due to Europol's decision to issue a full refusal of access to the complainant without having established the necessity to issue a full refusal of access to the complainant in relation to both sets of personal data that it was processing concerning him.

3.59. The EDPS also finds that in breach of Article 36(6) of the Europol Regulation read in connection with Article 41 of the Charter of the Fundamental Rights of the European Union, Europol did not sufficiently motivate its decision to issue a refusal of access, in particular in relation to its decision to issue a refusal based on the legal grounds provided by Article 36(6)(a) of the Europol Regulation, by failing to document internally the legal and factual reasons for this decision.

3.60. Further, the EDPS finds Europol in breach of Article 36(5) of the Europol Regulation, for having failed to consult the national competent authority on a decision to be taken with respect to the disclosure of personal data concerning the complainant's Twitter account.

4. Decision

4.1. The EDPS therefore decides to:

1. Order Europol, in accordance with Article 43(3)(c) of the Europol Regulation, to comply with the complainant's request to exercise his right to access his personal data, by providing the complainant with the full set of information which he is entitled to receive under Article 36(2) of the Europol Regulation, including a copy of the personal data pertaining to SIENA message 1346846-1-1, and a summary of information regarding the processing of his Twitter account;

2. Order Europol, in accordance with Article 43(3)(c) of the Europol Regulation, to provide to the EDPS confirmation that Europol took the measures ordered under 1) above;

3. Admonish Europol , in accordance with Article 43(3)(d) of the Europol Regulation:

a) for not sufficiently motivating its decision to refuse the exercise of the data subjects' right of access and in particular for not documenting all factual and legal reasons leading to it.

b) for not having complied with the procedure laid down in Article 36(5) of the Europol Regulation and in particular for not having consulted the national competent authority on a decision to be taken with respect to the disclosure of personal data concerning the complainant's Twitter account.

The present decision closes this complaint case.

The complainant will be informed of the EDPS' conclusions and the corrective measures applied.

5. Judicial Remedy

5.1. Pursuant to Article 48 of the Europol Regulation, any action against a decision of the EDPS can be brought before the Court of Justice of the European Union within two months from the adoption of the present Decision and according to the conditions laid down in Article 263 TFEU.

Done in Brussels, 8 September 2022

[e-signed]

Wojciech Rafał WIEWIÓROWSKI