



**Council of the European Union**

General Secretariat

Directorate-General Communication and Information - COMM

*The Director-General*

Brussels, 4 November 2020

**SGS 20/2341**

Mr Stefan Soesanto

Stefan Soesanto <ask+request-8434-5726548f@asktheeu.org>

**Subject:** Your Confirmatory Application 21/c/01/20

Dear Mr Soesanto,

Please find enclosed the reply from the Council to the Confirmatory Application you introduced on 22 September 2020 and which was registered by our service on the same day.

Yours sincerely,

Reijo KEMPPINEN

Enclosures: 2

**REPLY ADOPTED BY THE COUNCIL ON 4 NOVEMBER 2020  
TO CONFIRMATORY APPLICATION 21/c/01/20,  
made by email on 22 September 2020 and registered on the same day  
pursuant to Article 7(2) of Regulation (EC) No 1049/2001,  
for public access to document 5807/19**

The Council has considered this 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 (OJ L 145 of 31.5.2001, p. 43) (hereafter "Regulation No 1049/2001") and Annex II to the Council's Rules of Procedure (Council Decision 2009/937/EU, Official Journal L 325, 11.12.2009, p. 35) and has come to the following conclusion:

1. On 8 August 2020 the applicant introduced an initial application (registered on 10 August) for access to, among others, document **ST 5807/19** which is a Note drawn up by the European External Action Service focusing (EEAS) on the Cyber Diplomacy Toolbox and tabling options for a restrictive measures framework to respond to or deter cyber activities that threaten the security or foreign policy interests of the Union or its Member States.
2. In its reply dated 21 September 2020, the General Secretariat of the Council (GSC) refused to grant access to this document on the ground of Article 4(1), third indent of Regulation (EC) No 1049/2001 (protection of public interest with regard to international relations) and Article 4(3), second subparagraph of the abovementioned Regulation (protection of the decision-making process of the Council).
3. On 22 September 2020, the applicant introduced a confirmatory application, arguing in substance that:
  - qualifying the content of the requested document as sensitive, though it does not bear a classified marking, is not a sufficient reason to refuse access;
  - the General Secretariat has not explained in detail what would be the harmful consequences of disclosure;

- having regard to the time lapse since the production of the requested document, knowing at this stage the details of the options tabled by the EEAS would not undermine either the effectiveness and impact of future sanction regimes or the flexibility in decision-making, whereas there is a public interest (for academic research purposes, the interest of transparency as a whole, and EU citizen education purposes) in understanding the EU decision-making processes on cyber sanctions.
4. The Council has carefully considered the confirmatory application. Having thoroughly scrutinized the requested document in the light of the arguments brought forward by the applicant and after carrying out new consultations with the European External Action Service who authored the document, it has re-assessed whether, in full consideration of the principles underlying Regulation (EC) No 1049/2001, in particular the aim of ensuring the widest possible public access to documents, full public access or extended partial access can be provided at this stage.

#### **PRELIMINARY REMARKS ON THE EXCEPTION CONCERNING THE PROTECTION OF THE PUBLIC INTEREST AS REGARDS INTERNATIONAL RELATIONS**

5. Based on its content, the requested document comes within the remit of the exception of protection of the public interest as regards international relations (Article 4(1)(a), third indent of Regulation (EC) No 1049/2001).
6. At the outset, the General Secretariat recalls that, in accordance to 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, *"the Council must be recognised as enjoying a wide discretion for the purpose of determining whether the disclosure of documents relating to the fields covered by those exceptions relating to the public interest provided for in Article 4(1)(a) of Regulation (EC) No 1049/2001 could undermine the public interest"*.<sup>1</sup>

---

<sup>1</sup> ECJ case C-266/05, Sison, para. 34.

8. On the other hand, once the Council has come to the conclusion that 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 (EC) 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*".<sup>2</sup>
9. Therefore, the Council enjoys a wide discretion in assessing the impact of the release of documents on international relations, but is barred from taking into account other legitimate interests in order to override the conclusion that giving access to a document would harm the protected interest and grant access nonetheless.
10. 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 exceptions, the public disclosure of which would undermine the public interest protected by them.

#### **ASSESSMENT OF THE HARM TO PROTECTED INTERESTS THAT WOULD ENSUE FROM FULL DISCLOSURE OF THE REQUESTED DOCUMENT**

11. The requested document relates to the Common Foreign and Security Policy and some of its parts are sensitive since they reveal the Council's strategic approach to cyber sanctions as well as its *modus operandi* in the field of sanctions. The document is a revised option paper<sup>3</sup> which served as basis for discussion on different options, criteria and parameters to be taken into account by the EU institutions and the Member States and reflects considerations of a horizontal nature relating to sanctions. As such, its content is not an integral part of the proposal of the High Representative of the Union for Foreign Affairs and Security Policy to the Council for a Council Decision concerning restrictive measures to counter cyber-attacks threatening the Union or its Member States, that was submitted to the Council on 7th March 2019<sup>4</sup>.

---

<sup>2</sup> ECJ case C-266/05, Sison, para. 46.

<sup>3</sup> It reflects comments and observations received from Member States and following a meeting of the Horizontal Working Party on Cyber Issue held on 23 January 2019.

<sup>4</sup> Document ST 7298/19, in the public domain. The Council subsequently adopted its Decision in this field (Decision (CFSP) 2019/797) on 17 May 2019 (OJ L 129I , 17.5.2019, p. 13–19).

12. As regards the applicant's argument that document **ST 5807/19** is not bearing any classification marking of those foreseen on the Council's security rules for protecting EU classified information (EUCI), it should be stressed that the Council's appreciation of the applicability of the exceptions of Article 4 of Regulation (EC) No 1049/2001 (the so called thorough "harm test" carried out on the content of each and every requested document) is distinct and may not be limited to documents covered by the EUCI provisions concerning the labelling and the protection of classified information. Therefore, though unclassified according to EUCI provisions, a document can nevertheless be sensitive and its release deemed prejudicial to the interests of the EU referred to in Article 4 of Regulation (EC) No 1049/2001. In the present case, the Council maintains its view that there are clearly compelling reasons for opposing to full disclosure of the information in document 5807/19.
13. The fact that the document is 1,5 years old, as the applicant brings forward as an element in favour of granting public access, is irrelevant from this perspective as the information contained therein concerns an EU sanctions regime which is currently fully applicable, could be subject to updates based on lessons learned during the implementation of Decision (CFSP) 2019/797, and also reveals reflections on elements of horizontal nature. If this document was released, adverse actors could gain insight in, among others, the Council's margin of manoeuvre when setting up sanctions regimes and in relation to the review of listings. Full disclosure would enable third countries to foresee how far the Union is likely to go in its restrictive measures policy and to analyse what kind of specific types of pressure could be organised against that policy. Revealing that information would therefore be detrimental to the Union's ability to use restrictive measures to their maximum effect, weakening its position at the international level. As a consequence, full disclosure of the requested document would undermine the public interest as regards international relations (Article 4(1)(a), third indent of Regulation 1049/2001).
14. Moreover, granting public access to document **ST 5807/19** would create a breach in the climate of confidence among the Member States exchanging relevant information not only in the field of cyber sanctions, but also in other fields where sanctions regimes exist, in particular since the requested document reflects preliminary internal discussions in the competent Council Working Party on third parties potentially subject to restrictive measures, as well as a wide range of provided by the Member States in this regard. Therefore, disclosure would not only cause prejudice to the EU's international relations, but also to the Council's decision-making process on future proposals of a similar nature, thus seriously undermining the institution's decision-making process, as per Article 4(3), second subparagraph, of the Regulation.

15. Finally, the Council took note of the applicant's assertion, according to which *“it is in the interest of both academic research, EU transparency and EU citizens education alike to understand and follow EU decision-making on EU cyber sanctions”*.

- As abovementioned, pursuant to the case law and contrary to the allegations of the applicant, Article 4(1)(a) of Regulation (EC) No 1049/2001 does not provide for a test of balancing the harm to the protected interest against the public's interest in disclosure. On the contrary, once the Council has come to the conclusion that the release would indeed undermine the public interests protected pursuant to the third indent of Article 4(1)(a) of Regulation (EC) No 1049/2001, this conclusion is not mitigated by any obligation – or even possibility – to take into account "an overriding public interest" in disclosure.
- Nevertheless, the Council considered whether there is an overriding public interest in disclosure as regards the exception under Article 4 (3) of Regulation (EC) No 1049/2001 (protection of the decision-making process). Such an interest must first be public, and secondly, must outweigh the harm caused by disclosure. In that regard, the Council fully recognises the public interest in transparency and in being informed on the Council's decision-making process (*inter alia* for the purposes of academic research and education). In that regard, the Council notes that it has decided to grant access to a great part of the requested document (cf. paragraph 16 below). However, having examined the context in which this document was drafted and the current state of play on this matter, the Council could not identify any evidence suggesting an overriding public interest that would completely outweigh the need to preserve the interest protected under Article 4(3) of Regulation No 1049/2001.
- Therefore, the Council maintains its view that full access to the document must be refused.

#### **PARTIAL ACCESS PURSUANT TO ARTICLE 4(6) OF REGULATION (EC) NO 1049/2001**

16. In the interest of transparency, and also taking due account of the outcome of its new consultations with the EEAS, the Council is of the opinion that, at this stage, partial access should be granted to those parts of document **ST 5807/19** that, in the Council's view, are no longer covered by any of the exceptions of Regulation (EC) No 1049/2001, some of which were finally reflected, in substance, in Decision (CFSP) 2019/797. Moreover, to enable the applicant to better appreciate the evolution of discussions on the Cyber Diplomacy Toolbox tabled through document **ST 5807/19**, partial access is also granted to its revised version **ST 6309/19**.

## CONCLUSION

17. The Council therefore considers that partial access may be granted to document **ST 5807/19** as well as to its revised version **ST 6309/19**.
  18. Access to the remaining parts of the requested document (and to its revised version **ST 6309/19**) should be refused pursuant to the third indent of Article 4(1)(a) (protection of the public interest as regards international relations) and also pursuant to Article 4 (3), second subparagraph (protection of the decision-making process) of Regulation (EC) 1049/2001.
-