



Brussels, 16 November 2021
(OR. en)

13683/21

LIMITE

**CT 153
ENFOPOL 444
COTER 148
JAI 1246
FRONT 400
IXIM 247
COSI 230
COPS 436
COASI 163
COMIX 569**

NOTE

From: Presidency
To: Delegations
No. prev. doc.: WK 10904/2021; 12429/3/21 REV 3
Subject: Procedure on enhanced security checks on persons crossing or having crossed the EU's external borders following developments in Afghanistan

The procedure, as set out in the Annex, was approved by the Terrorism Working Party (TWP) on 10 November 2021.

The Standing Committee on Operational Cooperation on Internal Security (COSI) is kindly requested to endorse the proposed text.

ANNEX

1. Having regard to the **Statement adopted on 31 August 2021 by the extraordinary EU Justice and Home Affairs Council on the situation in Afghanistan¹** which, inter alia,
 - highlighted the potential implications of developments on EU internal security;
 - stressed that the EU and its Member States should do their utmost to ensure that the situation in Afghanistan does not lead to new security threats for EU citizens; and
 - emphasised, that the EU and its Member States, with the support of Frontex, remain determined to effectively protect the EU external borders and prevent unauthorised entries, and assist the most affected Member States. Appropriate security checks should be carried out, including through the full use of relevant EU databases, as well as registration in Eurodac;
 - underlined that the sharing of regular threat assessments and the exchange of information and intelligence, in line with national competences and also with trusted third countries, are of utmost importance; and
 - recalled that the timely performance of security checks of persons being evacuated from Afghanistan remains crucial.
2. Considering the **Counter Terrorism Action Plan on Afghanistan**, presented by the EU Counter Terrorism Coordinator² that recommends that TWP needs to develop, in close cooperation with other relevant Council working parties, a protocol for endorsement by COSI setting up a uniform procedure on the implementation of the several layers of enhanced security checks on persons crossing or having crossed the EU's external borders to mitigate potential security risks stemming from the situation in Afghanistan.

¹ 11385/21 (<https://www.consilium.europa.eu/en/press/press-releases/2021/08/31/statement-on-the-situation-in-afghanistan/>)

² 12315/21.

3. Referring to the analysis produced by Europol, as requested in the Statement, which concludes that, “(...) against the backdrop of an expected increase in migratory flows from Afghanistan to the EU, the threat of terrorists using this as a way to enter the EU undetected, is to be considered. Furthermore, similar to the modus operandi used by irregular migrants, terrorists with other nationalities might pose as Afghan nationals to enter the EU”.
4. Highlighting that the specific procedure set out in this document does not encroach on the principle that national security remains the responsibility of each Member State, and that it fully respects fundamental rights. The procedure is legally non-binding and its implementation by the Member States should respect national legislative provisions and procedures.
5. Observing that Member States' national security services often possess valuable information in relation to information shared by third countries on foreign terrorist fighters (FTFs) and could contribute to verify its accurateness. Member States are encouraged to harness the cooperation between intelligence services and law enforcement agencies at European and national level to avoid any possible information gaps.
6. Stressing that the procedure builds on ad hoc and ongoing work already carried out by the Member States' competent authorities, and is reflecting a political agreement by all Member States; that, therefore, it is without prejudice to existing legal obligations under international, Union or national law, notably under the Schengen Borders Code³, as well as to the implementation of the JHA interoperability architecture.
7. Recognising and respecting the position of Member States who (i) may not be participants to the full Schengen acquis and therefore cannot be subject to its application, and (ii) may not participate in all of the databases and information exchange systems referenced in this document.

³ Regulation (EU) 2016/399 of 9 March 2016 setting out the Schengen Borders Code (OJ L 77, 23.3.2016, p.1).

8. Clarifying that the uniform three level procedure for enhanced security checks of persons crossing or having crossed the EU's external borders applies to all types of borders (air, land, sea) and to humanitarian evacuations from Afghanistan. First level security checks mainly build on already existing obligations under EU legislation, notably the Schengen Borders Code, while second and third level checks set out measures to be carried out by law enforcement agencies and other competent authorities, when appropriate in cooperation with Europol and national intelligence and security services.
9. Specifying that the procedure is not applicable to holders of valid Schengen visas, as well as to long term visa holders, entering the EU. These individuals are *bona fide* travellers whose security status has already been thoroughly checked as part of the visa issuing procedure. Moreover, exempting them allows also for a more efficient use of administrative capacities by keeping the procedure focused on other individuals that have not yet gone through prior security checks.

OUTLINE OF THE PROCEDURE

A. First level checks

All individuals crossing or having crossed the EU's external borders⁴, following recent developments in Afghanistan, who arrived from Afghanistan or a neighbouring or transit country where they resided immediately prior to their arrival, in particular Afghan nationals; individuals declaring to be Afghan nationals; or individuals believed to be Afghan nationals shall be subject to timely first level security checks by the competent national authorities.

These first level checks shall serve the purpose (1) to establish the identity and nationality of the individual, and (2) to ascertain if, on the basis of the first level checks applicable to all individuals falling in the three afore-mentioned categories, the individual represents a potential risk for EU internal security.

⁴ Including those who were intercepted or rescued on their way to the EU Member States

These checks are carried out on the basis of and using

- (a) identity, travel or other documents;
- (b) data or information provided by or obtained from the individual concerned;
- (c) biometric data, including both facial images and dactyloscopic data;
- (d) any identity discovered during the identification or verification.

To this end, the Member States' competent authorities carry out queries and access data in relevant national, EU and international databases and information systems, consulting in particular the Schengen Information System (SIS), by using identity, travel document and dactyloscopic data⁵ (through SIS-AFIS), Interpol Stolen and Lost Travel Documents (SLTD) Database and where appropriate, the Interpol Notices and Diffusions, and Interpol Travel Documents Associated with Notices database (TDAWN).

Where relevant, the checks shall include also physically searching the means of transport and objects in possession of the individual and carrying out a search on the identifiable objects in the SIS.

Member States should make every effort to provide enough administrative capacities to ensure the proper and full implementation of these checks, including by possible requests for the assistance of the European Border and Coast Guard Agency (Frontex) in performing first level checks by deploying experts, including security-vetted interpreters and cultural mediators. Frontex experts deployed can assist with identification, documentary checks and debriefing tasks.

Member States' competent authorities shall ensure that during first level checks, and if applicable, during second and third level checks, individuals remain at their disposal.

⁵ When additional EU databases and information systems aimed at enhancing security and border checks, such as the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) will be operational, they shall also be consulted in the framework of these first level checks.

B. Second level checks

Where first level security checks do not allow a conclusion on the security threat posed by the individual or where there are elements pointing towards a potential threat to EU's internal security based on a risk assessment, the competent national authorities carry out second level checks, unless they decides to take any of measures listed in section D. The second level checks shall consist in:

- consulting further relevant Interpol and Europol databases (Europol Information System (EIS) and in the Organised Crime, Serious Crime and Anti-terrorism databases);
- consultation of national intelligence and security services through the sending of a trace request. The national intelligence and security services could, according to their mandate, inform the competent national authorities of the potential security threat posed by the individual.
- extracting and analysing information from mobile electronic devices in possession of the individuals, in line with national legislative provisions and procedures;
- holding in-depth security interviews.

To enable direct and quick access to Europol databases, the competent national authorities may request Europol's support, in particular the deployment of guest officers, to assist in carrying out risk assessment of individuals and assisting in performing the second level checks.

The relevant data collected on site may be transmitted by the competent national authorities via SIENA to be introduced in Europol databases.

Member States should ensure, with the support of Frontex and/or Europol, if needed and where available, that security-vetted interpreters and cultural mediators are made available for the security interviews.

C. Third level checks

Where, based on the information obtained and the analysis conducted during first and second level checks, duly justified security concerns subsist, the competent authorities proceed to carry out additional security checks consisting in:

- Further consultation of national intelligence and security services on the basis of initial results of the trace request and according to the mechanisms of cooperation and coordination they deem most appropriate, including a consultation with their foreign counterparts. The national intelligence and security services share, according to their mandate with the competent national authorities a consolidated outcome of this consultation in accordance with their national legislations.
- Consultation of relevant information shared by trusted third countries (e.g. on the base of evidence collected in Afghanistan on possible involvement in terrorist or other serious crime activities). Europol may be requested by the competent national authorities to support this process, as appropriate.

D. Follow-up in cases of confirmed security risks

In case security checks performed at one of the three levels reveal substantial security risks, Member States' competent authorities, in accordance with national, Union and international law, in particular Regulation (EC) No 1987/2006⁶ and Council Decision 2007/533/JHA^{7 8}, shall take the appropriate decision, including whether the individual should be arrested and/or eventually prosecuted.

⁶ Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4).

⁷ Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

⁸ Regulation (EU) 2018/1861 and (EU) 2018/1862 of the European Parliament and of the Council govern the establishment, operation and use of SIS. Once applicable, these Regulations will replace Council Decision 2007/533/JHA and Regulation 1987/2006, which currently apply in those matters.

E. Voluntary application to other arrival situations

Member States may decide to retroactively apply this protocol also to humanitarian evacuations carried out from Afghanistan before the endorsement of this protocol.

F. Review

This procedure, and especially its effectiveness, shall be subject to regular review as part of the review of the implementation of the Counter-Terrorism Action Plan, and could be extended to other nationalities. In view of this review, Member States' competent authorities shall keep the Presidency of the Council of the EU and Europol timely informed about the overall picture of security risks detected, and of their follow-up.
