

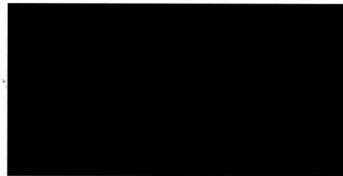


AFFGEN.2

Head of Division

Brussels, 12 JUL. 2019

eeas.sg.affgen.2 (2019) 4378826



Subject: Your request for access to documents of 6 June 2019
Our ref: 2019/031

Dear 

Thank you for your request for access to documents, which the EEAS has examined in the framework of Regulation (EC) No 1049/2001¹.

You have requested access to "all documents as well as internal and external communication (emails, minutes, faxes, mail, etc.) pertaining to the hacker attacks on the EU delegation in Russia which started in 2017".

The EU Delegation in Russia was indeed subject to a cyberattack in 2017 and the investigation on this event is still ongoing.

The information related to this investigation is classified, since the unauthorised disclosure of such information would harm the interests of the European Union and its Member States.

However, the EEAS has undertaken verification whether letter, emails, documents or other type of communications would correspond to your request. After a search in the EEAS filing systems, the document management databases and archives, the EEAS has identified the following documents matching your request, as referenced hereafter:

1. The mandate that the EEAS security authority gave after the cyberattack to the relevant services to investigate this event in accordance with Article 10 of the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service, ADMIN(2017)10².

¹ Regulation (EC) No 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (hereafter the "Regulation").

² OJ C 126, 10.04.2018, p.1

2. A request to different services to assist in the investigation.

It is not possible to release to the public domain neither those documents nor further elements of information related to the identified documents since it would harm the purpose of the investigation [as per Article 4(2), third indent, of the Regulation] by exposing the internal working and decision-making processes of the EU when dealing with and when planning a response to such incidents [as per Article 4(3), 1st subparagraph, of the Regulation]. Disclosing information on internal investigation methods, the way how the information is provided and shared and the internal decision-making would expose the *modus operandi* in the case of such incidents which would decrease the efficiency of the EU response to the attack and it would make the EU vulnerable to similar attacks in the future. It would also affect the trust of the Member States specialised services in the ability of the EU to handle classified information shared in confidence.

Furthermore, no public interest which would override the need to protect the investigation and internal decision-making process was identified.

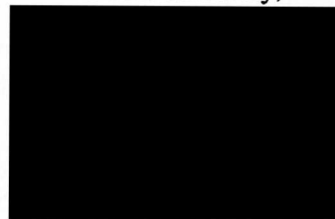
A potential vulnerability by exposing the internal methodology in case of cyber-attacks would be exploited by EU adversaries for future cyber-attacks. It would endanger the security of staff working in the EU Delegations and therefore the exception concerning public security, as established in Article 4(1), first indent, of the Regulation reinforces the reasons why the public release of further information is not possible.

Furthermore, the release of the information related to this incident would harm international relations between the EU institutions, the EU Member States and third countries since different indications and avenues to be explored during the investigation might affect the sensitivities of our external partners and thus negatively influence our diplomatic relations, as per Article 4(1), third indent, of the Regulation.

I take this opportunity to remind you that the information provided may not be reproduced for commercial purposes without prior consultation with the EEAS.

Should you wish this position to be reviewed, you may confirm your initial request within 15 working days.

Yours sincerely,

A large black rectangular redaction box covering the signature area.