Council of the European Union

Brussels, 13 October 2021
(OR. en)

12429/21

LIMITE

CT 124
ENFOPOL 340
COTER 119
JAI 1045
FRONT 347
IXIM 188
COSI 178
COPS 339
COASI 146
COMIX 510

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	WK 10904/2021
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, takes into account Member States' comments to the previous text (see WK 10904/2021).

It will be discussed at the meeting of the Terrorism Working Party of 14 October 2021.

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 Afghanistan**[1] 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's external borders should be effectively protected and unauthorised entries be prevented by carrying out, with the support of relevant EU Agencies, appropriate security checks, including through the full use of relevant EU databases and information systems, as well as registration in Eurodac, as already requested in relevant EU legislation;

   - 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 Coordinator[2] ~~(doc. 11556)~~ that recommends that TWP needs to ~~COSI~~ 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] 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. Observing 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 its accurateness. Highlighting that the specific procedure set out in this document does not encroach on the principle that national security remains responsibility of each Member State and is legally non-binding.

5. Stressing that t~~T~~he procedure~~, is~~ build~~s~~~~ing~~ 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 Code[3], as well as to the ~~future~~ Proposal for a Regulation for a general screening procedure for third-country nationals at the EU external borders[4] and the implementation of the JHA interoperability architecture.

~~5~~6. 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, and therefore cannot consult such systems and databases.

---

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

4 ~~Doc.~~ 11224/20.

7~~5~~. 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 the intelligence community.

8~~6~~. Specifying that the procedure is not applicable to holders of valid Schengen visas, as well as to long term visa holders, entering the EU.

OUTLINE OF THE PROCEDURE

A. First level checks

All individuals crossing or having crossed the EU's external borders[5] who are:

- Afghan~~i~~ nationals;

- declaring to be Afghan~~i~~ nationals; or

- believed to be Afghan~~i~~ nationals;

and

- arrived from Afghanistan or a neighbouring or transit country where they resided immediately prior to their arrival

shall be subject to timely first level security checks by the competent national authorities ~~at border crossing points, hotspots, or other dedicated premises~~. 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.

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 ~~fingerprints~~dactyloscopic data;

(d) any identity discovered during the identification or verification.

[5] Including those who were intercepted or rescued on their way to the EU Member States

To this end, the Member States' competent authorities shall carry out queries in relevant national, EU and international databases and information systems, consulting in particular the Schengen Information System (SIS), by using identity, travel document and fingerprint and/or palmprint data[6] (through SIS-AFIS), the Interpol Notices and Diffusions, Interpol Stolen and Lost Travel Documents (SLTD) Database, Interpol Travel Documents Associated with Notices database (TDAWN) and other relevant Interpol databases[7].

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 ~~In order~~ to ensure the proper and full implementation of these checks, ~~if the number of checks is exceeding administrative capacities, the Member States should~~ including by requesting the assistance of the European Border and Coast Guard Agency (Frontex) in performing first level checks by deploying experts, including security-vetted interpreters. Frontex experts deployed can assist with identification, documentary checks and debriefing tasks.

Member States' competent authorities shall ensure the necessary control and surveillance of individuals during first level security checks, and if applicable, during second and third level checks, to avoid absconding.

---

6 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.

7 [Suggestion to insert an overview of tools and databases].

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 ~~shall~~ carry out second level checks, unless ~~it~~ they decide~~s~~ 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 ~~CTG (Counter Terrorism Group)~~national intelligence and security services through the sending of a trace request. The ~~CTG~~ national intelligence and security services ~~shall~~ could, according to their mandate, inform the competent national authorities of the ~~results of this request~~ 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.

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.

To enable direct and quick access to Europol databases, t~~T~~he competent national authorities ~~shall~~ may request Europol's ~~assistance~~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~~,~~ ~~enabling direct and quick access to Europol databases~~.

The relevant data collected on site ~~will~~ 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, that security-vetted intepreters 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 individual concerned shall be subject to additional security checks consisting in:

- Further consultation of ~~CTG~~ national intelligence and security services and its foreign counterparts on the basis of initial results of the trace request. The ~~CTG~~ national intelligence and security services ~~shall~~ will according to their mandate share with the competent national authorities a consolidated outcome of this consultation.

- Consultation of 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 shall take the appropriate decision, in accordance with national, Union and international law, whether the individual should be:

- stopped, arrested and eventually prosecuted;

- [subject to a refusal of entry (Art. 14 Regulation (EU) 2016/399) as a result of first level checks, issued an entry ban and an alert for refusal of entry and stay in SIS (Art. 24 Regulation (EU) 2018/1861) or returned in accordance with Directive 2008/115/EC and with national law transposing that Directive;

- subject to an alert introduced in SIS for discreet checks, inquiry checks or specific checks (Art. 36 of Regulation (EU) 2018/1862.][8]

  Member States' competent authorities shall keep the Presidency of the Council of the EU and Europol ~~(ECTC)~~ timely informed of cases where security risks were detected, and of their follow-up. Upon request, Europol can provide a statistical overview to the Presidency. ~~The Presidency in turn keeps the European Commission (DG HOME), the EU Counter-Terrorism Coordinator, the Terrorism Working Party and, if appropriate, other relevant Council working parties (e.g. COTER and the Working Party on Frontiers) informed without communicating any operational information or personal data regarding the cases or individuals concerned.~~

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 clause

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.

---

[8] Text in square brackets to be further examined; part of the legislation is currently being negotiated.