FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

EUROPOL

Future Group on Travel Intelligence and Border Management

Outcome of the 3rd Workshop – 9 & 10 December 2019

Introduction

On 9 & 10 December 2019 the third Workshop of the Future Group on Travel Intelligence and Border Management, jointly organised by Frontex and Europol, was held at the Headquarters of Frontex in Warsaw, Poland. This report presents the outcome of that workshop, along with the related highlights of the discussions. This third Workshop is part of a series, aimed at identifying operational opportunities stemming from recent policy developments related to security, border management and interoperability at EU level.

Main focus of the meeting

This third workshop was aimed at discussing and comparing the different forms of profiling along the border continuum. The identification and use of risk, crime and threat patterns can be found in border management, security and migration. The differences and similarities might allow for mutual strengthening of existing processes and possible alignment into a more interconnected, holistic approach.

Risk Management Processes of Third Country Nationals before the Borders

The steady increase in number of **Schengen Visa** applications and visas issued raises the issue whether security screening i.e. mandatory/regulatory DBs checks could be "modulated" according to the risk picture of the TCN. In any case a harmonization of examination and decision process is required with a more important role of the Central Authority relying on consultation with different other EU and national authorities although local knowledge from the consulate remains critical.

Nationality based risk profiles are regularly reviewed and adding a new nationality to the risk group requires prior assessment of the visa authorities capacity to handle this. Proposed VIS recast will provide more information including more DBs to be checked for assessing the individual application but will also increase the workload for the examination of the application. VIS recast also provides the possibility to develop precise risk profiles on irregular migration, security and an high epidemic risks similar to ETIAS.

Risk assessment in the visa domain can also be implemented by data driven and knowledge-driven profiles. This would allow the visa officer to distinguish between high risk and low risk applicants and proceed respectively with intensive or fast tracking of the visa applications. Data driven profiles are based on factual data (e.g. past visa or border officers decisions) using solid and clear methodology. Apart from data driven risk profiles, the risk management process for the visa officer should also imply to assess the applicant or the sponsor themselves. It is interesting for the latter to cross-match sponsors names with illegal employers lists or registers, if available.

ETIAS risk management approach and methodology is still being developed based on the respective implementing and delegated acts discussed in the Commission Committee. It is clear that Irregular migration risks profiles will be mainly data-driven. EES records in particular refusals of entry at the external borders and over-stayers or ETIAS applications decisions will be

the most important data to be analysed. Security risks will be intelligence driven from information form MS and Europol which will have to be translated into ETIAS profiles and screening rules. High epidemic risks indicators for ETIAS screening rules will be based on recommendations from WHO / EU Health Security Committee on how to address the epidemic risk from a border management perspective.

Frontex has also developed **advance information guidelines** which demonstrate the possibilities for developing common approaches to the creation of risk profiles including risk profiles template also for sharing risk profiles or underlying intelligence. A clear separation can be made between the analytical work for the preparation of risk profiles including background information and preliminary analysis and their implementation which is normally performed by the targeting centre. The feedback loop on the results of the targeting in operations (e.g. at border checks) is essential for the quality review and regular update of the risk indicators.

EASO presented on the risk management aspects of its support to **asylum processes** of Member States. Of particular relevance in this context is the application of the asylum exclusion clause if for instance they committed serious crimes or acts of terrorism. This would justify an automated check against police systems, such as SIS, TDAWN and Europol data, but only a check against Eurodac is mandatory. These database checks thanks also to the future interoperability tools could potentially be aligned with the checks foreseen for ETIAS and for the visa application process in the future. Also the sharing of crime patterns and terrorism-related profiles is not a common practice for the screening of asylum applicants.

Processing of API/PNR data

The processing of API data and the combined processing of PNR and API data were presented from several national perspectives. Although the respective national legal frameworks differ, the main requirements for an effective contribution to border management and criminal investigations are comparable. For the definition of effective targeting rules, it is essential to have the right input from competent authorities, as well as a healthy appetite for the services of API-centres and PIUs (some barriers due to high data protection and procedural requirements were reported). Also the feedback from border forces and investigation departments on the results of the risky passengers reported on the basis of targeting is indispensable to refine and update the risk profiles and targeting rules.

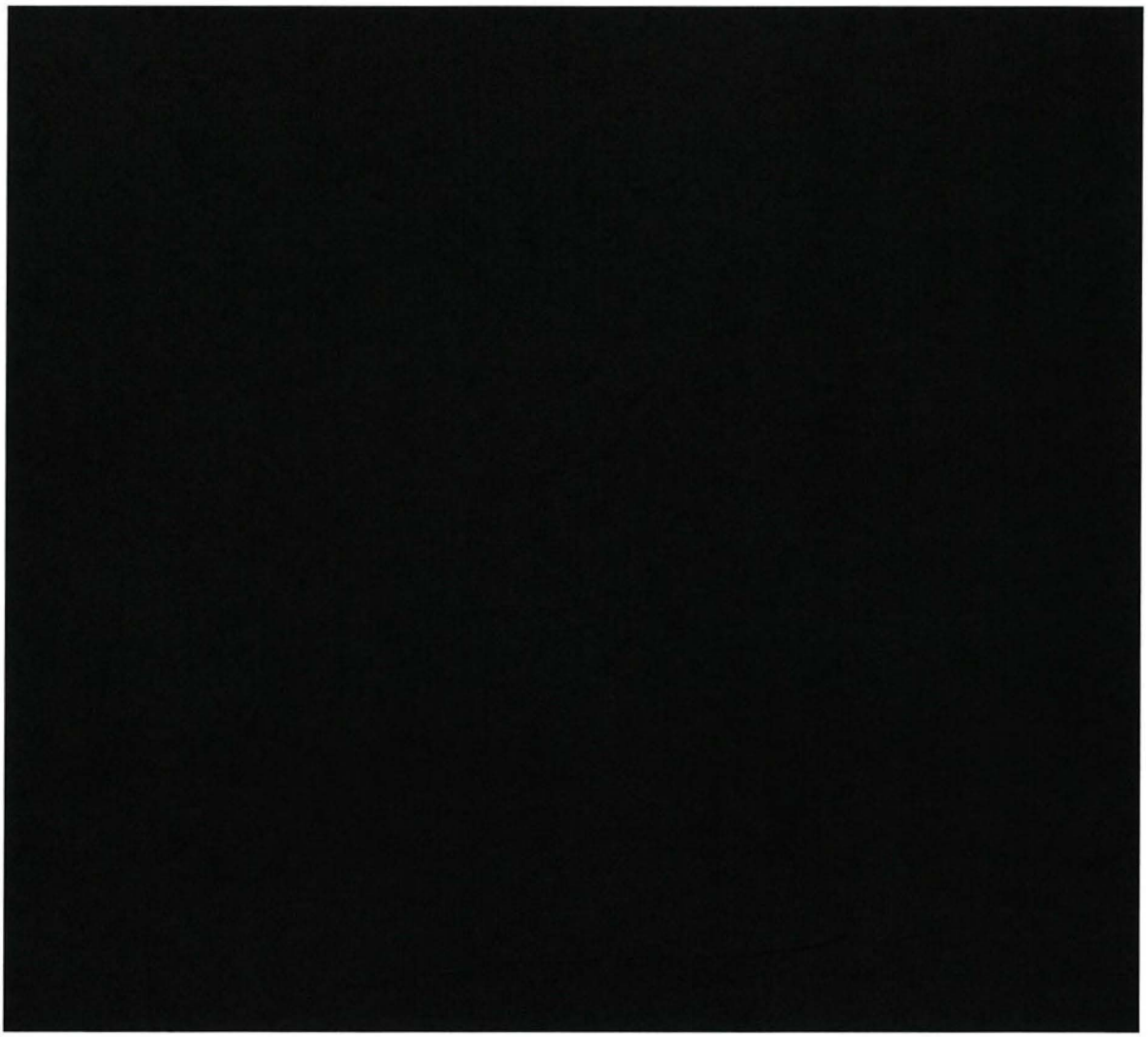
The presenting countries also elaborated on the targeting methods developed and applied. Although each approach was developed in function of the national conditions and characteristics, the general concepts that were designed and implemented were more or less similar, consisting mostly of list-based, rule-based and affiliate-based forms of targeting. Despite the high degree of operational orientation and independence, for the sharing of targeting rules and underpinning intelligence the respective targeting entities are largely dependent on the competent authorities that factually own that information. Some Member States combine the focus on risky travellers with the facilitation of a smoother passage for bona fide travellers.

Challenges are equally shared amongst Member States, including data quality. [redacted] The combination of API and PNR data is generally perceived as valuable, where the PNR data allows for the early risk assessment and the API-data can then serve to confirm the identity data.

The existing practices in targeting and risk management were also compared to the approaching reality of ETIAS, for which some foresee an integration with the API/PNR targeting function. The respective objectives, the methodology and the threat perspective would justify the combination of services into an integrated targeting capacity to support border checks. Yet, the partial differences in processing purposes require careful consideration as part of the realisation.

Europol presented its current and planned activities in the processing of PNR data, including some practical examples of how Member States and Europol's Analysis Projects are being supported. Whilst still in an early stage, the potential for the collection and sharing of intelligence for profiling and the exchange of targeting rules was also explained. Member States emphasized the importance of having smooth access to SIENA from the PIUs to make full use of Europol's assistance and services.

Main takeaways from the presentations and discussions



FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

EUROPOL

Operational pilot(s)

The possibilities were reiterated for suitable cross-border investigations that might benefit from a pro-active support from Europol and Frontex for enrichment by available travel intelligence and border management sources. A first potential investigation was assessed, but the practical possibilities for supporting it from a combined border/security perspective, were deemed limited.

Another case was suggested in view of its association to cross-border travel. Frontex and Europol will look into the suggested case.

Attendance

The Workshop was attended by representatives from several Member States, eu-Lisa, EASO, Frontex and Europol, from varying professional backgrounds and competent authorities, which allowed to approach the topics discussed from multiple relevant angles. The setting was informal among experts, without official, national or organisational positions, which stimulated the open and out-of-the-box orientation of the discussions.

Next meetings

- Workshop 4: 3 & 4 February 2020; Europol Headquarters, The Hague
- Workshop 5: 30 & 31 March 2020; Frontex Headquarters, Warsaw

Due to the absence of any Customs representatives at the third workshop, it was proposed to have a dedicated focus on Customs cooperation at one of the future workshops. Also the risk management from the Customs perspective can then be addressed. It was also considered to invite non-EU representatives for that discussion. This applies especially to US Customs and Border Protection, because that agency has a combined mandate for the border management concerning persons and goods.

Other topics for future meetings include security/border checks for EU citizens and residents; the mapping of data sources and follow-up channels for international cooperation; use/business cases for person-centric data management and a back office function supporting frontline border management.

Further information

The current report on the outcome of the third Workshop of the Future Group will be shared with the stakeholders associated to Frontex and Europol. Further information can be obtained by contacting:

- [redacted] at Frontex via [redacted] or
- [redacted] at Europol via [redacted].