European Ombudsman

Decision on the European External Action Service's refusal to give public access to documents related to the surveillance system used to secure its buildings (case 1915/2022/OAM)

Decision
Case 1915/2022/OAM - **Opened on** 27/10/2022 - **Decision on** 02/02/2023 - **Institution concerned** European External Action Service (No maladministration found) |

The case concerned the European External Action Service's (EEAS) refusal to give public access to documents related to the surveillance system used to secure its buildings. The EEAS argued that disclosure of the requested documents would undermine the protection of the public interest as regards public security.

The Ombudsman inquiry team met with representatives of the EEAS and inspected the documents to which access was denied. Based on the meeting and the inspection, the Ombudsman found that the EEAS's decision to refuse access was reasonable, given the specific nature and content of the documents.

The Ombudsman closed the inquiry finding no maladministration.

Background to the complaint

1. The complainant is a non-governmental organisation active in the area of civil liberties. In July 2022, it asked the European External Action Service (EEAS) for public access to documents related to the surveillance system used to secure its buildings.

2. More specifically, the complainant requested documents containing the following information:
- *"The number of CCTV cameras in operation in your buildings presently and the number of CCTV Cameras procured since 2017;*
- *The make and model of these CCTV cameras. Aggregate is sufficient (e.g., Company A model 1:10 cameras, Company B model 2:5 cameras…);*
- *Datasheets provided by the vendor/manufacturer of these CCTV cameras;*
- *Invoices, contracts, tenders, service agreements, purchases, orders, procurement documents, offers etc. concerning products and services related to CCTV cameras."*

3. In August 2022, the EEAS replied that the documents requested contain technical details concerning the security setup of its buildings. It refused to provide public access, invoking two exceptions to public access under the EU legislation on access to documents (Regulation 1049/2001). [1] It argued that disclosure would undermine the protection of the public interest as regards public security [2] and the protection of commercial interests of a natural or legal person, including intellectual property. [3] The EEAS did not list the documents identified.

4. The complainant asked the EEAS to review its decision (by making a 'confirmatory application').

5. In October 2022, the EEAS adopted a confirmatory decision, maintaining its position to refuse public access based on the same exceptions initially invoked. It explained that there were 55 documents falling within the scope of the request divided into three categories:
- *"Contractual documents: addendums and contractual price lists, specific contracts and order forms, offers, technical datasheet (30)*
- *Financial documents: invoices and related supportive documents (10)*
- *Operational documents: acceptance documents, reports and inventory files (15)".*

6. Dissatisfied with this outcome, the complainant turned to the Ombudsman in October 2022.

The inquiry

7. The Ombudsman opened an inquiry into the EEAS's refusal to provide public access to the requested documents.

8. In the course of the inquiry, the Ombudsman inquiry team met with the representatives of the EEAS and inspected the 55 documents identified by the EEAS as falling within the scope of the request. The report on the inspection was sent to the complainant, which commented on it.

Arguments presented

9. The **EEAS** argued in its confirmatory decision that the documents contain " *sensitive information related to the CCTV network and technical details pertaining to the security setup deployed to protect the buildings of the European External Action Service and all its assets and staff, located in Brussels* ". The EEAS said it had the duty to protect its staff and assets. Disclosing the information in the documents would expose details about its security system, which could be maliciously exploited by actors with adverse interests to those of the EU.

10. The EEAS noted that it enjoys wide discretion in assessing how disclosure of certain documents could harm public security and no further interests need to be taken into account. [4] The EEAS representatives confirmed in the meeting with the Ombudsman inquiry team that all documents identified as falling within the scope of the request were covered by the exception for the protection of the public interest as regards public security. In addition, some of those

documents were also covered by the exception for the protection of commercial interests of a natural or legal person, because they included, for example, invoices.

11. The **complainant** claims that there is a public interest in knowing *"the manufacturers and, types and models of CCTV systems used by European institutions such as EEAS".* He refers to the public debate around the use of certain CCTV cameras in EU institutions, namely that some manufacturers were allegedly involved in human rights violations in China [5] or that the use of CCTV systems with capabilities such as facial recognition is not clearly regulated in the EU. [6]

12. In his comments on the inspection report, the complainant added that he would be interested in receiving partial access to any parts not covered by the exceptions mentioned above. He also underlined his interest in knowing the brands of the CCTV cameras used by the EEAS.

The Ombudsman's assessment

13. The Ombudsman's inquiry aimed at assessing whether the EEAS's decision to refuse access to the relevant documents was reasonable, given the specific nature and content of the documents.

14. The Ombudsman notes that EU institutions enjoy a wide margin of discretion when determining whether disclosing a document would undermine any of the public interests protected under Article 4(1)(a) of Regulation 1049/2001. [7]

15. The inspection of the documents by the Ombudsman inquiry team showed that they contain highly sensitive information, including the number, locations, brands, types and characteristics of the CCTV cameras in place at the EEAS buildings in Brussels. All of the documents inspected contain one or more of these types of information.

16. The Ombudsman agrees with the EEAS's view that, by disclosing this information, it could expose the security of its buildings to external threats. Knowing the brand of the CCTV cameras, combined with other information obtained from different sources, including public sources, could for example reveal vulnerabilities of the cameras in use and of the security system in general. The Ombudsman therefore finds that it was reasonable for the EEAS to consider that releasing this information could undermine the public interest as regards public security.

17. The Ombudsman assessed whether partial access could be granted in respect of any remaining elements. However, given the nature of the documents and the extent of the redactions that would be required, the Ombudsman believes that no meaningful access could be granted.

18. The complainant argued that there is a public interest in knowing whether certain types of cameras are used.

19. The Ombudsman notes that the exceptions contained in Article 4(1)(a) are absolute and as such they cannot be overridden by the existence of another public interest. This means that, if an institution considers that any of these interests could be undermined by disclosure, they must refuse to give access. Thus, the complainant's arguments concerning a possible overriding public interest in disclosure could not be considered.

20. In reply to the complainant's concerns, the EEAS representatives confirmed in the meeting with the Ombudsman inquiry team that the security procedures in place are in full compliance with EU regulations, including data protection legislation and the legislation of the host Member State (Belgium). The EEAS also confirmed that its security system capabilities do not use facial recognition and that its CCTV cameras were not produced by manufacturers mentioned by the complainant in its complaint to the Ombudsman.

21. The Ombudsman notes that, since the EEAS was justified in refusing access to the documents in order to protect public security, there is no need to take a position on the other exception invoked, namely the protection of commercial interests.

22. In the light of all this, the Ombudsman finds that there was no maladministration in the EEAS's decision to refuse public access to the requested documents.

Conclusion

Based on the inquiry, the Ombudsman closes this case with the following conclusion [8] :

There was no maladministration by the EEAS in refusing public access to the documents at issue.

The complainant and the EEAS will be informed of this decision **.**

Rosita Hickey Director of Inquiries

Strasbourg, 02/02/2023

[1] Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001R1049 [Link].

[2] Article 4(1)(a), first indent of Regulation 1049/2001.

[3] Article 4(2), first indent of Regulation 1049/2001.

[4] The EEAS referred to various EU case law, for example the Judgment of the Court (First Chamber) of 1 February 2007, *Sison v Council* , C-266/05 P, paragraph 34: https://curia.europa.eu/juris/liste.jsf;jsessionid=1BEA842E24526E3574F784C505687403?num=C-266/05&language [Link].

[5] For example, the complainant refers to the European Parliament 2019 Discharge resolution raising concerns about certain companies which should not be part of the EU supply chain, paragraph 74, available at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0165_EN.html [Link].

[6] For example, the complainant refers to articles about the European Parliament position in relation to the Artificial Intelligence Act being negotiated by the co-legislators: https://www.euractiv.com/section/digital/news/ai-act-eu-parliaments-discussions-heat-up-over-facial-recognition-sco [Link] and https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/ [Link].

[7] See in that regard the Judgment of the General Court (Eighth Chamber) of 11 July 2018, *ClientEarth v European Commission,* Case T-644/16, paragraphs 23-25, available at: https://curia.europa.eu/juris/liste.jsf?num=T-644/16&language=en [Link].

[8] This complaint has been dealt with under delegated case handling, in accordance with the Decision of the European Ombudsman adopting Implementing Provisions [Link].