



Brussels, 7 October 2020  
(OR. en)

11564/20

**LIMITE**

CT 79  
ENFOPOL 245  
SIRIS 75  
COTER 82  
JAI 785  
IXIM 100  
COSI 145  
COMIX 448

**NOTE**

---

From:	Presidency
To:	Delegations
No. prev. doc.:	7741/20
Subject:	Defining a process for entering information from third countries on suspected non-EU terrorists in the Schengen Information System

---

1. The objective of this paper is to set out a process for evaluating information from third countries on suspected non-EU terrorists and possibly entering relevant data in the Schengen Information System (SIS) if legal prerequisites on national and EU level are met. An updated proposal for a process together with a visual chart can be found in the Annexes.

2. Since last autumn, it has been discussed at length, at both meetings in the Commission and Europol and in Council Working Parties<sup>1</sup> if and how to define an adequate procedure, taking into account legal and operational constraints (see the previous papers for a more elaborate background<sup>2</sup>). The attached updated draft describes a revised process that takes into account the concerns expressed by Member States following the consultations subsequent to the Standing Committee on Operational Cooperation on Internal Security (COSI) of 20 May 2020 and further deliberation. It aims at ensuring that appropriate and timely action is taken upon the receipt of a list of suspected non-EU FTFs from a third country.
3. Most Member States recognise the need to act at EU-level and have given detailed replies<sup>3</sup> to the requests for contribution, issued under the previous Presidency, aiming at finding an appropriate solution. Given the fact that Member States national security services often possess valuable information in relation to information shared by third countries on FTFs and could contribute to verify the accurateness thereof, the Service acting as Presidency of the Counter Terrorism Group (CTG)<sup>4</sup> was informally consulted by the Commission in late spring this year. While CTG clearly not being inside the framework of the EU, the draft develops now a mechanism which ensures through the Service acting as Presidency of the CTG that pertinent interests of Member States national security services are appropriately taken into consideration.

---

<sup>1</sup> Commission meetings of 15 November 2019 and 3 March 2020, meetings of the Terrorism Working Party (TWP) of 16 January and 4 March 2020, the Working Party on JHA Information Exchange (IXIM), and in written procedure subsequent to the Standing Committee on Operational Cooperation on Internal Security (COSI) of 20 May 2020. It was the intention of the Croatian Presidency also to focus on the border security aspects, in the Frontiers' Working Party on 17 March 2020, but this was cancelled due to the COVID-19 outbreak.

<sup>2</sup> 7741/20; 7699/20; 6322/20.

<sup>3</sup> WK 5002/2020 + ADD1 and 5865/1/2020 REV 1.

<sup>4</sup> The Counter Terrorism Group (CTG) is an informal grouping of intelligence agencies from 30 European countries. CTG was founded in 2001 and includes agencies from all 27 European Union members, Norway, United Kingdom and Switzerland.

4. The potential terrorist threat posed by FTFs, including returnees, is a major concern, both at political and operational level. It is estimated that 50 000 persons have travelled to Syria/Iraq since 2012 to join Da'esh. European FTF suspects represent just 10% of the estimated total. It is therefore critical that also non-European FTFs are detected should they try to cross EU borders, and that action is taken upon receipt of identities of suspected non-European FTFs. Much of the information on non-European FTFs is held by third countries.
5. Pending an agreed approach/process for entering those individuals in relevant databases, it has been done on an *ad-hoc* basis by Member States volunteering, duly verifying the information. In line with the SIS legislation, a Member State issuing an alert is responsible for the accuracy and lawfulness of the data.
6. Against this background, and taking into account Member States' comments from the repeated rounds of consultation, the Presidency, at this stage, suggests establishing a provisional and voluntary process: "provisional" in the sense that the procedure will be topic of evaluation and amendments due to possible changes, for example in relevant legislation<sup>5</sup>; and "voluntary", meaning that only Member States who would want to participate, including on a case-by-case basis, should do so. As regards the participation in a voluntary process, some Member States have already participated in the *ad hoc*-exercise, others confirmed their willingness to take an active role, in some instances on a case-by-case basis.
7. The process/draft outline for a process should apply when a list of suspected FTFs originating from a third country is transmitted either directly by a third country or by a Member State to Europol.
8. The Presidency invites Member States to agree on the suggested provisional and voluntary process to bring this pressing issue to a successful conclusion.

---

---

<sup>5</sup> Bearing in mind in particular the upcoming revision of the Europol-Regulation.

**Coordinated approach - Entering information on suspected Foreign Terrorist Fighters (FTF) received from third countries into the SIS****Draft outline for a process**

A list of suspected FTF originating from a third country is transmitted either directly by the third country or by a Member State to Europol.

**Step 1** [*Info-Link to the Service acting as Presidency of the CTG*]

Europol informs the Council Presidency, the Member States, the Commission and the EU CTC of having received a list with suspected FTF originating from a third country. At the request of a Member State, Europol transmits the full list to the requesting Member State. Europol reaches out to the Service acting as Presidency of the Counter Terrorism Group (CTG). The Service acting as Presidency of the CTG then has the possibility to comment and make recommendations in a coordination process with Europol on behalf of the CTG's member services.

The Service acting as Presidency of the CTG is encouraged to indicate to Europol if the list has already been received and if CTG member services are also processing the list, if possible. If this is the case, Europol and the Service acting as Presidency of the CTG will decide in mutual coordination on the further processing of the list.

**Step 2** [*Europol updates the list*]

Europol does a first quality check (trustworthiness of the source, completeness and accuracy of the data received, elimination of duplicated names, necessary technical work etc.) and verifies whether some of the persons are already inserted into the SIS. If a person is already in the SIS, Europol contacts the Member State having issued the alert bilaterally, in accordance with the relevant provisions of SIS Regulations (and provided it complies with Europol's rules on handling codes) to confirm that it indeed relates to the same person. Where appropriate, the Member State completes the alert (e.g. adds fingerprints and/or facial images when available). Europol updates the list accordingly, mentioning which alert by which Member State was entered.

Europol prepares an updated list, based on the one received from the third country, enriched with relevant additional information found in Europol's (facial recognition tool, EIS, etc.) and Interpol's databases. Europol will update and supplement the data in accordance with applicable restrictions imposed by the data owner on the access or use of such data (e.g. handling codes), in compliance with Europol's legal framework.

After the initial data processing has been completed by Europol, an updated list is communicated to the Presidency of the CTG. The Service acting as Presidency of the CTG is again encouraged to inform whether CTG member services<sup>6</sup> will further process the list and is also encouraged to communicate the results of this additional analysis to Europol, if possible.

Interpol may be requested to support this process by Europol, as appropriate.

**Step 3** [*MS have possibility to update the list*]

Europol informs the Member States on the outcome of the data processing exercise conducted by Europol and/or the CTG services<sup>7</sup> and addresses any restrictions as described under Step 2. On the basis of the updated list, the competent authorities of the Member States will have the opportunity to conduct a quality check of the list (e.g. reliability of the data received, check against national databases) and convey the results of the check back to Europol. Europol takes feedback by Member States into account and updates the list again.

**Step 4** [*Agreement on burden sharing*]

Europol seeks to establish a group of voluntary Member States who are willing to further process the list. This identification and verification process aims at the assessment of inserting alerts on the remaining suspected FTFs into the SIS, where appropriate and in full respect of national and EU legislation. The group of voluntary Member States will decide on a burden sharing among them. Europol keeps the Presidency informed of this process.

---

<sup>6</sup> EU Member States and Schengen Associated Countries only.

<sup>7</sup> EU Member States and Schengen Associated Countries only.

## Step 5 *[MS process the list]*

Each participating Member State processes and analyses the part of the list it has volunteered to examine. Where appropriate and in line with EU and national legislation, suspected FTFs are inserted into the SIS, with biometric data when available, under the most appropriate alerts that meet the conditions and thresholds established in national and EU law. Member States are encouraged to use alerts for refusal of entry alerts or alerts for arrest, if appropriate.

Before inserting a suspected FTF into SIS, Member States shall fulfil the legal requirements to:

- analyse each case on the basis of an individual assessment and, where appropriate, issue a judicial or administrative decision in accordance with their national law;
- assess whether the conditions and thresholds for inserting alerts to SIS are met in accordance with national and SIS legislation;
- review the need to keep each individual alert or delete the alert when appropriate, in accordance with the SIS legislation;
- provide for, in accordance with national law, the relevant remedies for individuals to bring action before competent authorities, including a court, in connection with an alert relating to him or her.

The Member State issuing such alert becomes the owner of the SIS alert containing the information originating from the third country and is responsible for ensuring that the data inserted in the alert is accurate, up-to-date and entered as well as processed in SIS lawfully, including the operational follow-up to that alert. Any new information concerning the subject of the alert should be submitted immediately to the responsible Member State in accordance with the relevant legislation.

Europol is available to support Member States' efforts during the whole life cycle of the alert.

**Step 6** [*MS inform stakeholders of progress and results*]

Participating Member States' competent authorities keep Europol informed of the progress on processing the list on a regular basis. Europol in turn keeps the Terrorism Working Party and, if appropriate, other relevant Council working parties (e.g. IXIM and the Frontiers' Working Party) informed (no operational information or personal data regarding the FTFs should be communicated in this context). Participating Member States' competent authorities notify Europol once their respective share of the list has been processed and provide information on created alerts.

Europol informs the Service acting as Presidency of the CTG in accordance with the applicable rules on transfer of personal data of the outcome of the exercise.

**Step 7** [*Feedback to Third Country*]

Europol and Member States shall ensure that information on hits related to FTFs inserted in SIS is shared in accordance with EU legislation. Hence, Europol can only send information back to a third country in accordance with SIS Regulations, subject to the consent of the issuing Member State. If the Member State allows the use of such information, its handling by Europol shall be governed by the applicable rules on transfer of personal data to third entities as set out in the Europol Regulation.

---

**Coordinated approach:** Assessment: Entering third party data on FTF into the SIS (*simplified scheme*)

