Europäische Ombudsstelle

Entscheidung im Fall 987/2020/EWM über den Umgang des Europäischen Auswärtigen Dienstes mit Bedenken in Bezug auf ein sicheres Instant-Messaging-System und eine potenzielle Datenschutz-Folgenabschätzung sowie einen Antrag auf Zugang der Öffentlichkeit zu den entsprechenden Dokumenten

Entscheidung
Fall 987/2020/EWM - **Geöffnet am** 11/06/2020 - **Entscheidung vom** 15/09/2020 - **Betroffene Institution** Europäischer Auswärtiger Dienst (Kein Missstand festgestellt) |

Die Beschwerde betraf die Weigerung des Europäischen Auswärtigen Dienstes (EAD), den Zugang der Öffentlichkeit zu Dokumenten über ein sicheres Instant-Messaging-System zu gewähren, das für den Austausch von sensiblen Informationen und Verschlusssachen innerhalb des EAD verwendet wird. Der EAD hat erklärt, dass die Offenlegung der Dokumente die öffentliche Sicherheit gefährden würde.

Die Bürgerbeauftragte hat den Inhalt der Dokumente geprüft und ist auf dieser Grundlage ebenfalls der Auffassung, dass der EAD Grund hatte, den Zugang der Öffentlichkeit zu verweigern. Sie konnte daher keinen Missstand feststellen und schloss den Fall ab.

Background to the complaint

1. The European External Action Service (EEAS) requires its employees to use secure systems when exchanging sensitive and classified information among themselves. One such system is a secure instant messaging system. That system is an integral part of the 'EU Restricted' classified communication system of the EEAS.

2. The complainant requested public access to documents related to this instant messaging solution that the EEAS has deployed since September 2019, including contracts with external suppliers. He also asked for access to the Data Protection Impact Assessment (DPIA) for the classified communication system. [1] [Link]

3. The EEAS refused to disclose the requested documents for security reasons and explained that no DPIA existed.

4. The complainant was not satisfied with the EEAS's view as set out in its confirmatory decision and turned to the Ombudsman.

The inquiry

5. The Ombudsman opened an inquiry into the EEAS's refusal to grant public access to the requested documents. In the course of the inquiry, the Ombudsman's inquiry team met with relevant staff of the EEAS and inspected the documents requested by the complainant.

Arguments presented to the Ombudsman

6. The EEAS explained that it could not disclose details of its secure communications devices, infrastructure and networks. The public release of such details would compromise that security in that releasing the documents would make the system more prone to cyberattacks. Therefore, the release of the documents would undermine public security. [2] [Link]

7. The EEAS confirmed that no DPIA had been prepared regarding the instant messaging solution.

8. The complainant stated that he takes issue with the blanket and wholesale refusal of his request. He acknowledged that disclosure of details of the secure communications platform has to be limited to a certain extent. However, the EEAS should disclose basic information about what kind of software and systems architecture the EEAS uses, about procurement of the software, as well as what type of protocols and encryptions it uses. In his view, providing such information is standard practice in IT security even for means of exchanging highly confidential information.

9. He argued that procurement information should be available to the same extent as in other EU public procurement contracts, with the exception of specific sensitive information.

10. The complainant pointed out that in the absence of a DPIA, the Ombudsman should refer the case to the European Data Protection Supervisor (EDPS) to check if it agrees that such a large-scale communications platform handling highly sensitive data really does not need a Data Protection Impact Assessment.

The Ombudsman's assessment

11. EU institutions have a **broad margin of discretion** when assessing whether or not the disclosure of a document could jeopardise public security. [3] [Link]

12. The EEAS stated that the public disclosure of details concerning the secure communication system would compromise security by making the system more prone to cyberattacks. Having

carefully inspected the categories of documents requested by the complainant, the Ombudsman agrees that the disclosure of the documents would undermine public security.

13. The documents contain sensitive information throughout. Granting meaningful partial access is not possible.

14. The Ombudsman thus concludes that the EEAS was entitled not to disclose the requested documents.

15. As regards the complainant's request for access to a possible DPIA, the EEAS has confirmed that no such document exists.

16. The complainant is of the view that, if no DPIA exists, the EDPS should examine the issue as regards compliance with data protection rules. The Ombudsman thus advises the complainant to pursue this matter with the EDPS.

Conclusion

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

There was no maladministration by the European External Action Service in refusing access to the requested documents.

The complainant and the European External Action Service will be informed of this decision **.**

Emily O'Reilly European Ombudsman

Strasbourg, 15/09/2020

[1] [Link] According to Article 39(1) of Regulation (EU) 2018/1725, which concerns the protection of natural persons with regard to the processing of personal data by the Union institutions, "[w] *here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data* ".

[2] [Link] Exception to the right to public access to documents in accordance with Article 4(1)(a) of Regulation 1049/2001, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001R1049 [Link].

[3] [Link] Judgment of the Court of 1 February 2007, Sison v Council, C-266/05 P, available at: http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-266/05%20P&td=ALL [Link].