Council of the European Union

Brussels, 16 November 2020
(OR. en)

11564/3/20
REV 3

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.:	11564/20
Subject:	Defining a process for evaluating and possibly entering information from third countries on suspected Foreign Terrorist Fighters in the Schengen Information System

1. The objective of this paper is to set out a process for evaluating information on suspected Foreign Terrorist Fighters (FTFs) from third countries 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 coordinated process together with a revised visual chart can be found in the Annex.

2. The revised draft is a compromise that intends to reflect a very diverse scene of Member States' comments. Due to the high importance of the subject, the Presidency intends to finalise the dossier and start a first, voluntary trial period. After an appropriate time frame and no later than 2 years after the adoption, TWP should evaluate the coordinated approach and possibly introduce changes to the process.

3. The background for the process is well-known: 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 all, European as well as non-European, FTFs are detected should they try to cross EU borders, and that action is taken upon receipt of identities of suspected FTFs. Much of the information on non-European FTFs is held by third countries.

4. 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.

5. Since autumn 2019, it has been discussed at length, at both meetings in the Commission and at Europol as well as in Council Working Parties[1] if and how to define an adequate procedure, taking into account legal and operational constraints (see the previous papers for a more elaborate background)[2]. The attached updated draft describes a revised process that takes into account the concerns expressed by Member States following the consultations subsequent to the Terrorism Working Party (TWP) of 13 October 2020 and further deliberation. It aims at ensuring that appropriate and timely action is taken upon the receipt by Europol of a list of suspected FTFs from a third country.

6. Most Member States recognise the need to act at EU-level and have given detailed replies[3] to the requests for contribution aiming at finding an appropriate solution. Against this background, and taking into account Member States' comments from the repeated rounds of consultation, the Presidency, at this stage, suggests establishing a flexible and voluntary process.

---

1 Commission meetings of 15 November 2019 and 3 March 2020, meetings of the Terrorism Working Party (TWP) of 16 January, 4 March 2020 and 13 October 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.

2 7741/20; 7699/20; 6322/20; 11564/20.

3 WK 5002/2020 + ADD 1, WK 5865/1/2020 REV 1 and WK 11551/2020 + ADD 1.

7. Member States have expressed divergent views on the role of Europol in this process. Due to the complex and diverse nature of the lists to be processed, the Presidency suggests to adopt a flexible approach. The proposed process will allow the Presidency to make use of the technical support by Europol to the extent to which this support would be in compliance with the existing legal framework and in respect of the Agency's mandate, especially during the updating of the list and the information to stakeholders on progress and results.

8. Member States' national security services often possess valuable information in relation to information shared by third countries on FTFs and could contribute to verify its accurateness, but Member States have expressed the will to continue this exchange at national level, without formally involving the Counter Terrorism Group (CTG)[4]. Member States are encouraged to harness the cooperation between intelligence services and law enforcement agencies at national level to avoid any possible information gaps.

9. In the process outlined in the annex, the Presidency will have a coordinating role on updating the list on the basis of Europol's comments and Member States' comments, as well as on informing stakeholders of progress and results.

10. The process/draft outline for a process should apply when a list of suspected FTFs originating from a third country is transmitted directly to Europol.

11. The Presidency invites Member States to agree on the suggested provisional and voluntary process to bring this pressing issue to a successful conclusion. The Presidency invites Member States to agree on the text and to its transmission to the Standing Committee on Internal Security (COSI) for endorsement.

---

[4] 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.

Coordinated approach - Evaluating information on suspected Foreign Terrorist Fighters (FTF) received from third countries for processing in SIS[5]

Draft outline for a process in cases where a list of suspected FTF is transmitted by a third country to Europol.[6]

Step 1 *[Europol informs stakeholders of list and transmits list to Member States and the Presidency)]*

Europol informs the Presidency, the Member States, the Commission and the EU CTC of having received a list with suspected FTF and transmits the list to Member States (through Europol National Units) and the Presidency (or the Presidency's designated national authority). Measures under Step 1 need to respect the current Europol Mandate as well as possible handling codes of the list.

Step *2* *[Europol updates the list]*[7]

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 individuals on the list 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 the SIS legal framework (and provided it complies with Europol's rules on handling codes) to confirm that it indeed relates to the same person and same reason. Where appropriate, the Member State completes the SIS 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.

---

5 This coordinated approach on a voluntary basis shall be evaluated and further modified for operational needs if and when necessary. In any case, Member States agree that an evaluation and discussion in TWP shall take place no later than October 2022.

6 When a list is transmitted to a Member State's authority and not to Europol, it is up to the MS to decide whether to send the list to Europol.

7 It may be decided on a case-by-case basis, if Steps 2 and 3 are carried out simultaneously or subsequently.

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.), SIS 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.

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

After the initial data processing has been completed by Europol, an updated list is communicated to the Presidency.

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

Europol informs the Member States on the outcome of the data processing exercise conducted by Europol by forwarding the updated list. On the basis of this 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 edit the list if necessary.[8] After common consolidation of the list by Member States' competent authorities the results are transmitted to the Presidency.

Step 4 *[Update of the list and agreement on burden sharing]*

The Presidency updates the list on the basis of Europol's comments (Step 2) and Member States' comments (Step 3). The Member States' competent authorities then 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 suspected FTFs allowing for possible entry into 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. Member States can request the Presidency's support in this process if so desired.

[8] A need for editing of the list may arise i.e. due to certain knowledge of a Member State that an individual on the list should in fact not be qualified as a FTF or if an SIS alert would interfere with an investigation.

Member States will inform the Presidency of the setup of this voluntary group and the decided burden sharing. Where for some reason Member States express an impossibility to set up a voluntary group, the Presidency will take on a coordinating role in order to set up such a voluntary group.

The Presidency may choose to request technical support from Europol for Step 4, if and to the extent to which this support would be in compliance with the existing legal framework.

Step 5 *[Participating MS process the list]*

Each participating Member State in the voluntary group processes and analyses the part of the list it has volunteered to examine. Where appropriate and in line with EU and national legislation, relevant information on suspected FTFs is 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 primarily issue decisions to refuse entry and stay or issue European Arrest Warrants, and to use alerts accordingly, 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[9] keep the Presidency informed of the progress on processing the list as frequently as possible, and when the list has been fully processed provide information on created alerts.[10] The Presidency in turn keeps Europol, the Terrorism Working Party and, if appropriate, other relevant Council working parties (e.g. IXIM and the Working Party on Frontiers) informed (no operational information or personal data regarding the FTFs should be communicated in this context).

The Presidency shares necessary information on created alerts with Europol as far as possible. The Presidency may choose to request technical support from Europol for Step 6, if and to the extent to which this support would be in compliance with the existing legal framework and in respect of the Agency's mandate.

Step 7 *[Feedback to Third Country]*

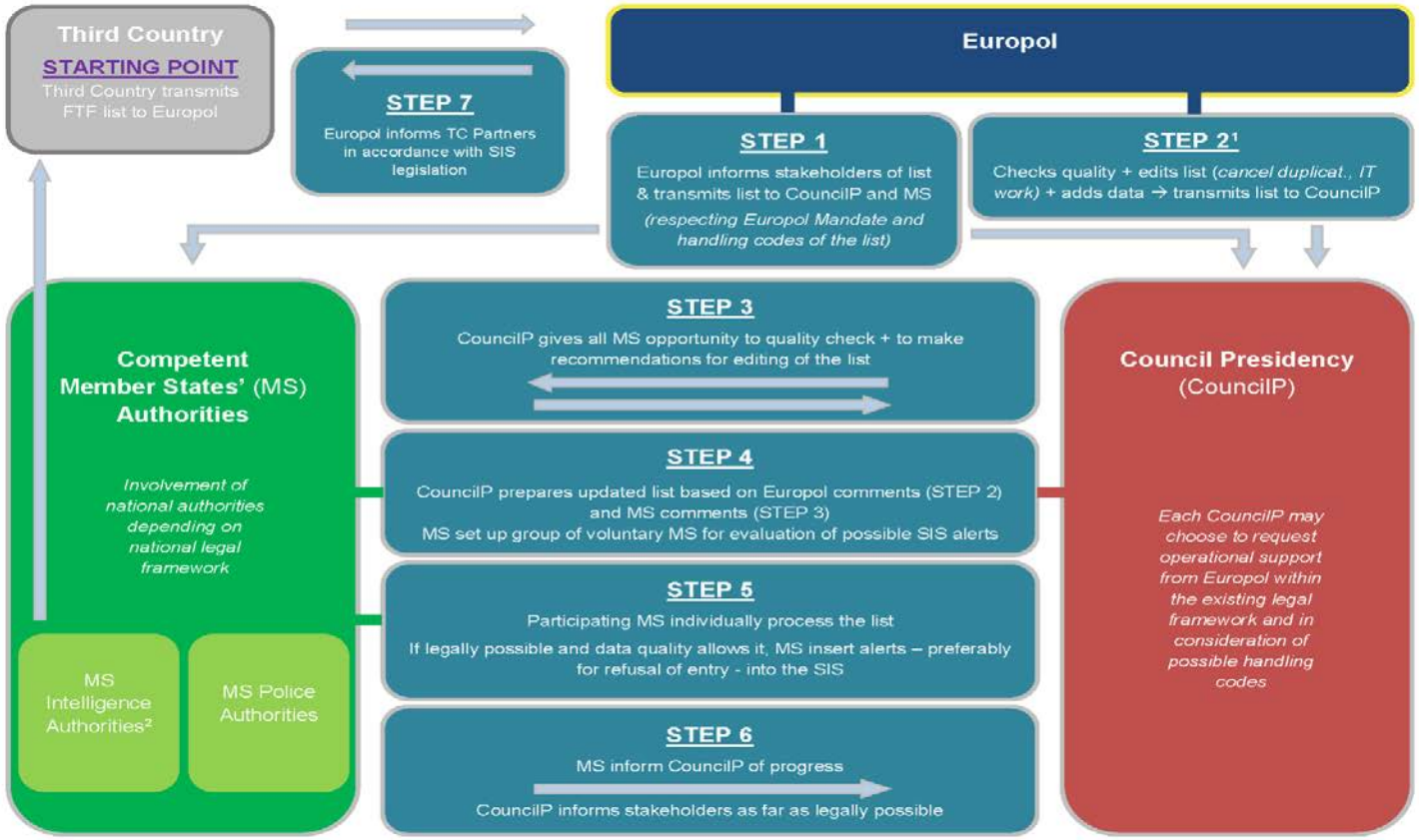
Without prejudice to the communication the European intelligence community may conduct with its foreign counterparts about the information gathered, Europol shall ensure that information on hits related to FTFs inserted in SIS is shared in accordance with EU legislation to the Agency's counterparts in its area of responsibility. Hence, Europol only can send information back to a third country in accordance with the SIS legal framework, 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.

---

[9] The competent authorities will coordinate their results before sending them to the Presidency.

[10] Operational information or personal data regarding the FTFs should only be communicated if legally possible and appropriate.

Coordinated approach: Assessment: Entering third party data on FTF into the SIS *(simplified scheme) (V2)*



[1] In some cases, Step 2 and Step 3 can be conducted simultaneously.
[2] Communication of the European intelligence community with its own foreign counterparts is not regulated by EU law and continues within the relevant legal framework.