|  |  |
| --- | --- |
|  | Brussels, 12 April 2021 |
| Mr Stefan Soesanto  Email: ask+request-9126-22469de2@asktheeu.org | |
| Ref. 21/0471-rh-vl/vk  Request made on: 24.02.2021  Deadline extension: 17.03.2021 | |
| Dear Mr Soesanto, | |

Thank you for your request for access to documents of the Council of the European Union.[[1]](#footnote-1)

Please find enclosed document **WK 3085/2019**.

Moreover, please find attached a partially accessible version of document **WK 3547/2019**.[[2]](#footnote-2) However, I regret to inform you that full access cannot be given for the reasons set out below.

Document **WK** **3547/2019** of 12 March 2019 is a working document from Europol to delegations on *Innovation in fighting cybercrime*. It contains a presentation given by Europol at the Horizontal Working Party on cyber issues on 8 March 2019.

Full disclosure of this document would reveal sensitive, detailed statistical operational information as regards investigative activities of the EU Member States. The information being intended for a limited group of audience, releasing it to the public domain would give an indication of law enforcement priorities in investigations related to criminality on the dark web as well as potential changes of strategy in EU Member States efforts. Full release of such sensitive information would undermine the proper fulfilment of Europol’s tasks and the investigations and operational activities of Member States, third parties or Union bodies. Full disclosure of such sensitive information would risk prejudicing the operational activities of Member States in their fight against serious crimes as well as undermine Europol’s partners’ trust, consequently preventing Europol from fulfilling its tasks.

Therefore, having consulted with the originating source of the document, the General Secretariat is of the opinion that full disclosure of the document would undermine the protection of the public interest as regards public security. As a consequence, the General Secretariat has to refuse full access to this document.[[3]](#footnote-3)

Furthermore, we regret to inform you that access to documents **WK 215/2019, WK 6958/2019 and WK 12992 2019** cannot be given for the reasons set out below.

Document **WK 215/2019** of 11 January 2019 is a working document drawn up by the Presidency for the Member States' delegations focusing on the Cyber Diplomacy Toolbox and in particular on 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. It contains Member States' comments on a revised version of the options paper on EU restrictive measures in this field.

Document **WK 6958/2019** of 5 June 2019 is a working document drawn by the Presidency for the Member States' delegations containing Member States' comments on a EEAS' narrative paper on a vision for an open, free, stable and secure cyberspace in the context of international security..

Having due regard to the outcome of consultations with the directorate responsible for these policy matters, the General Secretariat is of the opinion that the release of the information contained in these two documents to the wide public cannot be authorized. Their disclosure would enable hostile entities to take advantage from acknowledging the EU's and its Member States' internal views on the appropriate strategic common approach to detect and counter illegal disrupting cyber activities, thus enabling them to use such sensitive elements (among others, scope of the sanctions regime, perpetrator's profiles, evidence data analysis) to cause prejudice to the EU's planning and strategy, This would undermine public interest with regard to public security.(3)

Document **WK 12992/2019** of 15 November 2019 is a working document from the General Secretariat of the Council to delegations on *CYBER DIPLO TTX 19: Europol contribution*. It contains an input from Europol to the Horizontal Working Party on cyber issues on 7 November 2019.

Release of the information contained in this document would jeopardise the public security(3) by revealing sensitive details on operating procedures which are currently in use by the EU law enforcement authorities and Europol when responding to real-life cyber crisis.

Therefore, having consulted with the originating source of the document, the General Secretariat is of the opinion that disclosure of the document would undermine the protection of the public interest as regards public security, such as the proper fulfilment of Europol's tasks and the investigations and operational activities of Member States, third parties or Union bodies. The disclosure of such sensitive information, including details on law enforcement methods and strategies employed, risks prejudicing the effectiveness of present and future operations conducted by the EU Member States. The release of the information would undermine the trust between Europol and its partners and endanger their mutual cooperation, which is essential to Europol's activities, and would consequently hinder Europol's ability to effectively perform its tasks. As a consequence, the General Secretariat has to refuse access to this document.[[4]](#footnote-4)

We have also looked into the possibility of releasing parts of documents **WK 215/2019, WK 6958/2019** and **WK 12992 2019** .[[5]](#footnote-5) However, as the exception to the right of access applies to their entire content, the General Secretariat is unable to give partial access.

As regards the other documents concerned by your request (**WK 1298/2019, WK 9643/2019, WK 12984/2019, WK 12985/2019, WK 12987/2019, WK 12988/2019, WK 12995/2019** and **14056/2019**), unfortunately our consultations with the EEAS and one Member State delegation are still ongoing and we will provide you with a complementary reply as soon as possible, upon their completion (date envisaged: 19 or 20 April 2021).

Pursuant to Article 7(2) of Regulation (EC) No 1049/2001, you may ask the Council to review this decision within 15 working days of receiving this reply. Should you see the need for such a review, you are invited to indicate the reasons thereof.[[6]](#footnote-6)

Yours sincerely,

Fernando FLORINDO

Enclosures: 2.

1. The General Secretariat of the Council has examined your request on the basis of the applicable rules: Regulation (EC) No 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43) and the specific provisions concerning public access to Council documents set out in Annex II to the Council's Rules of Procedure (Council Decision No 2009/937/EU, OJ L 325, 11.12.2009, p. 35). [↑](#footnote-ref-1)
2. Article 4(6) of Regulation (EC) No 1049/2001. [↑](#footnote-ref-2)
3. Article 4(1)(a), first indent, of Regulation (EC) No 1049/2001. [↑](#footnote-ref-3)
4. Article 4(1)(a), first indent, of Regulation (EC) No 1049/2001. [↑](#footnote-ref-4)
5. Article 4(6) of Regulation (EC) No 1049/2001. [↑](#footnote-ref-5)
6. Council documents on confirmatory applications are made available to the public. Pursuant to data protection rules at EU level (Regulation (EU) No 2018/1725, if you make a confirmatory application your name will only appear in related documents if you have given your explicit consent. [↑](#footnote-ref-6)