European Union
EXTERNAL ACTION

AFFGEN.2
Head of Division

Brussels, 11 SEP. 2020
eeas.sg.affgen.2 (2020) 5452335

Mr Samuel Stolton

Subject: Your request for access to documents of 7 July 2020
Our ref: 2020/088

Dear Mr Stolton,

Thank you for your request for access to documents, which the EEAS has examined in the framework of Regulation (EC) No 1049/2001[1].

Regarding your request for '*any communication between hospitals or health authorities in the European Union and the European External Action Service since 1 January 2020*,' please note that the EEAS did not have any communication directly with hospitals and health authorities.

With regard to your request concerning '*any documentation transmitted between EU member states and the EEAS since 1 January 2020 detailing information on national cyber-attacks, cyber threats, weaknesses of cybersecurity systems, across EU health bodies or hospitals,*' as well as to *'any notification communicated from any public body within the EU to the EEAS, concerning cyberattacks to hospitals or health authorities in the EU, and any follow up communication between the EEAS and the specific body in such cases*,' please note that the EEAS identified a number of documents which match your request that we separated in two groups:

The first group contains documents that the EEAS received from the EU Member States or public bodies concerning cyberattacks or cyber threats to hospitals or health authorities in the EU. These documents were shared with the EEAS in the framework of the activities of the Computer Emergency Response Team for the Union's institutions, bodies and agencies (CERT-EU), the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) or in the

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").

framework of the exchange of information with the national intelligence and security services under the Common Foreign and Security Policy (CFSP) for the purposes of cross-border coordination and collective situational awareness.

The release of these documents to the public domain would reveal not only the working methods of the EEAS, but also of involved intelligence and security services. Any release of information about these documents would disclose elements which could provide information about potential weaknesses and vulnerabilities of critical infrastructures in the health sector, as well as about how and by whom this information was obtained and to whom it was communicated. Consequently, adverse actors would adapt their working methods in order to hamper the work of the intelligence and security services and increase the efficiency of their attacks.

The EEAS received these documents in confidence and under the commitment of non-public disclosure of any element of information which would compromise its sources. Therefore, these documents shall not be disclosed, as per Article 4(4) and Article 4(5) of the Regulation. A unilateral release of these documents would severely harm the trust between the intelligence and security services and the EEAS, since it would endanger the sources and methods through which the information was collected.

Therefore, the EEAS cannot disclose these documents, since it would seriously undermine the protection of the public interest as regards public security, as well as its relations with the Member States as per Article 4 (1), first indent (public security) and third indent (international relations), of the Regulation 1049/2001.

The second group contains documents that the EEAS can release to the public domain. These documents held by the EEAS relate to cyber-attacks, cyber threats, weaknesses of cybersecurity systems, across EU health bodies or hospitals, received from EU Member States and public bodies within the EU since 1 January 2020. I am pleased to forward to you the following documents in attachment to this letter:

1. National Cyber and Information Security Agency Warning against a cybersecurity threat in the form of an extensive campaign of cyberattacks on information and communication systems in the Czech Republic, and on the systems of healthcare facilities in particular.
2. Catching the virus: cybercrime, disinformation and the Covid-19 pandemic
3. Pandemic profiteering: How criminals exploit the Covid-19 crisis
4. TLP-WHITE-CERT-EU-MEMO-Attacks-on-Healthcare
5. TLP-WHITE-CERT-EU-Cyber_Brief-20-05 v1.0

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

Yours sincerely,

Gabriele Visentin