Decision in case 233/2021/OAM on how the European Border and Coast Guard Agency (Frontex) dealt with a request for public access to documents concerning tracking data of vessels used in Frontex maritime operations

Decision
Case 233/2021/OAM - **Opened on** 10/02/2021 - **Decision on** 30/03/2021 - **Institution concerned** European Border and Coast Guard Agency (No maladministration found) |

The case concerned the European Border and Coast Guard Agency's (Frontex) refusal to grant public access to tracking data of several vessels used in its maritime operations in the Aegean Sea. The complainant sought access to specific types of data regarding the location of the vessels. Frontex initially identified several documents containing location information but refused to grant public access on the grounds that doing so would undermine the public interest as regards public security. In its final reply, Frontex stated that it did not hold any documents containing the specific data requested.

The Ombudsman inquired into the issue and confirmed that Frontex did in fact not hold documents containing the specific data requested. She nevertheless assessed the substantive position set out by Frontex with respect to documents containing similar data, among others vessel positioning data, and found that the refusal was justified.

The Ombudsman called on Frontex to ensure a consistent approach when replying to requests for public access to documents. In particular, Frontex should be diligent in verifying what documents are in its possession and offer comprehensive explanations to applicants.

Background to the complaint

1. The European Border and Coast Guard Agency (Frontex) is an EU agency tasked with assisting Member States in monitoring the EU's external borders. A Member State may request Frontex to launch a joint operation in which other Member States can participate and provide technical equipment (for example vessels, aircraft, vehicles) or staff. [1] For several years, Frontex has been supporting Greece in the context of 'Joint Operation Poseidon' covering the area of the Greek sea borders with Turkey and the Greek islands - mainly the Aegean Sea. Operation Poseidon involves border control, search and rescue, registration and identification,

as well as coast guard functions and prevention of cross-border crime. [2]

2. The complainant is a Member of the European Parliament. On 29 September 2020, she asked Frontex for public access to documents [3] containing data regarding specific vessels used in Frontex maritime operations. Specifically, the complainant requested *"the Automatic Identification System data (AIS-data)* [**[4]**] *and Long Range and Identification Tracking data (LRIT-data)* [**[5]**] *of the following vessels used by FRONTEX since March 2020 until present day in the Aegean Sea."* The complainant then listed 16 vessels, for which she requested the data.

3. In November 2020, Frontex replied and explained that for the 16 th vessel listed by the complainant no documents were identified. For the remaining 15 vessels, *"documents mention the pieces of information sought by [the complainant] only in the [sic] passing".* Frontex did not list those documents and refused access, arguing that disclosure would undermine the protection of the public interest as regards public security as well as the protection of privacy and the integrity of the individual. [6]

4. In December 2020, the complainant asked Frontex to review its decision (by making a so-called 'confirmatory application').

5. In January 2021, Frontex replied, stating that it stands by the arguments presented in its initial reply. However, as part of its review of its initial position, it concluded that *"no documents containing AIS and/or LRIT data for any of the vessels [the complainant] mentioned can be retrieved."*

6. In February 2021, the complainant turned to the Ombudsman.

The inquiry

7. The Ombudsman opened an inquiry into how Frontex dealt with the request for public access concerning the tracking data of the respective vessels used in Frontex maritime operations. [7]

8. In the course of the inquiry, the Ombudsman received additional information from Frontex on its handling of the complainant's request as well as extracts from internal correspondence regarding the preparation of the replies. The Ombudsman's inquiry team also inspected one ' *Technical equipment mission report'* , as a sample of the documents identified by Frontex in its initial reply.

Arguments presented to the Ombudsman

By the complainant

9. The complainant argued that she was not interested in receiving personal data. Therefore,

she asked Frontex to prepare a document containing the requested information without including personal data – if necessary by extracting it from a database by using existing search tools. [8]

10. The complainant contended that Frontex had not explained, as established by case-law, [9] how disclosing the requested information would 'specifically and actually' undermine the public interest as regards public security. Also, she contended that tracking information from the past, as had been requested, could not undermine the protection of the public interest as regards public security since it could not be used by traffickers with respect to vessels in the present.

11. Finally, the complainant disapproved of the way Frontex had handled her request, notably the fact that in its final assessment, Frontex argued that it did not hold any documents containing the requested data, while in its initial reply it had identified such documents.

By Frontex

12. According to the explanations provided by Frontex in its initial reply, disclosure of the documents identified would undermine the protection of the public interest as regards public security. The documents in question included the information sought by the complainant only in passing . However, they included " *detailed information on the technical equipment deployed".* If traffickers were to gain hold of such information, along with the location of the vessels, they could avoid controls and endanger the vessels and their crew. The documents also included personal data whose release would undermine the protection of privacy and the integrity of the individual.

13. In its reply to the request for review, Frontex argued that it did not hold any documents containing the specific data requested by the complainant, namely AIS- and LRIT-data. Frontex explained that AIS systems operated on a radio communication frequency and sent radio messages that included, among others, the vessel's positions. AIS data, such as these radio messages, were stored in the AIS device itself in the respective vessel as well as in coastal stations and regional vessel traffic control systems. As such, they were not received or stored by Frontex itself. Similarly, Frontex did not itself receive or store LRIT-data.

14. In the additional information transmitted to the Ombudsman, Frontex explained that the documents identified in its initial reply were 'technical equipment mission reports' which, among others, contained positioning data of the concerned vessels. However, positioning data were not technically the same data as the specifically requested AIS- and LRIT-data. As such, Frontex's assessment in its confirmatory reply differed from its initial reply. In any case, the reports were sensitive and their disclosure would undermine the protection of the public interest as regards public security.

The Ombudsman's assessment

15. The right of public access to documents applies only to documents in the possession of the institution concerned. [10]

16. In this case, Frontex, in its final reply, refused to give public access on the grounds that it does not hold any documents that would fall within the scope of the complainant's request.

17. On the basis of the inquiry team's inspection, as well as Frontex's explanations, the Ombudsman does not have reason to doubt that Frontex does not hold documents containing the specific data requested by the complainant, namely AIS- and LRIT-data. As such, the Ombudsman does not identify maladministration as regards Frontex's final position on the public access request.

18. That having been said, Frontex stated in its initial reply and acknowledged during the inquiry, that it does possess documents containing positioning data, other than AIS- and LRIT-data, with respect to 15 vessels referenced by the complainant. Therefore, the Ombudsman considers it helpful to review Frontex's refusal to provide access to those documents.

19. The Ombudsman understands that, after each patrolling activity, assets (for example vessels, aircraft, vehicles) participating in the joint operations coordinated by Frontex have to fill in a 'technical equipment mission report', which includes the track followed. The documents identified by Frontex at the initial stage were 'technical equipment mission reports' for the 15 vessels. According to Frontex, there are around 15-25 such reports daily.

20. Frontex has argued that the disclosure of these documents would undermine the public interest as regards public security. The EU courts have found that, in general, the EU institutions enjoy wide discretion when determining whether disclosing certain information could pose a risk in that regard. [11] Any substantive review of such a decision must therefore be limited to examining whether there has been an obvious error in the institution's assessment.

21. The General Court has acknowledged, in a similar case of a refusal by Frontex to disclose information which could lead to vessel positioning data being ascertained, that if traffickers knew the location of vessels, they would have the information needed to avoid the controls aimed at preventing unlawful border access or to attack the vessels. [12] According to the same judgment, this was the case even if the data sought on the location of vessels concerned periods in the past. [13]

22. In this case, the complainant made the access request on 29 September 2020 asking for data relating to the period between 1 March 2020 and 29 September 2020. While the time period for which the data was requested had expired, the Joint Operation Poseidon 2020 was still ongoing at the time of the request.

23. In light of this, the Ombudsman finds that Frontex's explanation, namely that giving public access to the positioning data of the vessels constitutes a significant risk to achieving its operational mandate and as such to the security of the vessels and their crew, is plausible.

24. The public security exception which Frontex relied upon is absolute. This means that Frontex did not need to assess whether there was an overriding public interest in the disclosure of the documents.

25. Taking all the arguments into account, the Ombudsman considers that Frontex's position that disclosing documents containing tracking data of vessels used in its maritime operations could undermine the protection of the public interest as regards public security is reasonable. [14]

26. However, the Ombudsman suggests that in the future, Frontex ensure a consistent approach when replying to requests for public access to documents. In particular, Frontex should be diligent in verifying what documents are in its possession. In addition, Frontex should assist applicants in their requests. In this case, Frontex could have provided clearer explanations to the complainant on the documents which it does hold that are similar to those requested, even if those documents were likely to be covered by relevant exceptions to public access.

Conclusion

Based on the inquiry, the Ombudsman closes this case with the following conclusion:

There was no maladministration by Frontex.

The complainant and Frontex will be informed of this decision **.**

Emily O'Reilly European Ombudsman

Strasbourg, 30/03/2021

[1] See Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard, available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1573722151667&uri=CELEX%3A32019R1896 [Link];

See also Regulation (EU) No 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of

Operational Cooperation at the External Borders of the Member States of the European Union, available at:

https://eur-lex.europa.eu/legal-content/en/ALL/?uri=celex:32014R0656 [Link]

[2] For more information see https://frontex.europa.eu/we-support/main-operations/operation-poseidon-greece-/ [Link] and https://frontex.europa.eu/about-frontex/faq/frontex-operations/ [Link].

[3] Under Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R1049&from=EN [Link], applicable to Frontex pursuant to Article 114(1) of Regulation 2019/1896.

[4] Automatic identification system (AIS) - AIS is a maritime broadcast system, based on the transmission of very high frequency radio signals. Ships send reports with ship identification, position, and course, as well as information on cargo.

[5] Long range identification and tracking (LRIT) - LRIT is a global ship identification and tracking system based on communications satellites. Under International Maritime Organization regulations, passenger ships, cargo ships (300 gross tonnage and above), and mobile offshore drilling units on international voyages send mandatory position reports once every six hours.

[6] In accordance with Article 4(1)(a), first indent, and 4(1)(b) of Regulation 1049/2001.

[7] See correspondence on the Ombudsman's website: https://www.ombudsman.europa.eu/en/correspondence/en/138021 [Link].

[8] The complainant referred to the Judgment of the Court of 11 January 2017 in case C-491/15 P, *Typke v Commission* , paragraph 38, according to which EU institutions may establish a document from information contained in a database by using existing search tools. The judgment is available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186682&pageIndex=0&doclang=EN&mode=lst&dir [Link].

[9] The complainant referred to the Judgment of the Court of Justice of 3 July 2014 in case C-350/12 P, *Council v in 't Veld* , paragraph 52, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=154535&pageIndex=0&doclang=EN&mode=lst&d [Link]

and to the Judgment of the General Court of 7 February 2018 in case T-851/16, *In't Access Info Europe v Commission,* paragraph 37, available at:

https://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dec1c532f0f04b427aa881e31639a740f2

[Link].

[10] In accordance with Article 2(3) of Regulation 1049/2001.

[11] See, for example, judgment of the General Court of 11 July 2018, *ClientEarth v Commission* , T-644/16, paragraphs 23-25, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=203913&pageIndex=0&doclang=EN&mode=lst&dir [Link], and judgment of the Court of 1 February 2007, *Sison v Council* , C¤266/05 P, paragraphs 35-36, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=66056&pageIndex=0&doclang=EN&mode=lst&dir [Link].

[12] Judgment of the General Court of 27 November 2019, *Izuzquiza and Semsrott v Frontex* , T-31/18, paragraphs 72-73, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=221083&pageIndex=0&doclang=EN&mode=lst&d [Link].

[13] See judgment in *Izuzquiza and Semsrott v Frontex* , cited above, paragraphs 76-83.

[14] See also the Ombudsman's decisions in case 1328/2017/EIS, available at: https://www.ombudsman.europa.eu/en/decision/en/86680 [Link], and case 1767/2017/KM, available at: https://www.ombudsman.europa.eu/en/decision/en/85292 [Link].