EUROPEAN COMMISSION

Brussels, 10.7.2020
C(2020) 4859 final

Mr Alexander Fanta
netzpolitik.org
Rue de la Loi 155
1040 Bruxelles
Belgium

DECISION OF THE EUROPEAN COMMISSION PURSUANT TO ARTICLE 4 OF THE IMPLEMENTING RULES TO REGULATION (EC) NO 1049/2001 [1]

Subject: **Your confirmatory application for access to documents under Regulation (EC) No 1049/2001 - GESTDEM 2019/4947**

Dear Mr Fanta,

I refer to your letter of 4 October 2019, registered on the same day, in which you submitted a confirmatory application in accordance with Article 7(2) of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents [2] (hereafter 'Regulation (EC) No 1049/2001').

1. SCOPE OF YOUR REQUEST

In your initial application of 21 August 2019, addressed to the Directorate-General for Migration and Home Affairs, you requested access to I quote: '[a]ll national risk assessments submitted member states as part of the EU-wide risk assessment on the security of 5G networks, as announced by Commissioner Julian King on 19 July 2019'.

In its initial reply of 3 October 2019, the Directorate-General for Communications Networks, Content and Technology refused access to these documents based on the exceptions of the first indent of Article 4(1)(a) (protection of the public interest as regards public security) and of the first subparagraph of Article 4(3) (protection of the decision-making process) of Regulation (EC) No 1049/2001.

1 OJ L 345, 29.12.2001, p. 94.
2 OJ L 145, 31.5.2001, p. 43.

In your confirmatory application, you request a review of this position. You underpin your request with detailed arguments, which I will address in the corresponding sections below.

2. ASSESSMENT AND CONCLUSIONS UNDER REGULATION (EC) NO 1049/2001

When assessing a confirmatory application for access to documents submitted pursuant to Regulation (EC) No 1049/2001, the Secretariat-General conducts a fresh review of the reply given by the Directorate-General concerned at the initial stage.

Following this review, the following documents have been identified at confirmatory stage as falling within the scope of your request:

- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Austria, 2 July 2019, reference Ares(2019)5522964 (hereafter 'document 1'), which includes the following annexes:
  - Sectoral risk analysis (hereafter 'document 1.1');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Belgium, 12 July 2019, reference Ares(2019)5523636 (hereafter 'document 2');
- Risk assessments for 5G network infrastructure for Bulgaria, 31 July 2019, reference Ares(2019)5493163 (hereafter 'document 3');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Croatia, 15 July 2019, reference Ares(2019)5523421 (hereafter 'document 4');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Cyprus, 15 July 2019, reference Ares(2019)5521134 (hereafter 'document 5'), which includes the following annexes:
  - 5G risk assessment – final report (hereafter 'document 5.1');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Czechia, 16 July 2019, reference Ares(2019)5516068 (hereafter 'document 6'), which includes the following annexes:
  - Risk assessment of the 5G network infrastructure (hereafter 'document 6.1');
- Summary of findings for 5G cybersecurity risk assessments for Denmark, 15 July 2019, reference Ares(2019)5516613 (hereafter 'document 7');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Finland, 28 June 2019, reference Ares(2019)5524195 (hereafter 'document 8');

- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for France, 12 July 2019, reference Ares(2019)5522835 (hereafter 'document 9'), which includes the following annexes:
    - Risk assessment 5G network infrastructure (hereafter 'document 9.1');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Germany, 15 July 2019, reference Ares(2019)5522658 (hereafter 'document 10');
- Greek National Risk Assessment on Cybersecurity of 5G Networks, 29 August 2019, reference Ares(2019)5557775 (hereafter 'document 11');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Hungary, 15 July 2019, reference Ares(2019)5524455 (hereafter 'document 12');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Ireland, 15 July 2019, reference Ares(2019)5516509 (hereafter 'document 13'), which includes the following annexes:
    - National Risk Assessment: Cyber Security Risks Affecting 5G Networks (hereafter 'document 13.1');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Italy, 15 July 2019, reference Ares(2019)5516262 (hereafter 'document 14'), which includes the following annexes:
    - 5th Generation Network (5G) Italian Cybersecurity Risk Assessment (hereafter 'document 14.1');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Latvia, 10 July 2019, reference Ares(2019)5919219 (hereafter 'document 15');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Lithuania, 17 July 2019, reference Ares(2019)5515741 (hereafter 'document 16'), which includes the following annexes:
    - National Assessment Report on the Fifth Generation (5G) Network Infrastructure and Related Risks (hereafter 'document 16.1');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Luxembourg, 15 July 2019, reference Ares(2019)5516347 (hereafter 'document 17');
- Cybersecurity of 5G Networks - Malta National Risk Assessment, 23 July 2019, reference Ares(2019)5515629 (hereafter 'document 18');

- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for the Netherlands, 23 July 2019, reference Ares(2019)5515477 (hereafter 'document 19'), which includes the following annexes:
    - Accompanying letter of 1 July 2019 from the Minister of Justice and Security to the House of Representatives (hereafter 'document 19.1');
    - Informal translation into English of the accompanying letter of 1 July 2019 from the Minister of Justice and Security to the House of Representatives (hereafter 'document 19.2');
    - Accompanying letter of 4 February 2019 from the Ministry of Interior on National Security (hereafter 'document 19.3');
    - Informal translation into English of the accompanying letter of 4 February 2019 from the Ministry of Interior on National Security (hereafter 'document 19.4');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Poland, 16 July 2019, reference Ares(2019)5516148 (hereafter 'document 20'), which includes the following annexes:
    - Risk analysis table (hereafter 'document 20.1');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Portugal, 16 July 2019, reference Ares(2019)5515934 (hereafter 'document 21');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Romania, 2 July 2019, reference Ares(2019)5523989 (hereafter 'document 22');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Slovakia, 1 July 2019, reference Ares(2019)5524077 (hereafter 'document 23');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Slovenia, 12 July 2019, reference Ares(2019)5919091 (hereafter 'document 24');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for Spain, 15 July 2019, reference Ares(2019)5999063 (hereafter 'document 25');
- National 5G risk assessments – Sweden's response, 5 July 2019, reference Ares(2019)5919167 (hereafter 'document 26');
- Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings for the United Kingdom

– Summary of findings, 22 July 2019, reference Ares(2019)4799164 (hereafter 'document 27'), which includes the following annexes:

- Accompanying email from the National Cyber Security Centre (hereafter 'document 27.1');
- Risk analysis table (hereafter 'document 27.2');
- UK telecoms supply chain review report (hereafter 'document 27.3').

Following this review, I regret to inform you that I have to confirm the initial decision of Directorate-General for Communications Networks, Content and Technology to refuse access to the above-mentioned documents, based on the exceptions of the first indent of Article 4(1)(a) (protection of the public interest as regards public security) and Article 4(1)(b) (protection of privacy and the integrity of the individual) of Regulation (EC) No 1049/2001, for the reasons set out below.

2.1. Protection of the public interest as regards public security

The first indent of Article 4(1)(a) of Regulation (EC) No 1049/2001 provides that '[t]he institutions shall refuse access to a document where disclosure would undermine the protection of the public interest as regards public security'.

The Court of Justice has confirmed that 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.'[3]

The General Court has acknowledged that 'the institutions enjoy a wide discretion when considering whether access to a document may undermine the public interest and, consequently, […] the Courts review of the legality of the institutions' decisions refusing access to documents on the basis of the mandatory exceptions relating to the public interest must be limited to verifying whether the procedural rules and the duty to state reasons have been complied with, the facts have been accurately stated, and whether there has been a manifest error of assessment of the facts or a misuse of powers'[4].

Moreover, the General Court recently ruled that, as regards the interests protected by Article 4(1)(a) of Regulation (EC) No 1049/2001, 'it must be accepted that the particularly sensitive and fundamental nature of those interests, combined with the fact that access must, under that provision, be refused by the institution if disclosure of a document to the public would undermine those interests, confers on the decision which

[3] Judgement of the Court of Justice of 1 February 2007, *Sison* v *Council*, C-266/05 P, EU:C:2007:75 paragraph 46.

[4] Judgment of the General Court of 25 April 2007, *WWF European Policy Programme* v *Council*, T-264/04, EU:T:2007:114, paragraph 40.

must thus be adopted by the institution a complexity and delicacy that call for the exercise of particular care. Such a decision requires, therefore, a margin of appreciation'[5].

The Commission has recognised 5G deployment of network technologies as a major enabler for future digital services and a priority for the Digital Single Market strategy, with many critical services becoming dependant on 5G networks. Consequently, ensuring the cybersecurity of the 5G networks is an issue of strategic importance for the European Union and its Member States, at a time when cyber-attacks are increasing in frequency and sophistication.

In order to fulfil this objective, a Directive on security of networks and information systems[6] was adopted, among others, setting up a Cooperation Group composed of Member States and the European Union Agency for Cybersecurity, whose secretariat is ensured by the Commission, tasked with achieving a high common level of security of network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States.

The European Council of 21 March 2019 has expressed support for a concerted approach on the security of 5G networks that would, in time, ensure the strategic autonomy of the Union vis-à-vis other global players. Thus, the European Commission adopted a Recommendation[7] 0which, among others, requests each Member State to carry out national risk assessments of the 5G network infrastructure on the basis of a questionnaire.

The information provided by Member States allowed the collection of information on main assets, threats and vulnerabilities related to 5G infrastructure and main risk scenarios, describing potential ways in which threat actors could exploit a certain vulnerability of an asset in order to impact government objectives. While a certain part of the risk assessment reports is the same, reiterating the background and the questions sent to the Member States, each Member State chose to develop the answers to the questionnaire to a certain level of detail that would give a clear indication of actual risks, threats and vulnerabilities, as well as an identification of sensitive network assets, which may be more exposed to certain types of security threats. In addition, the documents identify existing or planned measures to address these risks. Moreover, some Member States decided to include additional detailed expert reports that were not based on the questionnaire.

---

5 Judgment of the General Court of 11 July 2018, *Client Earth v European Commission*, T-644/16, EU:T:2018:429, paragraph 23.

6 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereafter 'NIS Directive'), OJ L 194, 19.7.2016, p.1.

7 Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks, C(2019) 2335 final.

The above-mentioned documents were shared with the NIS Cooperation Group or, due to their sensitivity, addressed only to the European Commission and to the European Union Agency for Cybersecurity. Apart from the German contribution, which apparently was made public by the German authorities following a request for access to documents, none of the other contributions were made public.

In your confirmatory request, you argue that if the German competent authority agreed to disclosure of their contribution, 'hardly makes sense to argue against any kind of disclosure on security grounds when at least one authority saw no reason to withhold'. While the German authorities did not consider the content of their contribution sensitive, I consider that disclosure of these documents as a whole, would give a comprehensive view of the risks, vulnerabilities and mitigating measures of the Union and may expose potential gaps in existing mitigation measures, with an impact far greater than the individual disclosure of the contribution of one Member State.

Disclosure of these documents would also affect the ability of network operators and public authorities of Member States to protect effectively their networks against cybersecurity threats. This could have negative consequences for the security of present and future networks and digital infrastructures and lead to potential security risks for the society as a whole.

Based on the foregoing there is a real and non-hypothetical risk, that disclosure of these documents would undermine the protection of public interest, as regards public security as provided for in the first indent of Article 4(1)(a) of Regulation (EC) No 1049/2001.

Nevertheless, our assessment does not preclude your right to file individual requests for access to documents with the national administrations of the Member States concerned.

2.2. Protection of privacy and the integrity of the individual

Article 4(1)(b) of Regulation (EC) No 1049/2001 provides that '[t]he institutions shall refuse access to a document where disclosure would undermine the protection of […] privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data'.

In its judgment in Case C-28/08 P (*Bavarian Lager*)[8], the Court of Justice ruled that when a request is made for access to documents containing personal data, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[9] (hereafter 'Regulation (EC) No 45/2001') becomes fully applicable.

---

8 Judgment of the Court of Justice of 29 June 2010, *European Commission* v *The Bavarian Lager Co. Ltd* (hereafter referred to as *'European Commission* v *The Bavarian Lager* judgment') C-28/08 P, EU:C:2010:378, paragraph 59.

9 OJ L 8, 12.1.2001, p. 1.

Please note that, as from 11 December 2018, Regulation (EC) No 45/2001 has been repealed by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[10] (hereafter 'Regulation (EU) 2018/1725').

However, the case law issued with regard to Regulation (EC) No 45/2001 remains relevant for the interpretation of Regulation (EU) 2018/1725.

In the above-mentioned judgment, the Court stated that Article 4(1)(b) of Regulation (EC) No 1049/2001 'requires that any undermining of privacy and the integrity of the individual must always be examined and assessed in conformity with the legislation of the Union concerning the protection of personal data, and in particular with […] [the Data Protection] Regulation'[11].

Article 3(1) of Regulation (EU) 2018/1725 provides that personal data 'means any information relating to an identified or identifiable natural person […]'.

As the Court of Justice confirmed in Case C-465/00 (*Rechnungshof*), 'there is no reason of principle to justify excluding activities of a professional […] nature from the notion of private life'[12].

Documents 1.1, 19.3, 26, 27.1 contain personal data such as the names, initials or handwritten signatures of representatives of Member States in the NIS Cooperation Group or those of experts or coordinators in the Member States.

The names[13] of the persons concerned, who are not public figures, as well as other data from which their identity can be deduced, undoubtedly constitute personal data in the meaning of Article 3(1) of Regulation (EU) 2018/1725.

Pursuant to Article 9(1)(b) of Regulation (EU) 2018/1725, 'personal data shall only be transmitted to recipients established in the Union other than Union institutions and bodies if '[t]he recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests'.

Only if these conditions are fulfilled and the processing constitutes lawful processing in accordance with the requirements of Article 5 of Regulation (EU) 2018/1725, can the transmission of personal data occur.

---

10 OJ L 295, 21.11.2018, p. 39.

11 *European Commission v The Bavarian Lager* judgment, cited above, paragraph 59.

12 Judgment of the Court of Justice of 20 May 2003, *Rechnungshof and Others* v *Österreichischer Rundfunk*, Joined Cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 73.

13 *European Commission* v *The Bavarian Lager* judgment, cited above, paragraph 68.

In Case C-615/13 P (*ClientEarth*), the Court of Justice ruled that the institution does not have to examine by itself the existence of a need for transferring personal data[14]. This is also clear from Article 9(1)(b) of Regulation (EU) 2018/1725, which requires that the necessity to have the personal data transmitted must be established by the recipient.

According to Article 9(1)(b) of Regulation (EU) 2018/1725, the European Commission has to examine the further conditions for the lawful processing of personal data only if the first condition is fulfilled, namely if the recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest. It is only in this case that the European Commission has to examine whether there is a reason to assume that the data subject's legitimate interests might be prejudiced and, in the affirmative, establish the proportionality of the transmission of the personal data for that specific purpose after having demonstrably weighed the various competing interests.

In your confirmatory application, you do not put forward any arguments to establish the necessity to have the data transmitted for a specific purpose in the public interest. Therefore, the European Commission does not have to examine whether there is a reason to assume that the data subjects' legitimate interests might be prejudiced.

Notwithstanding the above, there are reasons to assume that the legitimate interests of the data subjects concerned would be prejudiced by the disclosure of the personal data reflected in the documents, as there is a real and non-hypothetical risk that such public disclosure would harm their privacy and subject them to unsolicited external contacts.

Consequently, I conclude that, pursuant to Article 4(1)(b) of Regulation (EC) No 1049/2001, access cannot be granted to the personal data, as the need to obtain access thereto for a purpose in the public interest has not been substantiated and there is no reason to think that the legitimate interests of the individuals concerned would not be prejudiced by the disclosure of the personal data concerned.

3. OVERRIDING PUBLIC INTEREST IN DISCLOSURE

The exceptions laid down in Article 4 of Regulation (EC) No 1049/2001 must be waived if there is an overriding public interest in disclosure. Such an interest must, firstly, be public and, secondly, outweigh the harm caused by disclosure.

While issues related to 5G generally stir public interest, Articles 4(1)(a) and 4(1)(b) of Regulation (EC) No 1049/2001 do not include the possibility for the exceptions defined therein to be set aside by an overriding public interest.

[14] Judgment of the Court of Justice of 16 July 2015, *ClientEarth* v *European Food Safety Agency*, C-615/13 P, EU:C:2015:489, paragraph 47.

Nonetheless, the public interest in the 5G national risk assessments was taken into consideration and on 9 October 2019, the NIS Cooperation Group, with the support of the European Commission and of the European Agency for Cybersecurity, published a high-level report[15] that sets out the key common findings emerging from the national risk assessments of 5G networks carried out by each Member State.

Contrary to your assertion, there is a significant difference in the level of detail between the individual contributions of the Member States and the high-level report, which warrants the protection of the former against public disclosure.

4. PARTIAL ACCESS

In accordance with Article 4(6) of Regulation (EC) No 1049/2001, I have considered the possibility of granting (further) partial access to the documents requested.

However, for the reasons explained above, no meaningful partial access is possible without undermining the interests described above.

Consequently, I have concluded that the documents requested are covered in their entirety by the invoked exceptions to the right of public access.

5. MEANS OF REDRESS

Finally, I draw your attention to the means of redress available against this decision. You may either bring proceedings before the General Court or file a complaint with the European Ombudsman under the conditions specified respectively in Articles 263 and 228 of the Treaty on the Functioning of the European Union.

Yours sincerely,

CERTIFIED COPY
For the Secretary-General,

Jordi AYET PUIGARNAU
Director of the Registry
EUROPEAN COMMISSION

For the Commission
Ilze JUHANSONE
Secretary-General

[15] Available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.