Council of the
European Union

Brussels, 30 September 2024
(OR. en)

12945/24

LIMITE

API 108
INF 216

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	12944/24
Subject:	Public access to documents - Confirmatory application No 24/c/04/24

Delegations will find attached a draft reply to confirmatory application No 24/c/04/24 (see 12944/24).

ANNEX

REPLY TO CONFIRMATORY APPLICATION 24/c/04/24
made by email on 31 August 2024 and registered on 2 September 2024

The Council has considered the confirmatory application under Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents and Annex II to the Council's Rules of Procedure and has come to the following conclusion:

1. This confirmatory application concerns the following documents: **ST 8155/23, WK 3449/2022, WK 10607/2022, WK 3170/2023 ADD 3, ADD 4 and ADD 5, WK 8586/2023,** a **Powerpoint presentation from the European Union Agency for Cybersecurity (ENISA)** and **ten working documents** containing listings of cyber-related equipment and services related to capacity development, including, among others, references to the use of Starlink in Ukraine.

2. In its reply to the Applicant on 30 August 2024, the General Secretariat refused access to the abovementioned documents on the ground of Article 4(1)(a), first, second and third indent of Regulation (EC) No 1049/2001 (protection of public security, defence and military matters, and international relations). Moreover, the refusal of document WK 10607/2022 was also motivated by Article 4(2), third indent (protection of the purpose of inspections, investigations and audits).

3. In his confirmatory application on 31 August 2024, the Applicant asked to review the General Secretariat's position, arguing in essence that its refusal to grant access was not explicitly based on a specific reasoning regarding the content of the documents in question and that the risk of jeopardizing international relations must be reasonably foreseeable and not purely hypothetical.

ASSESSMENT OF THE REQUESTED DOCUMENTS UNDER REGULATION (EC) No 1049/2001

4. Following to re-examination of the documents concerned and new consultations with their authors, the Applicant may have full access to **the presentation of ENISA** dated 19 April 2024 ("outline of the Nevers Report and Leo Satcom Cyber Security") and to document **WK 8586/2023**, presentation of the European Commission to the Horizontal Working Party on Cyber Issues on 23 June 2023 ("Update on the US TTC ministerial").

5. In the Council's view, the content of the following sixteen documents is covered by the exceptions to disclosure raised in reply to the initial request as their release would create a reasonably foreseeable risk of undermining public interest as regards public security, defence and military matters and the Union's international relations in the sense of Article 4(1)(a), first, second and third indent of Regulation (EC) No 1049/2001. These documents are:

- **ST 8155/23**, dated 5 April 2022, working document focusing on the topic European Union Military Committee (EUMC) and focusing on the topic "EUMC Strand D input to the EDA Capability Development Plan 2023 revision"
- **WK 3449/2022,** presentation of the European Commission to the Working Party on Space meeting on 9 March 2022 on the topic "Secure Connectivity Programme: Impact Assessment"
- **WK 10607/2022**, working document dated 19 July 2022, drawn up by the European Commission in liaison with the EEAS, Eurojust and Europol and containing information on the Ukraine's needs for the prosecution of war crimes and corresponding initiatives
- **WK 3170/2023 ADD 3, ADD 4 and ADD 5,** working documents dated respectively 21 March 2023, 29 March 2023 and 3 April 2024 drawn up by the EUMC and focusing on the abovementioned "EUMC Strand D input to the EDA Capability Development Plan 2023 revision"
- Ten tables produced by different sources:
  - A joint table dated 14 March 2022, drawn up by the European External Action Service (EEAS) and the European Commission and containing a list of cyber-related equipment and services
  - Six tables dated respectively 25 March 2022, 1 April 2022, 8 April 2022, 29 April 2022, 6 May 2022 and 23 June 2022, drawn up by the EEAS and containing information on the abovementioned topic, collected from different national sources
  - A table dated 28 March 2022 and its revised version dated 29 March 2022, drawn up by the former French presidency and containing a list of IT equipment
  - A table dated 14 June 2022 prepared by the European Commission and listing cyber-related equipment and services.

6. The Council recalls that, in accordance with the established case-law of the Court of Justice, the public interest exceptions laid down in Article 4(1)(a) of Regulation (EC) No 1049/2001 are subject to a particular regime as compared to the other exceptions included in Article 4.

7. On the one hand, "*in respect of the public interest exceptions provided for in Article 4(1)(a)*" of Regulation (EC) No 1049/2001, the Council must be recognised as "*enjoying a wide discretion for the purpose of determining whether disclosure of a document to the public would undermine the interests protected by that provision*". [1]

8. On the other hand, once the Council has come to the conclusion that the any release would indeed undermine the public interest in this area, it has no choice but to refuse access, because "*it is clear from the wording of Article 4(1)(a) of Regulation No 1049/2001 that, as regards the exceptions to the right of access provided for by that provision, refusal of access by the institution is mandatory where disclosure of a document to the public would undermine the interests which that provision protects, without the need, in such a case and in contrast to the provisions, in particular, of Article 4(2), to balance the requirements connected to the protection of those interests against those which stem from other interests*". [2]

9. Therefore, while the Council enjoys a wide discretion in assessing the impact of the release of documents on international relations, it is barred from taking into account other legitimate interests that might override the conclusion that giving access to a document or parts of a document would harm the abovementioned protected interest.

10. Besides, for the purpose of the assessment of a request for access to documents under Regulation (EC) No 1049/2001, it is not required to establish the existence of a definite risk of undermining the protection of public security, defence and military matters and the EU's international relations (*the three exceptions being crucial to justify refusing full disclosure of each of the documents concerned*), but rather the existence of a reasonably foreseeable and not purely hypothetical risk[3] for which, as previously recalled, the institution enjoys a margin of discretion.

---

[1] Judgments of 11 July 2018, *ClientEarth v Commission*, T-644/16, paragraph 25, and of 27 November 2019, *Izuzquiza and Semsrott v European Border and Coast Guard Agency (FRONTEX)*, T-31/18, paragraph 65.

[2] Judgment of 1 February 2007, *Sison v Council*, C-266/05, paragraph 46; and similarly judgment of 7 February 2018, *Access Info Europe v Commission*, T-851/16, paragraph 38.

[3] Judgment of 25 November 2020, *Bronckers v Commission*, T-166/19, paragraph 60.

11. It also results from the above that the Council has no choice but to refuse access to a document that falls within the scope of the abovementioned exception, the public disclosure of which would undermine the public interests protected by them.

12. After carefully considering all the principles related to this request, and given their sensitive contents (focused on EU military capacity building and detailed description of IT and cyber-related equipment and services needed by Ukraine to counter the continuous threats of Russia in the current war scenario), on balance the Council has concluded that the disclosure of these documents would seriously jeopardize the EU's ongoing activities aiming at strengthening the capabilities of the Ukrainian armed forces and provide military assistance and training in this field.

13. In particular, the release of these documents to the public would enable EU's adversaries to acknowledge the range of material and services provided to Ukraine and target those areas where that country needs to reinforce its capacities and resources, with a potential impact on the current hostilities and on the effectiveness of the ongoing EU's assistance. Hence, disclosure would have negative consequences for safety and security.

14. Moreover, the release of these documents would have a negative impact on mutual trust between the EU and its international partners, seriously weakening the confidential cooperative framework in the field.

15. Furthermore, the Council considers that the content of document **WK 10607/2022** is also covered by the exception of Article 4(2), third indent (purpose of inspections, investigations and audits), since it contains sensitive data on assistance requested by Ukraine. This document contains lists of logistical/technical requirements (also including forensic expertise) for the prosecution of war crimes investigations. If released to the public, this information would enable hostile entities to acknowledge critical areas in this field and the EU's envisaged support in progress, threatening the efficiency and effectiveness of the EU's assistance and its cooperation with Ukrainian authorities in this field.

16. The Council is not in a position to describe in more detail the harm that would be caused by the release of the requested documents, as this would necessarily entail disclosure of part of the very information of sensitive nature protected by the three exceptions concerned.

17. In the light of the above, the Council considers that public access to these documents would generate a highly concrete risk of causing prejudice to public interest as regards public security, defence and military matters, and international relations.[4]

18. The Council has also looked into the possibility of releasing parts of the sixteen documents in line with Article 4(6) of Regulation (EC) No 1049/2001 and has found that:

    a. the exceptions referred to in point 17 apply to the entire content of documents **ST 8155/23, WK 10607/22, WK 3170/2023 ADD 3, ADD 4 and ADD 5** and to **the abovementioned ten working documents;**

    b. document **WK 3449/2022** can be released partially, whilst pages 6 to 10 and 22 to 28, containing respectively a detailed outline of an entrusted security satellite study and Member States' questions/comments on, among others, evidence material, roadmaps, budget and prioritized areas cannot be disclosed. If acknowledged by hostile entities, that content could be used to target and weaken sensitive areas of strategic cooperation threatening EU and Ukraine security and defence plans and causing prejudice to the EU's international relations.[4]

CONCLUSION

19. The Council therefore considers that:

    a. the **ENISA presentation on 19 April 2024** and document **WK 8586/2023** can be released at this stage in their entirety;

    b. document **WK 3449/2022** can be released partially, the remaining content being refused on the ground of Article 4(1)(a), first, second indent and third indent of Regulation (EC) No 1049/2001;

    c. public access to documents **ST 8155/23, WK 10607/2022, WK 3170/2023 ADD 3, ADD 4 and ADD 5 and the abovementioned ten working documents** containing lists of cyber-related equipment and services must be refused in their entirety on the ground of Article 4(1)(a), first, second and third indent of Regulation (EC) No 1049/2001. Public access to document **WK 10607/2022** is also refused on the ground of Article 4(2), third indent of Regulation (EC) No 1049/2001.

---

[4] Article 4(1)(a), first, second and third indent of Regulation (EC) No 1049/2001.