

EUROPEAN COMMISSION
DIRECTORATE-GENERAL MIGRATION and HOME AFFAIRS

The Director General

Brussels, 27 June 2016
HOME/D3/LA/(2016)3688257

By registered letter with acknowledgment of receipt

Mrs Maryant FERNÁNDEZ
EDRi (European Digital Rights)
20 Rue Belliard
1040 Brussels

Advance copy by email:
ask+request-2876-e906cfee@asktheeu.org

Subject: Your applications for access to documents – Ref Gestdem No 2016/2692

Dear Mrs Fernandez,

1. We refer to your application for access to documents, GestDem No 2016/2692, dated 13/05/2016, registered on the same date, referring to the launch of the Joint Referral Platform.
2. In your application, you requested the following documents:
 - 1) *The launch of the 'Joint Referral Platform'*
 - 2) *The involvement of Europol and Europol's Internet Referral Unit (IRU) involvement in the 'Joint Referral Platform';*
 - 3) *Statistics relating to flagged content and content that has been removed;*
 - 4) *Statistics relating to the follow-up by law enforcement after content has been removed;*
 - 5) *Agreed on goals and (legal) principles;*
 - 6) *Minutes of meetings with industry;*
 - 7) *The list of companies from the internet industry partaking in the 'Joint Referral Platform';*
 - 8) *The exchange of e-mails between industry and the Commission with regards to the 'Joint Referral Platform';*
 - 9) *Documents relating to the costs involved.*

3. In addressing request 1, it is important to clarify that the Joint Referral Platform as set out in the Communication on delivering on the European Agenda on Security (COM2016 -230¹) to fight against terrorism and pave the way towards an effective and genuine security union is currently being developed by the industry and has therefore not been launched. Therefore no document on the launch of the Joint Referral Platform exists. Similarly, there are no documents relating to the costs involved of the launch (which addresses request 9). In response to request 2, once we have sight of the industry's proposal, discussions will then take place with Europol to determine its exact role. In response to request 7, as discussions amongst the companies are ongoing, we do not have any documents setting out which companies plan to partake in the Joint Referral Platform. To summarise, there are no documents relating to requests 1, 2, 7, 8, and 9.
4. With regards to request 3, as set out in the same Communication, the EU IRU has assessed over 4,700 pieces of material from across 45 platforms and made over 3,200 referrals for internet companies to remove content, with an effective removal rate of 91%.
5. It is important to emphasise that the role of the EU IRU is to support the companies in optimising the referral process and reducing accessibility to terrorist content online, not to initiate investigations. Whilst the EU IRU works closely with Member States as part of the referrals process and can provide operational support, you would need to ask Member States about follow-up by their law enforcement authorities after content has been removed. The Commission does not hold any document with information relating to request 4.
6. The goal of the Joint Referral Platform (request 5) is to prevent known terrorist/violent extremist material removed from one site, from simply being re-uploaded onto to another, as set out in the aforementioned Communication.
7. With regards to request 6, one document has been identified as relevant for your request. This is an internal document entitled 'Flash Report: Mission to California' dated 10 April 2017. I regret to inform you that your application cannot be granted, as disclosure is prevented by exceptions to the right of access laid down in Article 4 of this Regulation. For access to this document, I am of the opinion that the entities that my services met during the mission (whose views are reflected in this document) have legitimate expectations that their views are treated in confidence and not disclosed. References to potential shortcomings or individual positions and views would undermine the relationship of mutual trust which is essential for the further work in this sensitive area closely linked to matters of public security, protected under Article 4 (1) a) first indent of Regulation 1049/2001.
8. Furthermore, as some of the views expressed reveal the position taken by attendees to the meeting, this could affect their commercial interests within the meaning of Article 4(2) first bullet point of Regulation 1049/2001. Article 4(2), first indent of Regulation No. 1049/2001 stipulates that *[t]he institutions shall refuse access to a document where disclosure would undermine the protection of (...) commercial interests of a natural or legal person, including intellectual property, (...) unless there is an overriding public interest in disclosure.*

¹ See under http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf

9. Public disclosure of the identified document would undermine the protection of their commercial interests in a reasonably foreseeable and not purely hypothetical way, because it would expose them to terrorist threats and possible attacks. This has already been the case for some of the companies as reported in the press².
10. At the same time, public disclosure of the document would risk undermining the integrity of the companies' managers, in accordance with the exception of Article 4(1)b of Regulation 1049/2001, as they can personally become the targets of threats and possible attacks of terrorist groups. This has already been the case, as reported in the press³.
11. Pursuant to this Article, access to a document has to be refused if its 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. The applicable legislation in this field is 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 data⁴.
12. When access is requested to documents containing personal data, Regulation (EC) No 45/2001 becomes fully applicable⁵. According to Article 8(b) of this Regulation, personal data shall only be transferred to recipients if they establish the necessity of having the data transferred to them and if there is no reason to assume that the legitimate rights of the persons concerned might be prejudiced. We consider that, with the information available, the necessity of disclosing the aforementioned personal data to you has not been established and/or that it cannot be assumed that such disclosure would not prejudice the legitimate rights of the persons concerned.
13. Moreover, Article 4(3), first subparagraph of Regulation 1049/2001 provides that *[a]ccess to a document, drawn up by an institution for internal use or received by an institution, which relates to a matter where the decision has not been taken by the institution, shall be refused if disclosure of the document would seriously undermine the institution's decision-making process, unless there is an overriding public interest in disclosure*. In this instance, any premature release about information on planned concrete actions, particularly whilst many of them are still under discussion in the framework of a climate of confidentiality and mutual trust, would entail the risk of having the work over digital fight against terrorism to collapse.
14. In light of the above, I am of the opinion that access to this document has to be refused as its disclosure would
 - a. - undermine public security in a sensitive area, protected under Article 4(1)a) first indent,

² See e.g. article in the Independent about Isis hackers threatening Facebook and Twitter founders for shutting accounts: <http://www.independent.co.uk/news/people/isis-hackers-threaten-facebook-and-twitter-founders-for-shutting-accounts-a6894921.html>,

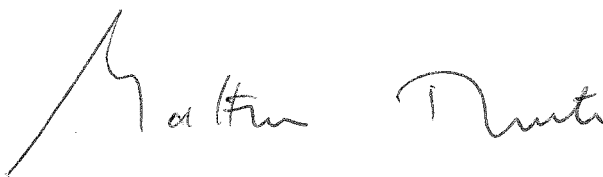
<http://money.cnn.com/2016/02/29/technology/mark-zuckerberg-threat-isis/>
³ See e.g. <http://www.theguardian.com/technology/2016/feb/24/isis-video-targets-twitter-and-facebook-ceos-over-suspended-accounts>, <http://money.cnn.com/2016/02/24/technology/isis-mark-zuckerberg/?iid=EL>

⁴ Official Journal L 8 of 12.1.2001, p. 1

⁵ Judgment of the Court of Justice of the EU of 29 June 2010 in case 28/08 P, Commission/The Bavarian Lager Co. Ltd, ECR 2010 I-06055.

- b. – undermine the protection of the commercial interests of the companies involved in the Joint Referral Platform according to Article 4(2), first indent
 - c. jeopardise the protection of integrity of their managers according to Article 4(1)(b) and
 - d. Undermine a highly sensitive on-going process to be protected according to Article 4(3), first subparagraph of Regulation 1049/2001.
15. I have considered whether partial access could be granted to the documents requested. The exceptions laid down in Article 4(2) and 4(3) of Regulation 1049/2001 apply unless there is an overriding public interest in disclosure of the documents. In view of the sensitivity of the matters dealt with during this mission and the urgent need for getting results with stakeholders involved in view of tackling security threats, I am of the opinion that no such overriding public interest exists in this case.
16. Full disclosure would result in the public release of the position expressed by attendees who have shared important information with the Commission in confidence and on a sensitive subject. Such public disclosure would clearly undermine the climate of mutual trust with the stakeholders concerned. There is thus a real and non-hypothetical risk that industry representatives will no longer be willing to co-operate with the Commission and EU Member States in this field, which would in turn greatly jeopardise the success of the Commission's response to this challenge.
17. Against this background, and in light of recent terrorist attacks and attempted attacks, I take the view that keeping data confidential is essential for the safety and security of EU citizens and for ensuring the viability and integrity of co-operation with the relevant stakeholders.
18. In accordance with Article 7(2) of Regulation 1049/2001, you are entitled to make a confirmatory application requesting the Commission to review this position.
19. Such a confirmatory application should be addressed within 15 working days upon receipt of this letter to the Secretary-General of the Commission at the following address:
European Commission
Secretary-General
Transparency unit SG-B-4
BERL 5/327
B-1049 Bruxelles
or by email to: sg-acc-doc@ec.europa.eu

Your sincerely,



Matthias Ruete