



Decision in case 1731/2018/FP on the refusal by the Innovation and Networks Executive Agency to grant public access to the documents submitted by a public undertaking for a funding approval in the context of a call for proposals by the Connecting Europe Facility

Decision

Case 1731/2018/FP - Opened on 10/10/2018 - Recommendation on 01/04/2019 - Decision on 04/10/2019

The case concerned the refusal by the Innovation and Networks Executive Agency (INEA) to grant public access to documents submitted by a national cybersecurity authority that was seeking funding from INEA.

The Ombudsman inquired into the issue and proposed that INEA should partially disclose the requested documents, redacting only information that it considers to be genuinely commercially sensitive or personal data.

INEA rejected the Ombudsman's proposal, arguing that most of the information that could be disclosed was already in the public domain and the proposed partial disclosure would impose a disproportionate administrative burden on INEA. It also said that it accepted the arguments of the national cybersecurity authority regarding the likely damage disclosure would cause to its commercial interests.

The Ombudsman found INEA's refusal to grant even partial access to the requested documents to be maladministration and recommended that INEA partially disclose the relevant Grant application.

INEA rejected the Ombudsman's recommendation. Consequently, the Ombudsman now closes the case, confirming her finding of maladministration.

Background to the complaint

1. On 26 July 2018, the complainant asked the Innovation and Networks Executive Agency (INEA), to grant him public access to the complete documentation submitted by a public body (the national cybersecurity authority of a Member State) seeking funding from INEA. [1]

2. On 1 August 2018, INEA replied to the complainant identifying the requested documents as the Grant application forms A to D. It refused to grant him public access on the basis of the commercial interests exception in Article 4(2), first indent, and the personal data



exception in Article 4(1)(b) of Regulation 1049/2001. [2]

3. On the same day, the complainant made a request for review (a so called “ *confirmatory application* ”) requesting INEA to review its previous refusal and to grant him public access to the requested documents.

4. On 7 August 2018, INEA consulted the national cybersecurity authority in accordance with Article 4(4) of Regulation 1049/2001.

5. On 21 August 2018, INEA confirmed its previous decision refusing public access to the requested documents.

6. On 7 October 2018, the complainant submitted a complaint to the Ombudsman. The Ombudsman then opened an inquiry.

The Ombudsman's proposal for a solution

7. In the course of the inquiry, the Ombudsman noted that INEA consulted the national cybersecurity authority from which the documents originated on the possibility of disclosing the requested documents. When doing so, INEA made a proposal for partial disclosure, indicating the information it thought should be redacted (because it was commercially sensitive or contained personal data), and invited the national cybersecurity authority to provide its views on the suggested disclosure. The national cybersecurity authority indicated that it was not in agreement with the disclosure of the documents.

8. The Ombudsman noted that INEA was not bound by the national cybersecurity authority's opinion, as established in the case *Terezakis v Commission* . [3]

9. The Ombudsman found that the requested documents contained some information of commercial value and agreed that disclosing this would be likely to create an unfair advantage in future calls for tenders and proposals. The complainant did not establish an overriding public interest in disclosure that would justify denying the protection of this commercial interests. Thus, the Ombudsman found that this information should be considered commercially sensitive, in accordance with Article 4(2), first intent, of Regulation 1049/2001.

10. However, the documents also contained some information which did not appear to be commercially confidential. This was general information about the project, in line with the publicly available call for proposals. [4] The Ombudsman noted that not only was the call for proposals already publicly available, but so too was the project information, as confirmed by the complainant [5] and INEA [6] . The Ombudsman concluded that this information was not sensitive and its disclosure would not undermine the public undertaking's commercial interests nor the intellectual property rights.

11. As regards the redacted personal data, the Ombudsman considered that the complainant



had not established the necessity of having personal data transferred [7] and agreed that the personal data in the requested documents should be redacted, in line with Article 4(1)(b) of Regulation 1049/2001 and Article 8(b) of Regulation 45/2001.

12. Consequently, the Ombudsman proposed that INEA should partially disclose the relevant Grant application forms A and D, redacting only information that it considered to be genuinely commercially sensitive or personal data. The Ombudsman suggested that INEA's initial proposal for partial disclosure (made in the course of the consultations with the public undertaking) was the appropriate basis on which to proceed.

The Ombudsman's recommendation

13. INEA rejected the Ombudsman's proposal for partial disclosure. INEA noted that information on the scope and objectives of the project is already publicly available and "basically coincides" with the information included in the parts of the documents that the Ombudsman proposed should be disclosed. It argued that the administrative burden of implementing the Ombudsman's proposal would be too high, and that partial access would be meaningless since the information that could be disclosed was already public. [8]

14. INEA also stressed that the project concerns cybersecurity, which is an area where confidentiality is essential. It argued that if the requested documents were to be disclosed, trust between the Commission and the relevant implementing actors would be breached and could lead to reluctance to apply for the grants in the future. It said that such actors provide, in their project proposals, details on their personnel and operations which, if disclosed, would enable external entities to understand their functioning. In addition, it noted that some of the implementing actors are part of the security and intelligence infrastructure of the Member States. As a result, it argued that disclosure could also damage the cybersecurity of the Member States through targeted cyber-attacks.

15. The Ombudsman considered that the implementation of her proposal would not impose an additional administrative burden on INEA, since INEA had already made an initial proposal for partial disclosure when consulting the relevant national cybersecurity authority.

16. The Ombudsman also considered that the fact that information is already in the public domain does not mean that public access to the requested documents would be pointless. She noted that disclosure could only be deemed meaningless, or pointless, if the redactions are so extensive as to render a document "*entirely deprived of its content*". [9] This is not so in the present case. If any conclusion is to be drawn from the fact that certain information in the documents is already in the public domain, it is that the interests protected by Regulation 1049/2001 cannot be undermined by the disclosure of that information.

17. The Ombudsman noted that her proposal for public disclosure concerned information that cannot be considered sensitive, such as the scope and objectives of the project, its relevance and the descriptions of activities. The redaction of information which may be commercially sensitive or contain personal data is justified. [10] Therefore, the Ombudsman



found that partial disclosure of the requested documents would not undermine the trust between the Commission and the public undertaking.

18. The Ombudsman also found that national cybersecurity could not be undermined by partial disclosure, since the parts of the documents which should be disclosed contain information that is already public. In any event, that information does not contain detailed technical information which would enable external entities to understand the functioning of the national cybersecurity agencies and consequently damage the Member States' cybersecurity.

19. In light of the above, the Ombudsman found that INEA's refusal to grant partial access to the documents constituted maladministration. She therefore made the following recommendation (in accordance with Article 3(6) of the Statute of the European Ombudsman):

"The Innovation and Networks Executive Agency should partially disclose the requested Grant application forms A and D, redacting only information that is genuinely commercially sensitive or is personal data requiring protection."

INEA's reply to the Ombudsman's recommendation

20. INEA rejected the Ombudsman's recommendation. It argued that EU Courts recognise a general presumption of non-disclosure for tenders [11], which by analogy also applies to grant award procedures. It said that the European Commission's proposed practice is to refuse access to documents requests concerning grant applications on the grounds of protecting commercial interest and privacy.

21. INEA asserted that its initial suggestion for partial disclosure was *"merely a basis to initiate discussions and not a final position of the Agency."* It now considers that deleting the sensitive information would make the disclosed part of the document meaningless. It also said that the redacted documents would be meaningless to the complainant, since the information is already publicly available. INEA stated that EU Courts have judged that institutions are allowed to refuse partial access in such cases [12].

22. INEA claimed that since the non-sensitive information is spread out in the requested documents, *"a partial deletion would involve a serious risk that punctual release of publicly available elements could still lead to a disclosure of sensitive information"*. It also noted that the Commission and itself were concerned that a possible confidentiality breach on cybersecurity could undermine the trust of the national cybersecurity authority in question, as well as future collaboration partners.

23. INEA argued that transparency and the participation of citizens in the decision-making process cannot be used as an argument for an overriding public interest in disclosure in this case, since grants applications are not part of the legislative procedure.



The Ombudsman's assessment after the recommendation

24. The Ombudsman is disappointed with INEA's reply to her recommendation.

25. She finds INEA's new argument for refusing partial access based on a general presumption of non-disclosure of tenders/grants to be not convincing. Without necessarily accepting that such a general presumption applies, the Ombudsman notes that all general presumptions regarding under EU access to documents rules are subject to rebuttal. The Ombudsman has clearly explained why certain information in the documents cannot be considered confidential. As such, any general presumption that might be applicable as regards tender bids is rebutted in this case.

26. It is also clear from INEA's confirmatory decision and subsequent correspondence with the Ombudsman that INEA has already carried out an individual assessment of the requested documents and identified the parts of the document that are subject to exceptions under Regulation 1049/2001 and other parts that are already in the public domain.

27. Moreover, the Ombudsman disagrees with INEA's assessment that releasing a redacted version of the documents would be meaningless in this case. While some of the non-sensitive information in the requested documents is already available to the public, the (partial) release of the document might help the complainant to ascertain if the grant application **contains the same information that is already publicly available**. Even a redacted version of the documents would therefore be somewhat useful to the complainant.

28. On the basis of the above the Ombudsman reaffirms her conclusion that the INEA's refusal to grant partial public access to the documents in question constituted maladministration.

Conclusion

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

The Ombudsman is not satisfied with Innovation and Networks Executive Agency's response to her recommendation that the Innovation and Networks Executive Agency should partially disclose the requested Grant application forms A and D and confirms her finding of maladministration.

The complainant and the Innovation and Networks Executive Agency will be informed of this decision .

Emily O'Reilly

European Ombudsman



Strasbourg, 04/10/2019

[1] The funding was related to Enhanced National Cyber Security Services and Capabilities for Interoperability (eCSI), Action 2016-RO-IA-0128, available at INEA's website: <https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-ro-ia-0128> ; Call for proposals concerning projects of common interest under the Connecting Europe Facility in the field of trans-European Telecommunication networks, CEF-TC-2016-3: Cyber Security, available at:

https://ec.europa.eu/inea/sites/inea/files/2016-3_ceftelecom_calltext_cybersecurity_200916_final.pdf , Annex, Work programme 2016, available at: https://ec.europa.eu/inea/sites/inea/files/wp2016_adopted_20160303.pdf .

[2] Regulation 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R1049&rid=1> .

[3] Judgment of the Court of First Instance of 30 January 2008 in *Terezakis v Commission* , T-380/04.

[4] Call for proposals concerning projects of common interest under the Connecting Europe Facility in the field of trans-European Telecommunication networks, CEF-TC-2016-3: Cyber Security, available at:

https://ec.europa.eu/inea/sites/inea/files/2016-3_ceftelecom_calltext_cybersecurity_200916_final.pdf , Annex, Work programme 2016, available at: https://ec.europa.eu/inea/sites/inea/files/wp2016_adopted_20160303.pdf .

[5] Contract notice, 2018/S 019-040409, available at:

<https://ted.europa.eu/udl?uri=TED:NOTICE:040409-2018:TEXT:RO:HTML> .

[6] INEA's website, available at:

<https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-ro-ia-0128> ,

<https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2016-cef-telecom-cal>

; the public undertaking's website, available at: <https://www.cert.ro/pagini/ecsi-page> ; the

project dedicated website, available at: <https://ecsi.cert.ro/> ; the Romanian Public

Procurement System/Platform, available at: www.e-licitatie.ro ; and Tenders Electronic Daily,

available at: www.ted.europa.eu .

[7] In accordance with Article 2(a) of Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, available at:

<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045> .



[8] INEA makes reference to the Judgments of the Court of First Instance of 12 July 2001 in *Mattila v Council and Commission* , T-204/99, paragraph 69 and of 20 March 2014; in *Reagens v Commission* , T-181/10, paragraph 161-175; judgments of the Court of First Instance of 19 July 1999 in *Hautala v Council* , case T-14/98 paragraph 30 and of 7 February 2002 in *Kuijter v Council* , T-211/00, paragraph 57.

[9] See *Reagens v Commission* , T-181/10, paragraph 172 and 175.

[10] In accordance with Articles 4(1)b and 4(2), first indent, of Regulation 1049/2001.

[11] For example, Judgment of the General Court of 26 May 2016, *International*

Management Group v European Commission, Case T-110/15, paragraph 30 and Judgment of the General Court of 13 November 2015, *ClientEarth v European Commission* , T-424/14 and T-425/14, paragraph 65.

[12] Judgement of the General Court of 12 July 2001, *Mattila v Council and Commission* , Case T-204/99, paragraph 69.