

From:

To:

CC:

Sent at: 29/06/20 16:29:23

Subject: Informal consultation: possible development a Social Media Monitoring (SMM) capability by Frontex

Dear [REDACTED],

I am contacting you regarding a possible development a Social Media Monitoring (SMM) capability by Frontex. I tried to call you several times during the day.

As you may know, following the ban issued by the EDPS in September 2019, SMM reports are not longer produced by EASO. Given the importance of social media monitoring in the context of external borders, following internal reflections within DG HOME, we produced a note (enclosed) describing the possible development of a Social Media Monitoring (SMM) capability by Frontex in accordance with its new mandate.

I was advised by your ex colleague, [REDACTED], to contact you as a the best person to seek the very first informal technical views of the EDPS office on this issue. We understand that some preliminary contacts also took place at the level of Cabinet of Commissioner Johansson and possible of your Cabinet.

My colleague, [REDACTED], will be available as of Wednesday morning to reply to any question you may have on the proposed approach and/or to discuss it at your convenience via a VC.

With best regards



European Commission

Directorate-General Migration and Home Affairs
Unit B1 Borders and Schengen

[REDACTED]

The views expressed above are the writer's alone and may not in any circumstances be regarded as stating an official position of the European Commission. If you have received this message in error, please contact the sender by e-mail or telephone [REDACTED] and then delete this message. Thank you.

Note on development of a Social Media Monitoring capability in FRONTEX

The present note describe to develop in FRONTEX a Social Media Monitoring (SMM) capability covering the external borders in order to offer an alternative to the SMM reports, previously produced by EASO before the ban by the EDPS in September 2019.

FRONTEX would add SMM to its existing surveillance tools and establish a link with EUROPOL which coordinates the criminal investigations.

All the phases described below would require a prior clearance from the EDPS, and the identification and acquisition of the necessary technical and human resources by FRONTEX.

Social media monitoring and the role of HOME Agencies is described in Annex 1. The data protection issues and how the new FRONTEX mandate can help address it are presented in Annex2.

1. WHY IS FRONTEX THE MOST APPROPRIATE AGENCY?

FRONTEX is continuously providing surveillance tools and intelligence products to the Member States' border control authorities, ranging e.g. from the monitoring of suspicious vessels to the analysis of migrants' interviews. Social Media Monitoring would perfectly complement these existing FRONTEX services and lead to an enhanced intelligence picture.

Furthermore, for many years FRONTEX is present at the external borders via its joint operations and thus knows exactly what should be looked for when e.g. monitoring the activities of smuggling networks in social media. SMM would allow FRONTEX to gather intelligence for the European Border and Coast Guard, i.e. not only for the Agency but also for Member States' border guard authorities, to better target operations and further enhance risk analyses.

The new FRONTEX mandate, contrary to EASO, allows to process personal data for law enforcement purposes and to monitor social media. However, any kind of police or judicial investigation remains outside the FRONTEX mandate. Once collected, FRONTEX shall transmit such personal data to EUROPOL or the competent Member States' law enforcement authorities for the purposes of investigation and prosecution.

Finally, FRONTEX is being given sufficient financial and human resources to quickly set up the SMM in line with its new mandate.

2. FIRST PHASE: SMM AS PART OF A SPECIFIC FRONTEX JOINT OPERATION (END 2020)

In order to quickly test the concepts of SMM and deliver the first reports, FRONTEX would launch a new type of Joint Operation "on line" focusing on SMM. As for any Joint Operation, FRONTEX would identify a target area and partner with a Member State to "host" this operation. The host Member State would be responsible for the targeting of the suspects, and would access all the corresponding personal data. Frontex would transmit operational personal data packages to EUROPOL as appropriate.

In parallel, the SMM activity would also contribute to risk analysis reports, which, once anonymized¹, would be transmitted to the European Border and Coast Guard community, to the Commission, and other relevant stakeholders through the European Border Surveillance

System (EUROSUR)ⁱⁱ. These reports would offer a first alternative to the SMM reports previously produced by EASO. The first “new” SMM reports could be available by the end of 2020, but the FRONTEX operation could last longer.

This first phase would help FRONTEX develop the necessary procedures, identify the relevant tools and profiles, and address in a proactive manner any concern that the EDPS may have, before moving into a larger scale monitoring of social media and other internet activities of interest related to a wider spectrum of cross border crime, in the following phase.

3. SECOND PHASE: SMM AS PART OF FRONTEX SURVEILLANCE TOOLS (BY 2023)

In order to implement the provision related to data protection in its new mandate, FRONTEX needs to adopt a series of implementing decisionsⁱⁱⁱ, which will frame the application of the relevant Articles^{iv} of the new Regulation (EU) 2019/1896 on the European Border and Coast Guard. This also applies to the processing of operational personal data.

Based on the lessons learned from the first phase, FRONTEX would prepare a specific implementing decision, which would frame the online surveillance activities of FRONTEX, specifying the purpose of the activities, the various procedures, etc.

In parallel FRONTEX would acquire the relevant tools and recruit the necessary staff to increase its coverage, creating an in-house structure comparable to EUROPOL’s Internet Referral Unit but focusing on countering cross border crime and illegal migration.

The new entity in FRONTEX would be able to produce SMM reports on the main areas of interest for the European Border and Coast Guard, and provide contributions to the operational response by informing the competent law enforcement authorities of the Member States, EUROPOL and EUROJUST.

ANNEX 1: What is social media monitoring?

Social Media Monitoring entails specific constraints related to personal data protection. Because of the functioning of social media, large scale SMM of illegal activities implies the processing of “operational personal data”. Such personal data, which are collected for law enforcement purposes following very specific procedures, are bound to the specific data protection rules and particularly affects the exercise of data subjects’ rights.

Social media^v can be abused to advertise, organize, promote and facilitate criminal activities to the victims, but also to coordinate and liaise with other criminals. Criminal entrepreneurs and organised crime groups involved in migrant smuggling and, trafficking of in human beings (THB) as well as and in other forms of cross border crime, including the provision of forged documents, are making wide use of social media. The irregular migrants using the ‘services’ of facilitators as well as witnesses of such traffic are also making use of social media and constitute valuable sources of useful intelligence.

Social Media Monitoring (SMM) aims at gathering and analysing information from social media and developing actionable intelligence accessing these social media platforms and content with a view to

- trigger and support the identification and investigation with a view to convict those criminals and stop their activities, and
- support situational awareness and perform risk analysis, focusing on migratory trends and routes.

SMM requires a technical capacity to access the targeted online content, in a discrete manner and with a good understanding of the languages, cultures and modus operandi of the corresponding individuals, groups and organizations.

The European Migrant Smuggling Centre of EUROPOL, supports concrete investigations in migrant smuggling, where the digital smuggling aspects are increasing. The information previously received from EASO SMM reports, coupled with data on criminal entities already contributed to EUROPOL databases has led to several cross-match reports and intelligence notifications being provided to Member States to trigger investigations against migrant smuggling criminal networks.

EUROPOL’s EU Internet Referral Unit (EU IRU), part of EUROPOL’s European Counter Terrorism Centre (ECTC), has the mandate

1. to flag terrorist and violent extremist content refer to Online Service Providers (OSPs) and support MS in Internet investigations and share this with relevant partners, and
2. to contribute to the disruption of illegal immigrant smuggling networks, by detecting and requesting removal of internet content used by traffickers to attract migrants and refugees, upon MS requests.

EUROPOL’s expertise in SMM is therefore highly valuable.

The European Asylum Support Office (EASO) had developed an SMM capacity used to assess migratory trends. On 30th September 2019, the European Data Protection Supervisor established a temporary ban on EASO SMM reports^{vi}. Since then there is no dedicated SMM capacity addressing migratory challenges at EU level.

ANNEX 2: Social media monitoring and personal data protection

FRONTEX can already process such personal data as part of its Joint Operations. This provision set in Article 88 of Regulation (EU) 2016/1624 was kept in the new mandate. The main channel to obtain personal data is currently through interviews with migrants^{vii}. The information provided by the migrant is then inserted in a FRONTEX-managed system called PEDRA. In order to do that, the operational plans of each Joint Operation must contain specific provisions related to the processing of personal data. FRONTEX is in the process of expanding its data collection sources by moving beyond debriefing interviews and using other information that can be collected within a Joint Operation. This set-up could be used to test initial solutions for SMM.

In addition, the new mandate^{viii} foresees that FRONTEX *can process operational personal data, which it has collected while monitoring migratory flows, carrying out risk analyses or in the course of operations, for the purpose of identifying suspects of cross-border crime, with a view to transmitting it to the competent authorities of the Member States, EUROPOL or EUROJUST. Such personal data may include personal data of victims or witnesses where those personal data supplement the personal data of suspects processed by FRONTEX.*

ⁱ All personal data would be removed at this stage.

ⁱⁱ As provided for in Article 28(2)(h) of Regulation (EU) 2019/1896.

ⁱⁱⁱ At the level of its management board.

^{iv} Chapter V Section 2 of Regulation (EU) 2019/1896.

^v Such as Facebook, WhatsApp, Telegram, etc.

^{vi} https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf

^{vii} Also called debriefing interviews.

^{viii} Article 90 of Regulation 2019/1896.