



Emily O'Reilly

European Ombudsman

# Proposal

for a solution on the European Union Agency for Cybersecurity's (ENISA) refusal to give public access to documents related to its follow-up to an investigation by the European Anti-Fraud Office (OLAF) (case 1689/2024/MIG)

made in accordance with Article 2(10) of the Statute of the European Ombudsman<sup>1</sup>

## Background to the complaint

1. One of the tasks of the European Anti-Fraud Office (OLAF) is to conduct independent administrative investigations into serious misconduct by staff and members of the EU institutions. This can, for example, include a failure to seek approval for an outside activity or a failure to notify a conflict of interest. Following its investigations, OLAF can make recommendations for actions to be taken by the EU institution concerned, including 'disciplinary recommendations' aimed to sanction any wrongdoing by staff and members of EU institutions.<sup>2</sup> Through its annual report, OLAF informs the public about the number of disciplinary recommendations it made to the EU institutions concerned in a given period and whether the institutions followed-up on these.<sup>3</sup>

2. The complainant, a journalist, wanted to know more about OLAF's findings and the EU institutions' follow-up decisions in the period 2015 to 2023. To this end, he made several requests<sup>4</sup> for public access to documents to relevant EU institutions, including, in June 2024, to the European Union Agency for Cybersecurity (ENISA), asking for

- *OLAF's final report(s) and recommendations (and related documents), and*
- *the final reports issued by ENISA on the disciplinary follow-up action it had taken.*

3. Between 2015 and 2023, OLAF had conducted one investigation concerning an ENISA staff member based on which it had made two recommendations to ENISA.

<sup>1</sup> Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2021.253.01.0001.01.ENG&toc=OJ%3AL%3A2021%3A253%3ATOC](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.253.01.0001.01.ENG&toc=OJ%3AL%3A2021%3A253%3ATOC)

<sup>2</sup> For more information, visit: [https://anti-fraud.ec.europa.eu/about-us/what-we-do\\_en](https://anti-fraud.ec.europa.eu/about-us/what-we-do_en) or [https://anti-fraud.ec.europa.eu/investigations/internal-administrative-investigations\\_en](https://anti-fraud.ec.europa.eu/investigations/internal-administrative-investigations_en).

<sup>3</sup> See, for example, the OLAF report 2021, page 52: [https://anti-fraud.ec.europa.eu/document/download/8d92a187-fae8-449f-8600-e84af9b2dabf\\_en?filename=olaf-report-2021\\_en.pdf](https://anti-fraud.ec.europa.eu/document/download/8d92a187-fae8-449f-8600-e84af9b2dabf_en?filename=olaf-report-2021_en.pdf).

<sup>4</sup> Under Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents: <http://data.europa.eu/eli/reg/2001/1049/oj> applicable to documents held by ENISA according to Article 28(1) of Regulation 2019/881 on ENISA and on information and communications technology cybersecurity certification: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.



4. ENISA refused to give public access to the OLAF report “*and related information*”, relying on the need to protect the personal data of the person concerned in the OLAF investigation and of other individuals.<sup>5</sup> ENISA did not specify what documents it had identified as falling within the scope of the complainant’s access request.

5. The complainant challenged ENISA’s decision to refuse access (by making a ‘confirmatory application’). He did not challenge the redaction of personal data of individuals other than the person concerned in the OLAF investigation.

6. In reply, ENISA maintained its position that no public access could be granted to the documents at issue as disclosure of the documents, even in part, would undermine the protection of personal data.<sup>6</sup>

7. Dissatisfied with this outcome, the complainant turned to the Ombudsman.

## The inquiry

8. The Ombudsman opened an inquiry into ENISA’s decision to refuse to give public access to the documents at issue to the extent that they do not constitute personal data of individuals other than the person concerned in the OLAF investigation.

9. In the course of the inquiry, the Ombudsman received ENISA’s reply to the complaint, including confidential information. The Ombudsman inquiry team also held a meeting with a representative of ENISA and inspected the documents at issue, that is,

- 1) the OLAF final report and the annexes to it,
- 2) two recommendations issued by OLAF, and
- 3) three documents related to ENISA’s follow-up [REDACTED]

as well as related documents.

## Arguments presented

10. The **complainant** argued that disclosure was of significant public interest for the following reasons: it would (i) illustrate the EU’s commitment to the principles of transparency and accountability, (ii) enhance public trust in the EU institutions’ integrity by demonstrating that misconduct is addressed effectively), and (iii) contribute to improving policies and procedures related to staff conduct.

11. ENISA took the view that the documents at issue constitute personal data in their entirety. In other words, even if it were to redact identifiers such as names and operational data, the remaining information might still risk that the person concerned be identified.

---

<sup>5</sup> In accordance with Article 4(1)(b) of Regulation 1049/2001.

<sup>6</sup> In accordance with Articles 4(2), first indent, of Regulation 1049/2001.



**12.** As ENISA considered that the complainant had not established that there is a need for disclosure of the personal data in the public interest (a ‘necessity’), it concluded that no public access was possible.

## The Ombudsman's assessment

**13.** The concept of ‘personal data’<sup>7</sup> is very broad. It covers any information related to an identified or identifiable person. The information does not need to be linked to a person’s private life. Information concerning a person’s professional activity can also constitute personal data, namely if it allows for the identification of the individual concerned.

**14.** It was therefore reasonable for ENISA to consider that “*identifiers such as the name*” of the person concerned in the OLAF investigation as well as certain operational information related to this individual constitute personal data.

**15.** However, based on the inspection of the documents by the inquiry team and the information provided by ENISA, the Ombudsman considers that the documents do not constitute personal data throughout. Rather, it would seem that certain parts could be disclosed whilst protecting the privacy and integrity of the person concerned. More specifically, the Ombudsman finds that information related to the kind of misconduct that was found by OLAF as well as the kind of follow-up measure taken by ENISA as such do not reasonably qualify as personal data. It would seem that, on its own, this information is not likely to allow for the identification of the person concerned.

**16.** As regards such general information, the Ombudsman therefore considers that ENISA was not justified in relying on the need to protect the privacy and integrity of the individual concerned in refusing public access to the documents in their entirety. The Ombudsman will therefore make a corresponding proposal for a solution below.

**17.** Concerning the parts of the documents that do contain personal data, any disclosure must fulfil the conditions for transfer of personal data set out in the EU rules on data protection (Regulation 2018/1725<sup>8</sup>). According to these rules, EU institutions must follow a three-stage analysis in considering whether they can grant public access.<sup>9</sup> First, they must assess whether the applicant established a specific need for disclosure of the personal data that is in the public interest. Second, if such ‘necessity’ exists, they must assess whether disclosure might undermine the legitimate interests of the individual(s) concerned. Third, if this is the case, they must establish that, in light of the objective pursued by the applicant, disclosure would be proportionate nevertheless.

**18.** As regards the need for disclosure, the complainant argued, in essence, that the documents at issue should be disclosed so as to ensure transparency, accountability and public trust, and to improve the EU’s policies and procedures related to staff conduct.

---

<sup>7</sup> Article 3(1) of Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data: <https://eur-lex.europa.eu/eli/reg/2018/1725/oj/eng>.

<sup>8</sup> See footnote 7 above.

<sup>9</sup> Article 9(1)(b) of Regulation 2018/1725.



**19.** Whilst the Ombudsman considers that the objective pursued by the complainant is legitimate, she is not convinced that disclosure of the identity of the person concerned would be necessary to achieve it. In particular, as noted above, the Ombudsman considers that parts of the documents at issue do not reasonably constitute personal data. They are therefore not covered by the exception for the protection of personal data and should, thus, have been disclosed by ENISA. What is more, disclosure of this information would allow for public scrutiny and could also inform a debate on rules and procedures related to staff conduct.

**20.** In addition, staff members who breach their obligations under the EU Staff Regulations<sup>10</sup> do not forfeit their right to privacy. Such misconduct is addressed by the relevant administrative procedures, including investigations by OLAF and possible disciplinary measures. As the inspection showed, these procedures have been applied here.

**21.** In light of this, the Ombudsman finds that the complainant did not establish a necessity for disclosure of the personal data at issue, as required by Regulation 2018/1725.

**22.** The assessment of the second and third stages of the test described above in relation to the personal data at issue is therefore obsolete.

## The proposal for a solution

**Based on the above findings, the Ombudsman proposes that ENISA should re-consider its decision to refuse public access with a view to providing meaningful partial access to the requested documents, whilst protecting the privacy and integrity of the individuals concerned.**

ENISA is invited to inform the Ombudsman by 26 May 2025 of any action it has taken in relation to the above solution proposal.

Emily O'Reilly  
European Ombudsman

Strasbourg, 24/02/2025

---

<sup>10</sup> Regulation 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community:  
[http://data.europa.eu/eli/reg/1962/31\(1\)/2014-05-01](http://data.europa.eu/eli/reg/1962/31(1)/2014-05-01).